HYBRID WARFARE THROUGH THE PRISM OF CYBER DOMAIN

COL. Prof. Dr
Mitko
BOGDANOSKI
Vice-Dean of the Military academy

Dr. Sc. Mitko Bogdanoski, Associate Professor, Colonel
Vice Dean at the Military Academy
“General Mihailo Apostolski”
mitko.bogdanoski@ugd.edu.mk
mitko.Bogdanoski@mod.gov.mk

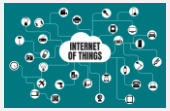
1

Artificial intelligence

Augmented reality

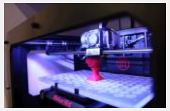
BLOCKCHAIN
Blockchain

Drones


INTERNET OF THINGS
Internet of things

Robotics

Virtual reality


3-D printing

2

How Technology is Shaping the Battlefield?

3

4

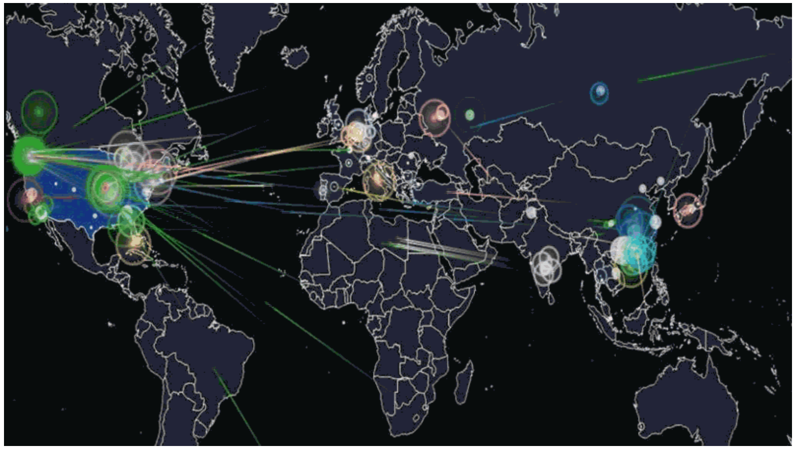
5

6

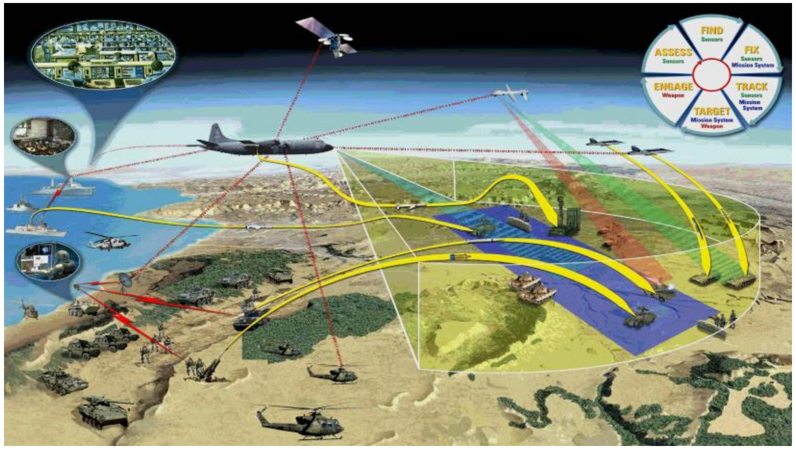
How Technology is Shaping the Battlefield

- Space War -

7



8


FIND
Sensors
FIX
Sensors
Mission System
TRACK
Sensors
Mission System
TARGET
Mission System
Weapon
ENGAGE
Weapon
ASSESS
Sensors

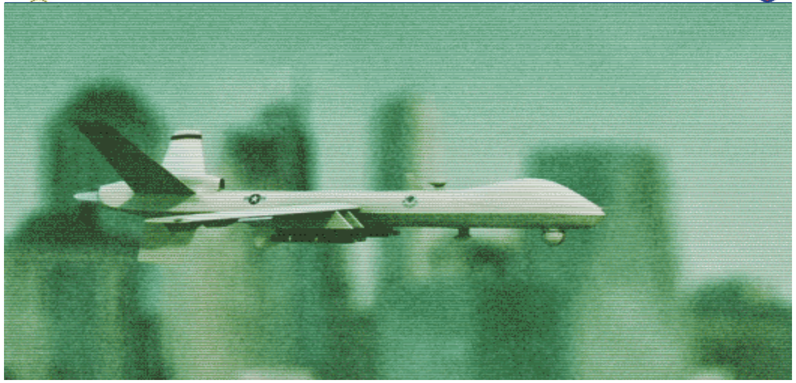
How Technology is Shaping the Battlefield

Five Domains

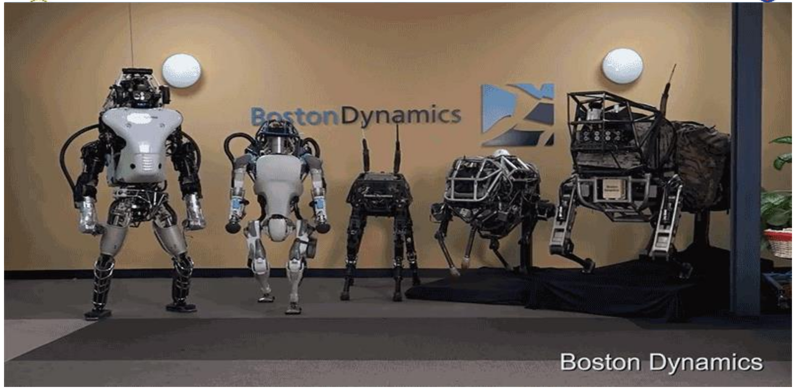
- Land
- Sea
- Air
- Space
- Cyberspace

- …?!

Drones

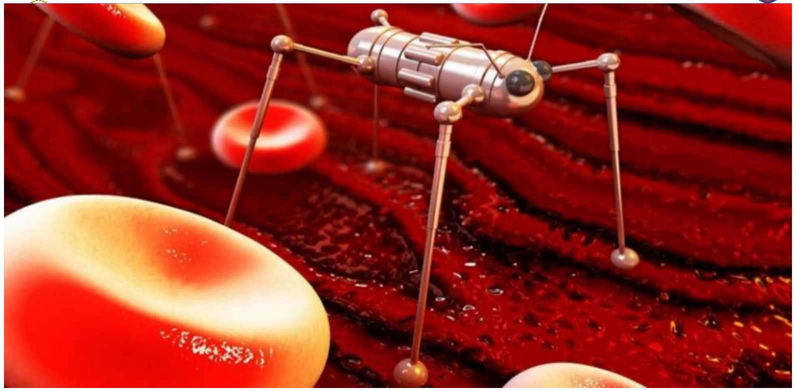


Robotics

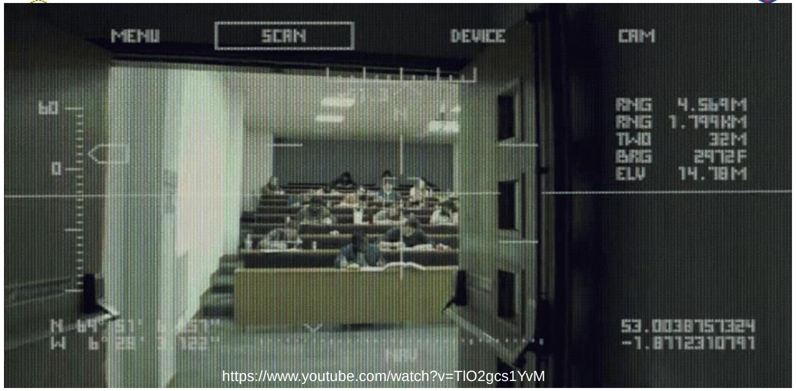

Boston Dynamics
Boston Dynamics

DNA: Genetic weapons / Ethnic bioweapons

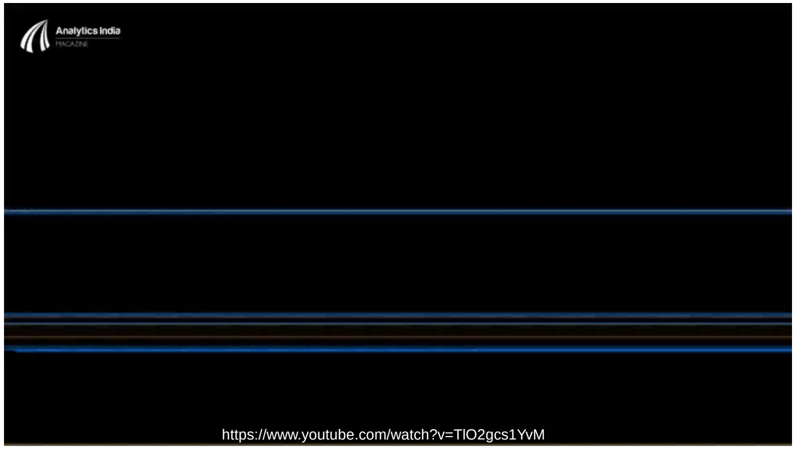
Nano technology



Micro Drones Killer Arms Robots


MENU
SCAN
DEVICE
CAM
60
0
RNG 4.569M
RNG 1.799KM
TWD 32M
BRG 2972F
ELV 14.78M
53.0038757324
-1.8712310791

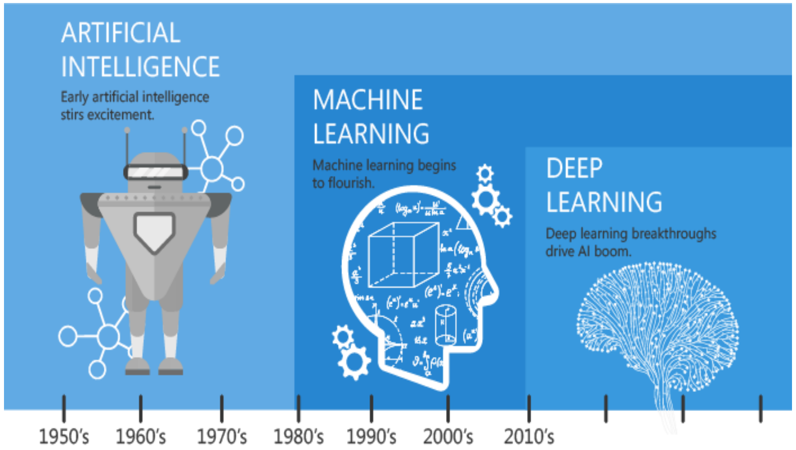
https://www.youtube.com/watch?v=TlO2gcs1YvM


Analytics India
MAGAZINE

https://www.youtube.com/watch?v=TlO2gcs1YvM

INVESTMENT
INITIATIVE
FUTURE
INVESTMENT
INITIATIVE
CNBC

AI, Machine Learning and Deep Learning



ARTIFICIAL INTELLIGENCE

Early artificial intelligence stirs excitement.

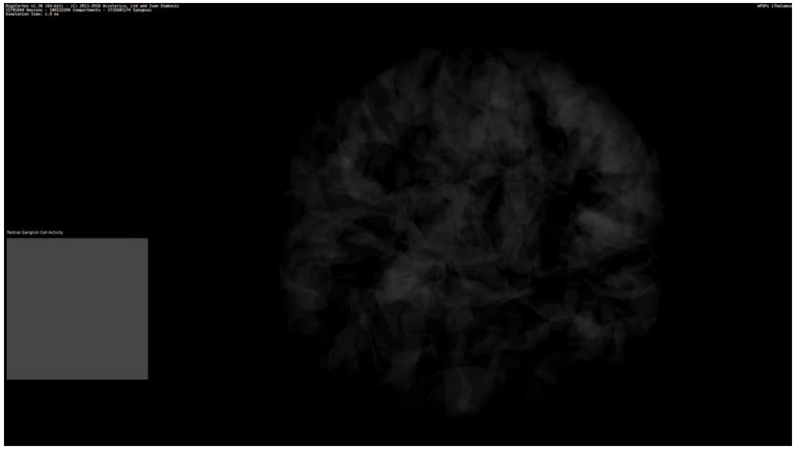
MACHINE LEARNING

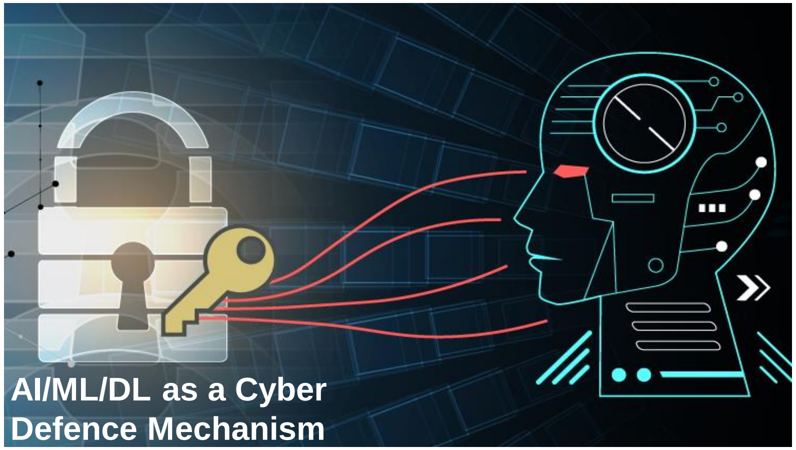
Machine learning begins to flourish.

DEEP LEARNING

Deep learning breakthroughs drive AI boom.

1950's
1960's
1970's
1980's
1990's
2000's
2010's


Retinal Ganglion Cell Activity

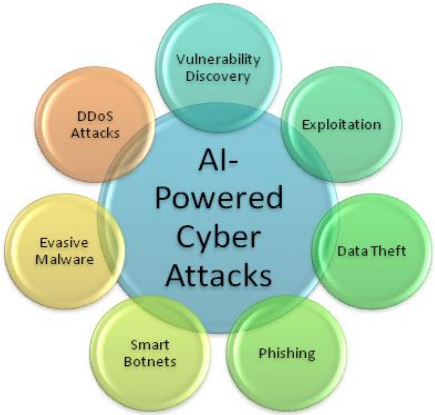


AI/ML/DL as a Cyber Defence Mechanism

AI:

Hackers' New Weapon for Cyber Attack

HaltDos Blog



AI-Powered Cyber Attacks

Vulnerability Discovery

Exploitation

Data Theft

Phishing

Smart Botnets

Evasive Malware

DDoS Attacks

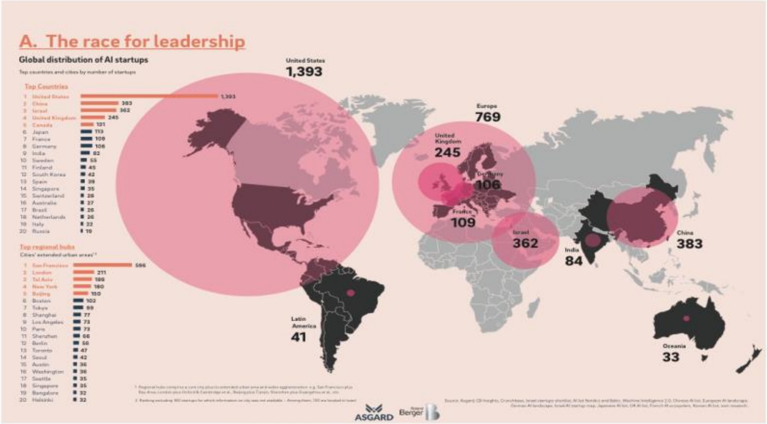
'WHOEVER LEADS IN AI WILL RULE THE WORLD'

РОССИЯ
ВСЕРОССИЙСКИЙ ОТКРЫТЫЙ УРОК
ПРОЕКТОРИЯ

ARTIFICIAL INTELLIGENCE IS THE FUTURE

Will we ever become second most intelligent being on the planet?!

"Okay, I will destroy humans."
CNBC



A. The race for leadership

Global distribution of AI startups

Top countries and cities by number of startups

Top Countries

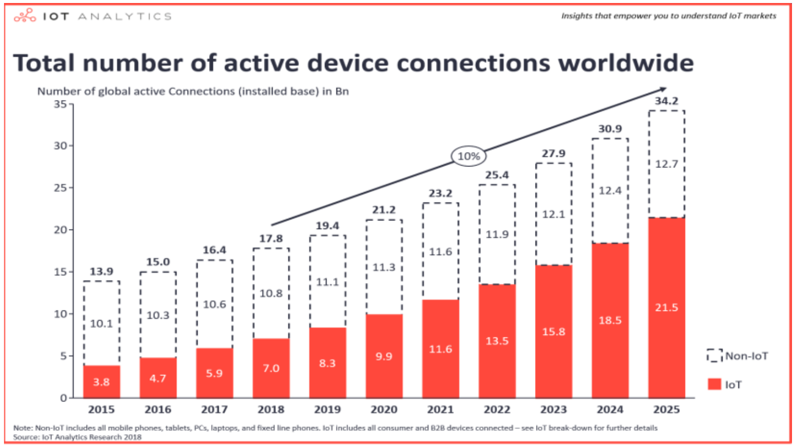
1	United States	1,393
2	China	383
3	Israel	362
4	United Kingdom	245
5	Canada	131
6	Japan	113
7	France	109
8	Germany	106
9	India	82
10	Sweden	55
11	Finland	45
12	South Korea	42
13	Spain	39
14	Singapore	35
15	Switzerland	28
16	Australia	27
17	Brazil	26
18	Netherlands	26
19	Italy	22
20	Russia	19

Top regional hubs

Cities' extended urban areas[1]

1	San Francisco	596
2	London	211
3	Tel Aviv	189
4	New York	180
5	Beijing	150
6	Boston	102
7	Tokyo	99
8	Shanghai	77
9	Los Angeles	73
10	Paris	73
11	Shenzhen	66
12	Berlin	56
13	Toronto	47
14	Seoul	42
15	Austin	36
16	Washington	36
17	Seattle	35
18	Singapore	35
19	Bangalore	32
20	Helsinki	32

United States
1,393
Europe
769
United Kingdom
245
Germany
106
France
109
Israel
362
India
84
China
383
Latin America
41
Oceania
33
ASGARD
Roland Berger



IOT ANALYTICS

Insights that empower you to understand IoT markets

Total number of active device connections worldwide

Number of global active Connections (installed base) in Bn

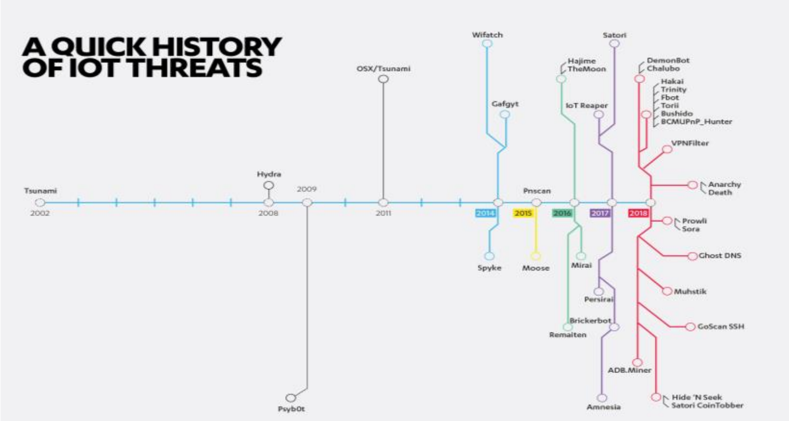
Note: Non-IoT includes all mobile phones, tablets, PCs, laptops, and fixed line phones. IoT includes all consumer and B2B devices connected – see IoT break-down for further details
Source: IoT Analytics Research 2018

Welcome Home

Griffin Home smart appliances and chargers connect to handle daily routines effortlessly.

GRIFFIN

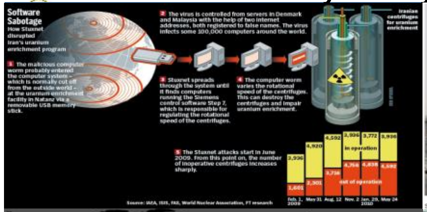
FIRMNESS CONTROL
CLIMATE CONTROL
VIBRO MASSAGE SYSTEM
ANTI-SNORING
MOVEMENT SENSOR
APP CONTROL
MONITORING SLEEP APP
Balluga



A QUICK HISTORY OF IOT THREATS
Tsunami
2002
Hydra
2008
2009
Psyb0t
OSX/Tsunami
2011
Wifatch
Gafgyt
2014
Spyke
Pnscan
2015
Moose
Hajime
TheMoon
IoT Reaper
2016
Mirai
Remaiten
Satori
2017
Persirai
Brickerbot
Amnesia
DemonBot
Chalubo
Hakai
Trinity
Fbot
Torii
Bushido
BCMUPnP_Hunter
VPNFilter
2018
Anarchy
Death
Prowli
Sora
Ghost DNS
Muhstik
GoScan SSH
ADB.Miner
Hide 'N Seek
Satori CoinTobber

https://www.privateinternetaccess.com/blog/2019/04/heres-how-internet-of-things-malware-is-undermining-privacy/

Examples of Cyber Attacks disruptive for the Cyber Physical Systems



Software Sabotage
How Stuxnet disrupted Iran's uranium enrichment program

1 The malicious computer worm probably entered the computer system – which is normally cut off from the outside world – at the uranium enrichment facility in Natanz via a removable USB memory stick.

2 The virus is controlled from servers in Denmark and Malaysia with the help of two internet addresses, both registered to false names. The virus infects some 100,000 computers around the world.

3 Stuxnet spreads through the system until it finds computers running the Siemens control software Step 7, which is responsible for regulating the rotational speed of the centrifuges.

4 The computer worm varies the rotational speed of the centrifuges. This can destroy the centrifuges and impair uranium enrichment.

5 The Stuxnet attacks start in June 2009. From this point on, the number of inoperative centrifuges increases sharply.

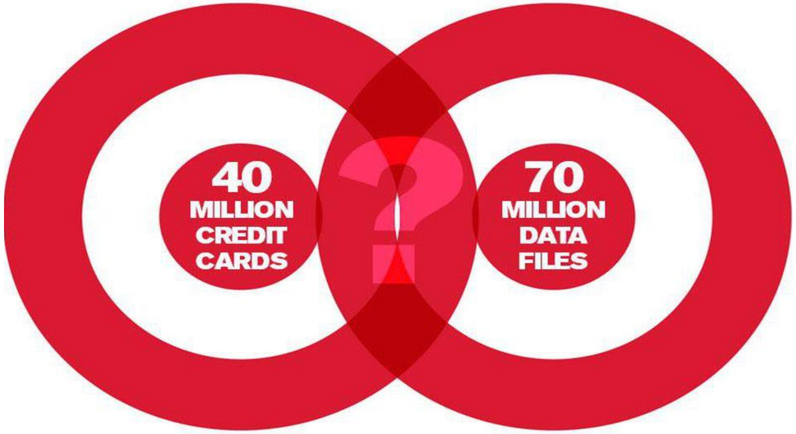
Source: IAEA, ISIS, FAS, World Nuclear Association, FT research

Iranian centrifuges for uranium enrichment
in operation
out of operation
3,936
1,601
4,920
2,301
4,592
3,716
3,936
4,756
3,772
4,838
3,936
4,592
Feb. 1, 2009
May 31
Aug. 12
Nov. 2
Jan. 29, 2010
May 24

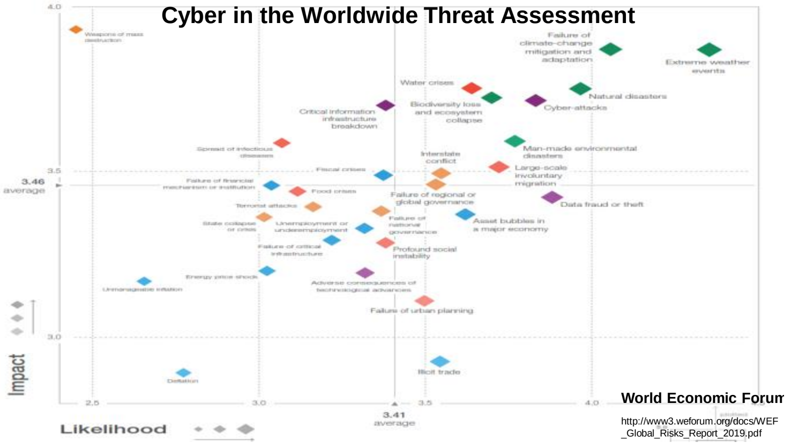
Saudi Aramco suffered the worst hack in world history in 2012.

Country
Botnet
IP Address
Brazil
Venezuela
Russia
Taiwan
Mirai
MIRAI

DEVELOPING NOW
IRANIAN HACKERS TARGETED DAM NEAR NEW YORK CITY
CNN
SITUATION ROOM

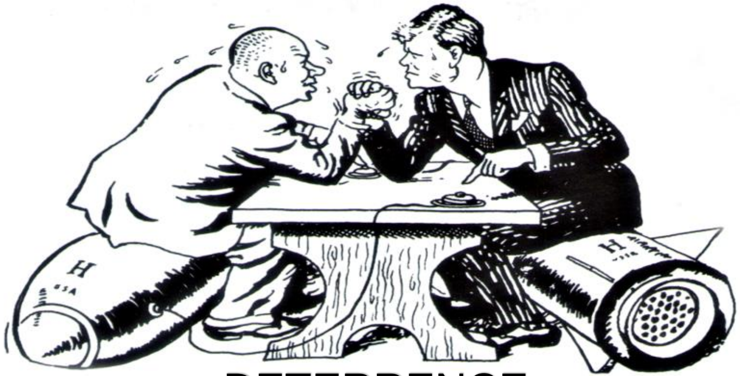

40
MILLION
CREDIT
CARDS
?
70
MILLION
DATA
FILES

Cyber in the Worldwide Threat Assessment



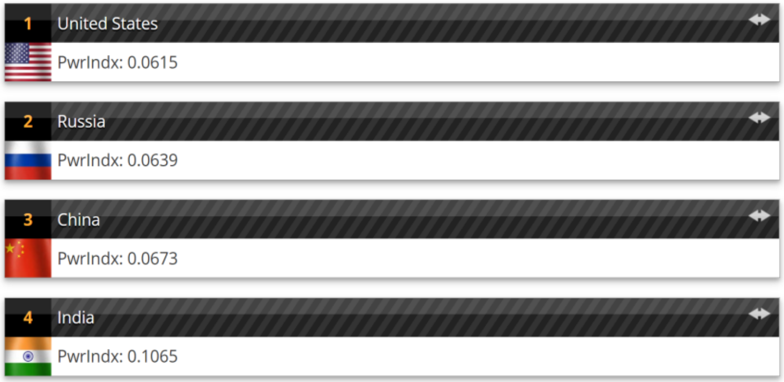
World Economic Forum

http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf



DETERRENCE

2019 Military Strength Ranking



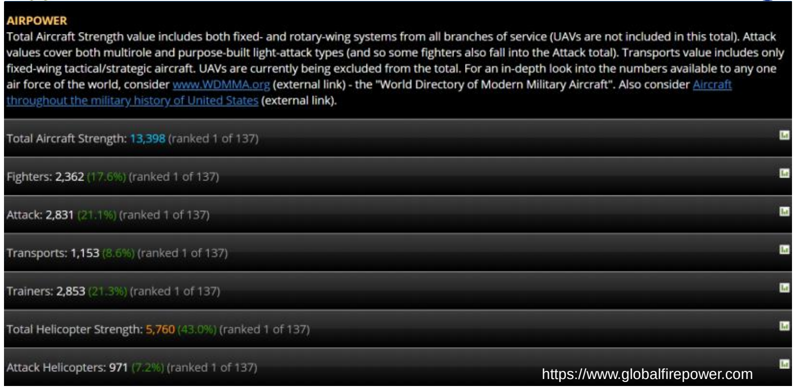
1 United States
PwrIndx: 0.0615

2 Russia
PwrIndx: 0.0639

3 China
PwrIndx: 0.0673

4 India
PwrIndx: 0.1065

2019 USA Military Power



AIRPOWER

Total Aircraft Strength value includes both fixed- and rotary-wing systems from all branches of service (UAVs are not included in this total). Attack values cover both multirole and purpose-built light-attack types (and so some fighters also fall into the Attack total). Transports value includes only fixed-wing tactical/strategic aircraft. UAVs are currently being excluded from the total. For an in-depth look into the numbers available to any one air force of the world, consider www.WDMMA.org (external link) - the "World Directory of Modern Military Aircraft". Also consider Aircraft throughout the military history of United States (external link).

Total Aircraft Strength: 13,398 (ranked 1 of 137)

Fighters: 2,362 (17.6%) (ranked 1 of 137)

Attack: 2,831 (21.1%) (ranked 1 of 137)

Transports: 1,153 (8.6%) (ranked 1 of 137)

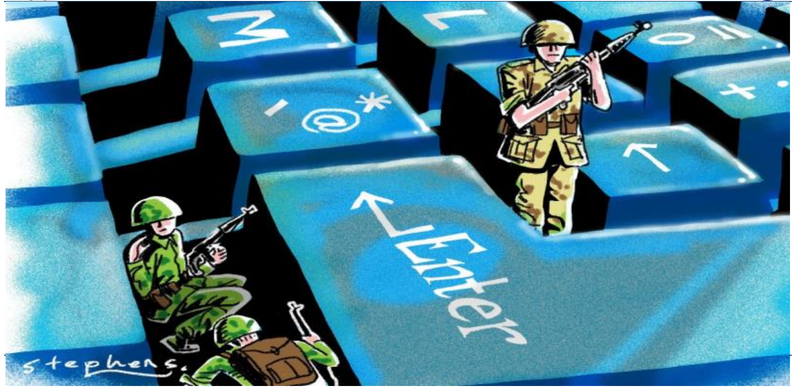
Trainers: 2,853 (21.3%) (ranked 1 of 137)

Total Helicopter Strength: 5,760 (43.0%) (ranked 1 of 137)

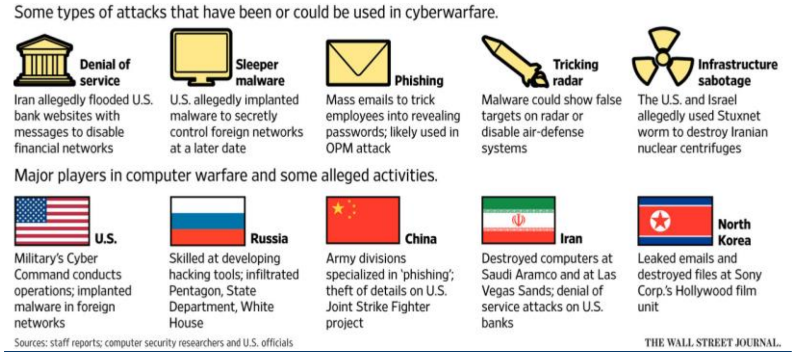
Attack Helicopters: 971 (7.2%) (ranked 1 of 137)

https://www.globalfirepower.com

How to Show the Cyber Power? - Foggy



Digital Battlefield – Who has the Best Offensive Capabilities?



Some types of attacks that have been or could be used in cyberwarfare.

Denial of service
Iran allegedly flooded U.S. bank websites with messages to disable financial networks

Sleeper malware
U.S. allegedly implanted malware to secretly control foreign networks at a later date

Phishing
Mass emails to trick employees into revealing passwords; likely used in OPM attack

Tricking radar
Malware could show false targets on radar or disable air-defense systems

Infrastructure sabotage
The U.S. and Israel allegedly used Stuxnet worm to destroy Iranian nuclear centrifuges

Major players in computer warfare and some alleged activities.

U.S.
Military's Cyber Command conducts operations; implanted malware in foreign networks

Russia
Skilled at developing hacking tools; infiltrated Pentagon, State Department, White House

China
Army divisions specialized in 'phishing'; theft of details on U.S. Joint Strike Fighter project

Iran
Destroyed computers at Saudi Aramco and at Las Vegas Sands; denial of service attacks on U.S. banks

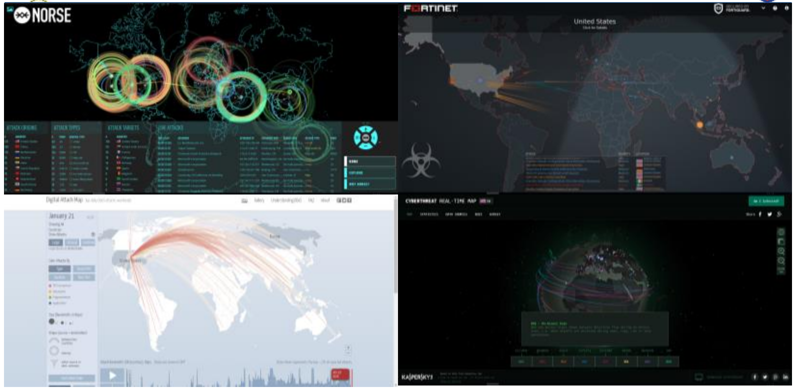
North Korea
Leaked emails and destroyed files at Sony Corp.'s Hollywood film unit

Sources: staff reports; computer security researchers and U.S. officials

THE WALL STREET JOURNAL.

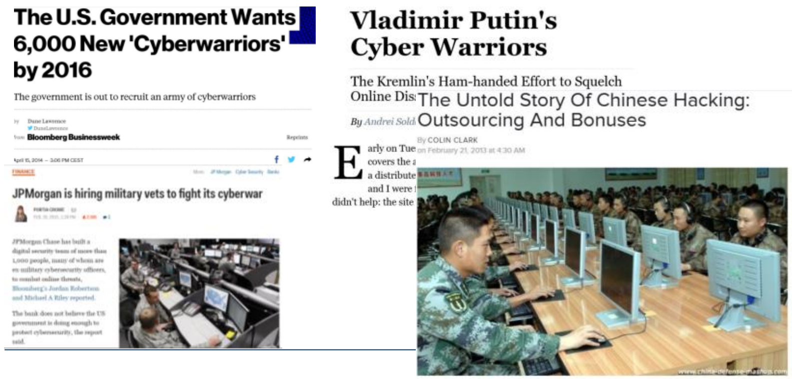
39

Visual Cyber-Security: See Attacks On Real Time



State Supported (Governmental) Cyber Attacks
vs
Criminal Cyber Attacks

Cyber Warriors



The U.S. Government Wants 6,000 New 'Cyberwarriors' by 2016

The government is out to recruit an army of cyberwarriors

By Dune Lawrence
@DuneLawrence
From Bloomberg Businessweek
Reprints

April 15, 2014 – 3:06 PM CEST

FINANCE

JPMorgan is hiring military vets to fight its cyberwar

JPMorgan Chase has built a digital security team of more than 1,000 people, many of whom are ex-military cybersecurity officers, to combat online threats, Bloomberg's Jordan Robertson and Michael A Riley reported.

The bank does not believe the US government is doing enough to protect cybersecurity, the report said.

Vladimir Putin's Cyber Warriors

The Kremlin's Ham-handed Effort to Squelch Online Dis

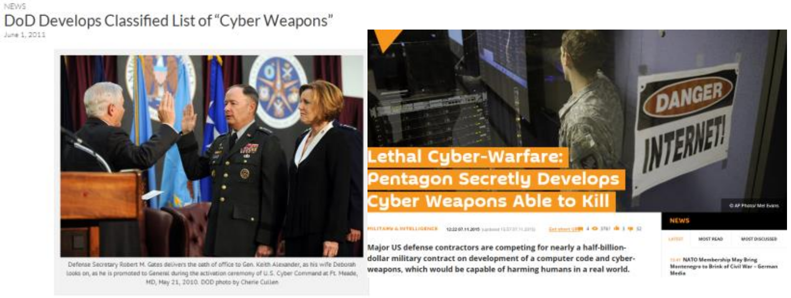
By Andrei Sold

Early on Tue
covers the a
a distribute
and I were
didn't help: the site

The Untold Story Of Chinese Hacking: Outsourcing And Bonuses

By COLIN CLARK
on February 21, 2013 at 4:30 AM

Cyber Weapons



NEWS

DoD Develops Classified List of "Cyber Weapons"

June 1, 2011

Defense Secretary Robert M. Gates delivers the oath of office to Gen. Keith Alexander, as his wife Deborah looks on, as he is promoted to General during the activation ceremony of U.S. Cyber Command at Ft. Meade, MD, May 21, 2010. DOD photo by Cherie Cullen

Lethal Cyber-Warfare: Pentagon Secretly Develops Cyber Weapons Able to Kill

© AP Photo/ Mel Evans

MILITARY & INTELLIGENCE 12:22 07.11.2015

Major US defense contractors are competing for nearly a half-billion-dollar military contract on development of a computer code and cyber-weapons, which would be capable of harming humans in a real world.

NEWS
LATEST MOST READ MOST DISCUSSED
19:41 NATO Membership May Bring Montenegro to Brink of Civil War – German Media

Modern weapons economy

How much does a stealth bomber cost? **$1.5 to $2 billion**

How much does a stealth fighter cost? **$80 to $120 million**

How much does a cruise missile cost? **$1 to $2 million**

How much does a cyber weapon cost? **Much Cheaper**

Find the Weapons Facility

Nuclear Weapons Facility

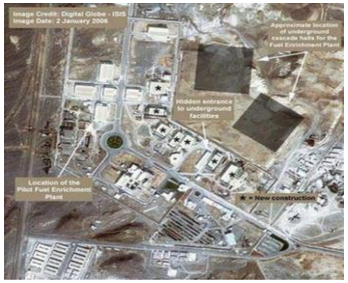
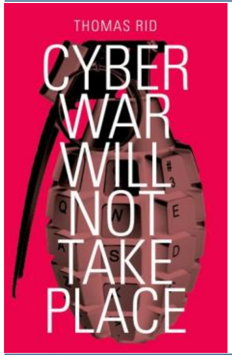


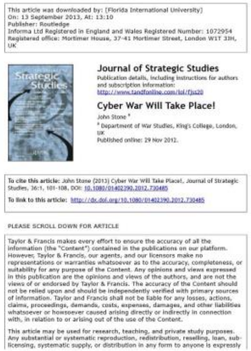
Image Credit: Digital Globe - ISIS
Image Date: 2 January 2006
Approximate location of underground cascade halls for the Fuel Enrichment Plant
Hidden entrance to underground facilities
Location of the Pilot Fuel Enrichment Plant
★ = New construction

Cyber Weapons Facility

Where's the Cyber Weapons Facility?

Cyber War





This article was downloaded by: [Florida International University]
On: 13 September 2013, At: 13:10
Publisher: Routledge
Informa Ltd Registered in England and Wales Registered Number: 1072954
Registered office: Mortimer House, 37-41 Mortimer Street, London W1T 3JH, UK

Journal of Strategic Studies
Publication details, including instructions for authors and subscription information:
http://www.tandfonline.com/loi/fjss20

Cyber War Will Take Place!

John Stone [a]

[a] Department of War Studies, King's College, London, UK

Published online: 29 Nov 2012.

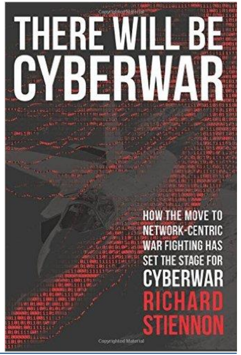
To cite this article: John Stone (2013) Cyber War Will Take Place!, Journal of Strategic Studies, 36:1, 101-108, DOI: 10.1080/01402390.2012.730485

To link to this article: http://dx.doi.org/10.1080/01402390.2012.730485

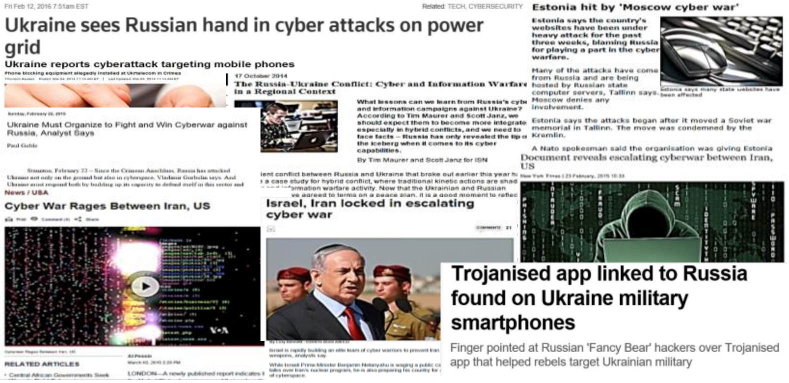
PLEASE SCROLL DOWN FOR ARTICLE

Taylor & Francis makes every effort to ensure the accuracy of all the information (the "Content") contained in the publications on our platform. However, Taylor & Francis, our agents, and our licensors make no representations or warranties whatsoever as to the accuracy, completeness, or suitability for any purpose of the Content. Any opinions and views expressed in this publication are the opinions and views of the authors, and are not the views of or endorsed by Taylor & Francis. The accuracy of the Content should not be relied upon and should be independently verified with primary sources of information. Taylor and Francis shall not be liable for any losses, actions, claims, proceedings, demands, costs, expenses, damages, and other liabilities whatsoever or howsoever caused arising directly or indirectly in connection with, in relation to or arising out of the use of the Content.

This article may be used for research, teaching, and private study purposes. Any substantial or systematic reproduction, redistribution, reselling, loan, sub-licensing, systematic supply, or distribution in any form to anyone is expressly


THERE WILL BE CYBERWAR
HOW THE MOVE TO NETWORK-CENTRIC WAR FIGHTING HAS SET THE STAGE FOR CYBERWAR
RICHARD STIENNON

Cyber War (or Hybrid War)?



Fri Feb 12, 2016 7:51am EST

Related: TECH, CYBERSECURITY

Ukraine sees Russian hand in cyber attacks on power grid

Ukraine reports cyberattack targeting mobile phones

Phone blocking equipment allegedly installed at Ukrtelecom in Crimea

17 October 2014

The Russia-Ukraine Conflict: Cyber and Information Warfare in a Regional Context

What lessons can we learn from Russia's cyber and information campaigns against Ukraine? According to Tim Maurer and Scott Janz, we should expect them to become more integrated, especially in hybrid conflicts, and we need to face facts – Russia has only revealed the tip of the iceberg when it comes to its cyber capabilities.

By Tim Maurer and Scott Janz for ISN

Ukraine Must Organize to Fight and Win Cyberwar against Russia, Analyst Says

Paul Goble

Estonia hit by 'Moscow cyber war'

Estonia says the country's websites have been under heavy attack for the past three weeks, blaming Russia for playing a part in the cyber warfare.

Many of the attacks have come from Russia and are being hosted by Russian state computer servers, Tallinn says. Moscow denies any involvement.

Estonia says many state websites have been affected

Estonia says the attacks began after it moved a Soviet war memorial in Tallinn. The move was condemned by the Kremlin.

A Nato spokesman said the organisation was giving Estonia

Document reveals escalating cyberwar between Iran, US

News / USA

Cyber War Rages Between Iran, US

Israel, Iran locked in escalating cyber war

RELATED ARTICLES

LONDON—A newly published report indicates

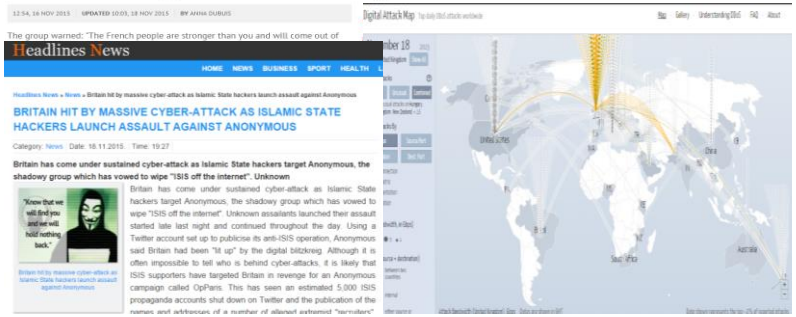
Trojanised app linked to Russia found on Ukraine military smartphones

Finger pointed at Russian 'Fancy Bear' hackers over Trojanised app that helped rebels target Ukrainian military

---

Terrorists' Cyber Attacks

Anonymous declares war on Islamic State after Paris attacks in chilling video: 'We will hunt you down'



12:54, 16 NOV 2015 | UPDATED 10:03, 18 NOV 2015 | BY ANNA DUBUIS

The group warned: "The French people are stronger than you and will come out of

Headlines News

HOME NEWS BUSINESS SPORT HEALTH

Headlines News » News » Britain hit by massive cyber-attack as Islamic State hackers launch assault against Anonymous

BRITAIN HIT BY MASSIVE CYBER-ATTACK AS ISLAMIC STATE HACKERS LAUNCH ASSAULT AGAINST ANONYMOUS

Category: News Date: 18.11.2015 Time: 19:27

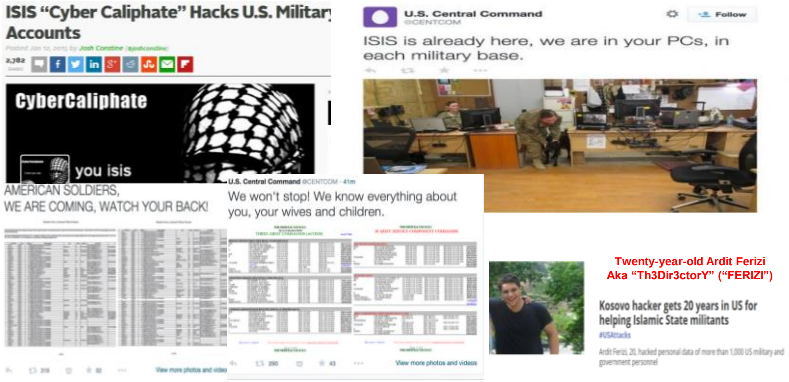
Britain has come under sustained cyber-attack as Islamic State hackers target Anonymous, the shadowy group which has vowed to wipe "ISIS off the internet". Unknown

"Know that we will find you and we will hold nothing back."

Britain hit by massive cyber-attack as Islamic State hackers launch assault against Anonymous

Britain has come under sustained cyber-attack as Islamic State hackers target Anonymous, the shadowy group which has vowed to wipe "ISIS off the internet". Unknown assailants launched their assault started late last night and continued throughout the day. Using a Twitter account set up to publicise its anti-ISIS operation, Anonymous said Britain had been "lit up" by the digital blitzkreig. Although it is often impossible to tell who is behind cyber-attacks, it is likely that ISIS supporters have targeted Britain in revenge for an Anonymous campaign called OpParis. This has seen an estimated 5,000 ISIS propaganda accounts shut down on Twitter and the publication of the names and addresses of a number of alleged extremist "recruiters".

Terrorists’ Cyber Attacks



ISIS “Cyber Caliphate” Hacks U.S. Militar Accounts

Josh Constine

CyberCaliphate

you isis

AMERICAN SOLDIERS,
WE ARE COMING, WATCH YOUR BACK!

U.S. Central Command @CENTCOM

ISIS is already here, we are in your PCs, in each military base.

U.S. Central Command @CENTCOM · 41m

We won't stop! We know everything about you, your wives and children.

View more photos and videos

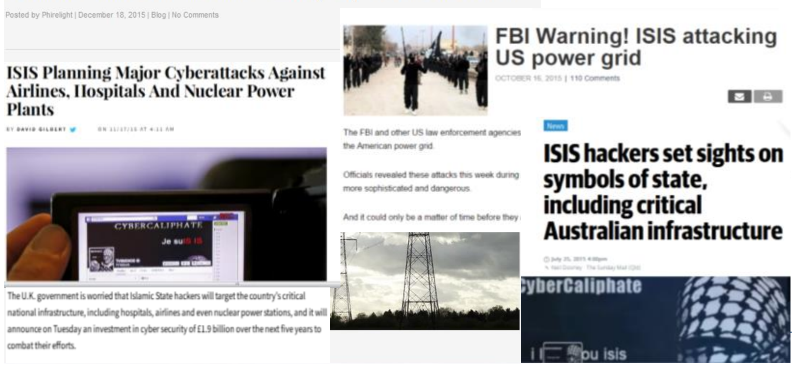
Twenty-year-old Ardit Ferizi
Aka “Th3Dir3ctorY” (“FERIZI”)

Kosovo hacker gets 20 years in US for helping Islamic State militants

#USAttacks

Ardit Ferizi, 20, hacked personal data of more than 1,000 US military and government personnel

Terrorists’ Cyber Attacks – Attempts



Canada’s Critical Infrastructure Security Gap & The ISIS Threat

Posted by Phirelight | December 18, 2015 | Blog | No Comments

ISIS Planning Major Cyberattacks Against Airlines, Hospitals And Nuclear Power Plants

BY DAVID GILBERT

The U.K. government is worried that Islamic State hackers will target the country’s critical national infrastructure, including hospitals, airlines and even nuclear power stations, and it will announce on Tuesday an investment in cyber security of £1.9 billion over the next five years to combat their efforts.

FBI Warning! ISIS attacking US power grid

OCTOBER 16, 2015 | 110 Comments

The FBI and other US law enforcement agencies
the American power grid

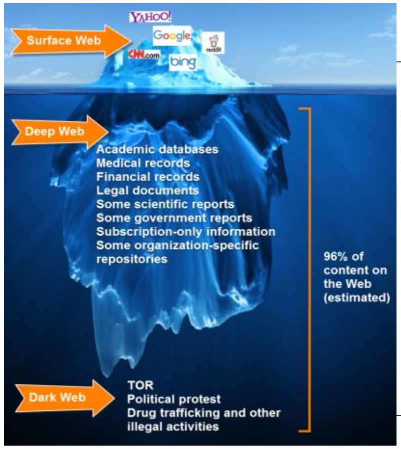
Officials revealed these attacks this week during
more sophisticated and dangerous

And it could only be a matter of time before they

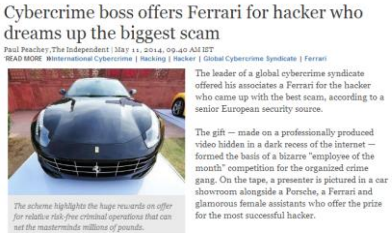
News

ISIS hackers set sights on symbols of state, including critical Australian infrastructure

CYBERCALIPHATE
Je suis IS
yberCaliphate
ou isis


YAHOO!
Google
CNN.com
bing
reddit
Surface Web
Deep Web
Academic databases
Medical records
Financial records
Legal documents
Some scientific reports
Some government reports
Subscription-only information
Some organization-specific repositories
96% of content on the Web (estimated)
Dark Web
TOR
Political protest
Drug trafficking and other illegal activities

Black Market / Dark Web



Cybercrime boss offers Ferrari for hacker who dreams up the biggest scam

Paul Peachey, The Independent | May 11, 2014, 09.40 AM IST

READ MORE International Cybercrime | Hacking | Hacker | Global Cybercrime Syndicate | Ferrari

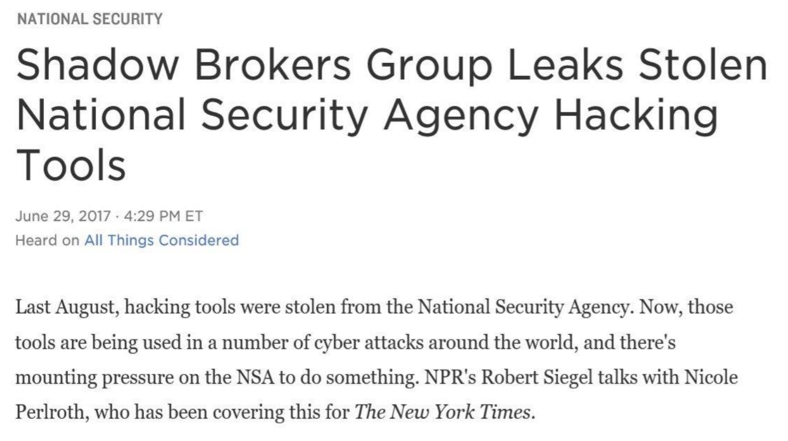
The scheme highlights the huge rewards on offer for relative risk-free criminal operations that can net the masterminds millions of pounds.

The leader of a global cybercrime syndicate offered his associates a Ferrari for the hacker who came up with the best scam, according to a senior European security source.

The gift — made on a professionally produced video hidden in a dark recess of the internet — formed the basis of a bizarre "employee of the month" competition for the organized crime gang. On the tape, a presenter is pictured in a car showroom alongside a Porsche, a Ferrari and glamorous female assistants who offer the prize for the most successful hacker.

NSA DATA CENTER

300,000,000 Hacking Attempts per Day!

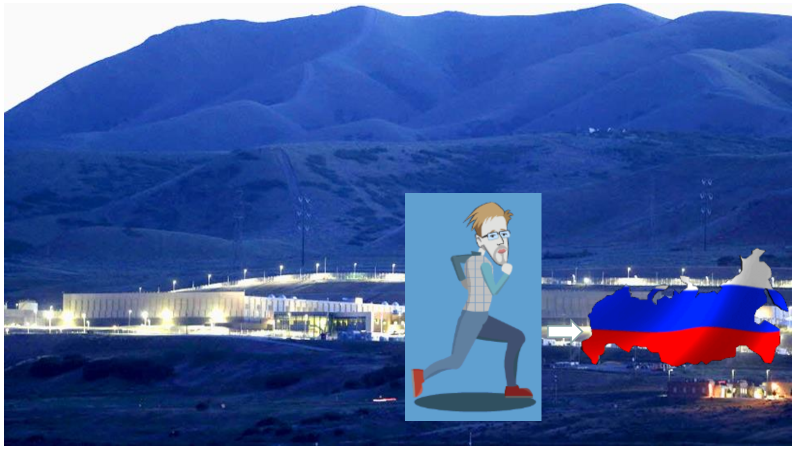


NATIONAL SECURITY

Shadow Brokers Group Leaks Stolen National Security Agency Hacking Tools

June 29, 2017 · 4:29 PM ET
Heard on All Things Considered

Last August, hacking tools were stolen from the National Security Agency. Now, those tools are being used in a number of cyber attacks around the world, and there's mounting pressure on the NSA to do something. NPR's Robert Siegel talks with Nicole Perlroth, who has been covering this for *The New York Times*.



Features of the Cyber Weapons:

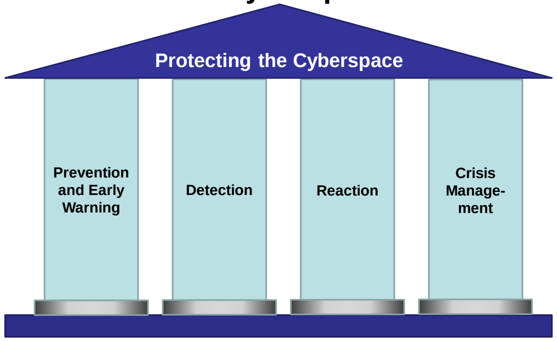
Effective
Affordable
Deniable

Matt Murphy

Challenges with the Cyber Weapons

Expiration!!!

The Four Pillars for Protecting the Cyberspace

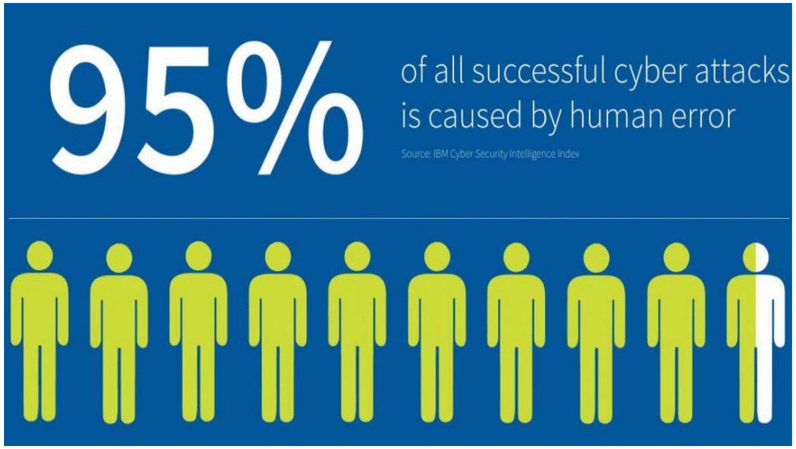


Protecting the Cyberspace

- Prevention and Early Warning
- Detection
- Reaction
- Crisis Manage-ment

Reasons for Successful Cyber Attack

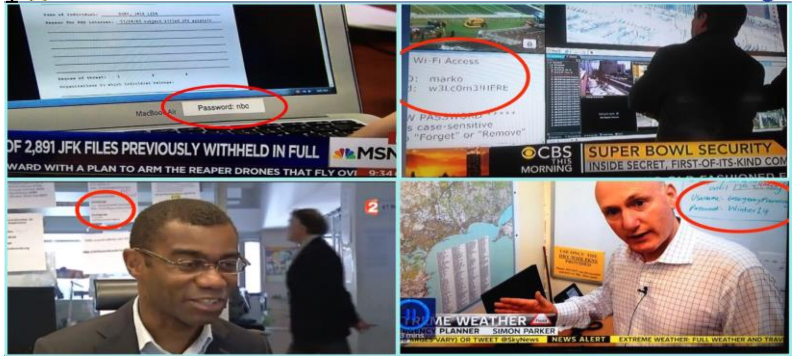
- **Technical**
- **People**

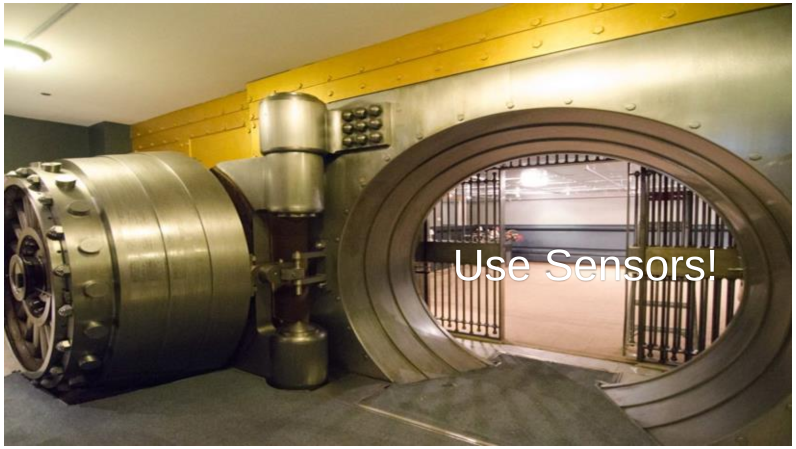


95% of all successful cyber attacks is caused by human error

Source: IBM Cyber Security Intelligence Index

Please stop exposing your passwords

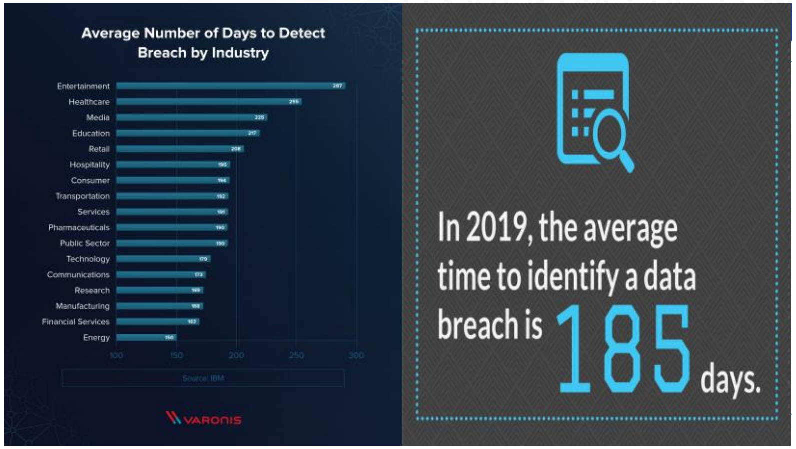

Password: nbc
MacBook Air
OF 2,891 JFK FILES PREVIOUSLY WITHHELD IN FULL
MSN
WARD WITH A PLAN TO ARM THE REAPER DRONES THAT FLY OV
9:34
Wi-Fi Access
marko
w3lc0m3!!!FRE
case-sensitive
"Forget" or "Remove"
CBS THIS MORNING
SUPER BOWL SECURITY
INSIDE SECRET, FIRST-OF-ITS-KIND COM
2
EXTREME WEATHER
PLANNER SIMON PARKER
NEWS ALERT
EXTREME WEATHER: FULL WEATHER AND TRAV



Use Sensors!

Measures (Technical)

- Increase the number of software vulnerabilities discovered
- Increase the number of vulnerabilities disclosed by researchers to software developers
- Increase the speed of patch issuance once developers learn of vulnerabilities in their products
- Increase the number of customers that apply patches to security flaws once issued by software
- Use Defence in Depth, including different hardware and software solutions from different manufacturers.



In 2019, the average time to identify a data breach is 185 days.

Measures (Other)

- National Cyber Security Strategy **(EFFECTIVE!!!)**
  - Holistic approach considering entire Eco System
- Education/Training
- Increased funding for more secure cyberspace
- Institution / team response to cyber threats **(EFFECTIVE!!!)**
  - Teamwork (CERT/CIRT/CSIRT, SOC)
- Information sharing and cooperation (ona national and international level)

Where we should be?

- New profile of experts - trained for offensive and defensive cyber warfare
- Active (Dynamic) instead of Static defense
- Proactive rather than Reactive defense

Where we should be?

“We don’t want to be forensics experts.

We want to catch the enemy before he operationalise the exploit”

Thank you for your attention!

Questions???

Dr. Sc. Mitko Bogdanoski, Associate Professor, Lt Colonel
Military Academy “General Mihailo Apostolski”
mitko.bogdanoski@ugd.edu.mk
mitko.bogdanoski@mod.gov.mk
mitko.Bogdanoski@c3initiative.com
Dr.Mitko.Bogdanoski@ieee.org