



Cyberwar Is India Ready

Presented At
28th Regional Conference
of
WIRC of ICAI

On
Dec. 07, 2013
At
The Lalit, Mumbai

By
Dinesh O. Bareja
Information Security &
Management Advisor

In The Next Half Hour...

- What is war – then, now, ahead
- Cyberwar (what's that!), Estonia and Stuxnet – eye openers or game changers
- India Under Attack
- India Preparedness Scenario
- Conclusions / The Bottom Line

A Brief Introduction

Dinesh O Bareja

- Principal Advisor – Pyramid Cyber Security & Forensic Pvt Ltd
- Cyber Surveillance Advisor – Cyber Defense Research Centre (Jharkhand Police – Special Branch)
- Member IGRC – Bombay Stock Exchange
- COO – Open Security Alliance

Enterprise & Government Policy
Development; Cyber Security Strategy and
Design Architect; Current State Maturity
Assessment & Optimization; Digital
Forensics, Cloud Forensics and Security

Now... Lets talk about ...

- **What is war – then, now, ahead**

- Cyberwar (what's that?) Estonia and Stuxnet – eye openers or game changers
- India Under Attack
- India Preparedness Scenario
- Conclusions / The Bottom Line

Cyberwar Q1: What Is War

War

- Country A against Country B

- India / Pakistan

- US / Iraq

WAS

- Iraq / Kuwait

- NATO / Germany

- World War 1, 2 ... etc...



WAR

WAR



Brings death and destruction
Extensive use of human beings, arms,
bombs, aircraft, ships etc
It had evolved from hand to hand, animal
and chariots to modern warfare

That's What War... WAS!

WAS!

dirty and bloody with a lot of noise, blackouts and mayhem

but now.....

- Times have changed and so have the definition of war
- “modern warfare” is still in the industrial age
- Remember how the definition of heroes has changed since 9/11

Cyberwar Q1: What Is War

Now



Israel raid on Entebbe

War



26/11 attack

IS



Virus attack on Iran Nuclear Plant

Virus attack on Aramco, Saudi Arabia

Pakistani groups mass defacement of Indian websites

Cyberwar Q1: What Is War

Now

Drone Attacks

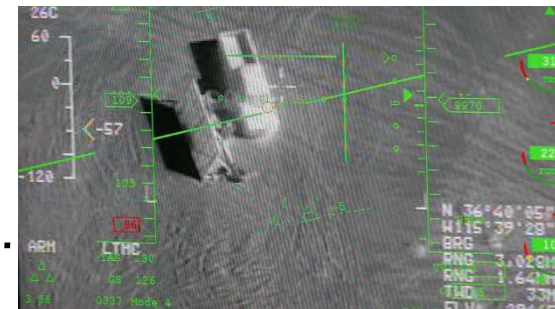


Laser guidance systems

Night vision

War

Bullet Proof vests..



IS

ESSENTIALLY

MINIMUM CONTACT MAXIMUM DAMAGE

Moving on... we look at

- What is war – then, now, ahead
- **Cyberwar (what's that!), Estonia and Stuxnet – eye openers or game changers**
- India Under Attack
- India Preparedness Scenario
- Conclusions / The Bottom Line

- Traditional wars are fought on land, air, sea
- Attack is by a country on a country
- Battlefield is required
- Highly visible damage to life, property
- Lots of flashes, fires and noise
- Involves strict supply chain management to control logistics of movement and support to 1000's of troops, munitions, food etc
- Eventually - Someone wins someone loses

Now For the Million ~~Dollar~~
Rupee Question

WHAT IS CYBERWAR

Cyber

War

IS

Country A
against

<**God-knows-who**>

Cyberwar - Who is your adversary

- Country
- Non-state actors
- Hacktivist
- Cracker / Hacker (age 6 to anything)
- Automation

Cyber

War

IS

According to WIKIPEDIA

Cyberwarfare refers to politically motivated hacking to conduct sabotage and espionage. It is a form of information warfare sometimes seen as analogous to conventional warfare.

and wreaks havoc with the centrifuges

Estonian Internet paralyzed



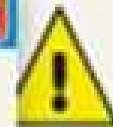
May 2007 | Pro-Russian hackers shut down Estonian websites to avenge the moving of a Soviet-era statue



Intelligence sites hacked by Iran

September 2011 | Iranian hackers break into computers of a Dutch data security firm and forge certificates to gain access to Mossad, CIA and MI6 websites

Water pumps crippled



November 2011 | Hackers break into the computer systems of Texas' and Illinois' water systems, proving the vulnerability of the U.S. water infrastructure

Credit card information exposed



December 2011 | A Saudi hacker announces that he has posted the details of 400,000 Israeli cardholders. In response, Israeli hackers expose information from Saudi accounts

Smart worm found in Iran



May 2012 | The Flame virus is identified. Experts say the virus, 20 times the size and complexity of Stuxnet, spied on computers and users in Iran and the Palestinian Authority

Lockheed Martin hacked

May 2011 | Hackers target

NASA attacked



March 2011 | The aerospace agency admits 13 successful breaches within two years and says it lost codes to the international space station's control system

In Cyberwar This is The Stuff That Should Happen

- DDOS / APT
- Power Shutdown
- Affects Telecom, Banking, Manufacturing, Transport
- Satellite Malware
- Theft of Data / Information – patents, designs, information

In Cyberwar This is The Stuff That Should Happen

- Disrupt Railway network
- Affect Supply Chain - defence, foodstuff, raw material
- Contaminate Water Supply
- APT attack on defence armaments

Three Big Players in the CW game

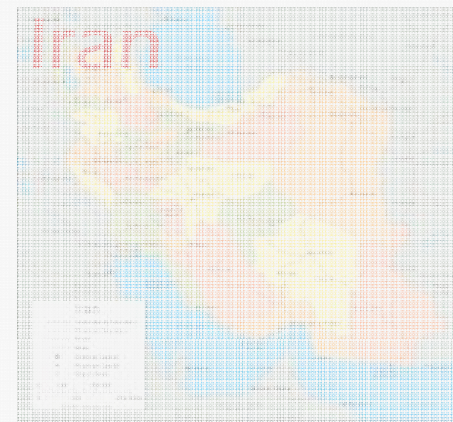
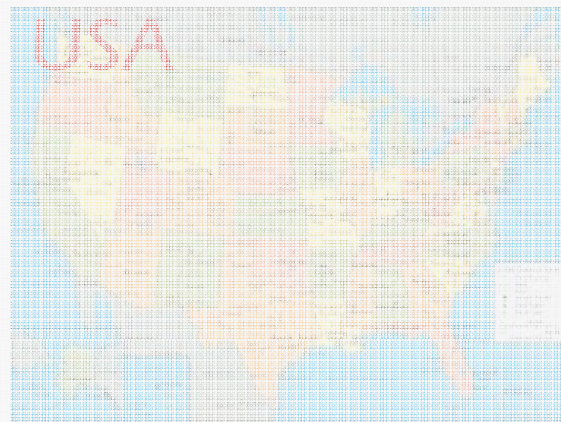


Other Players in the CW game

Israel Russia

Pakistan, Myanmar, Bangladesh, Indonesia, India, Belarus, Ukraine...

Three Big Players in the CW game



They have infiltrated each other, destroyed the Nuclear program, spy on each other, alleged to have brought down systems with virus attacks.

What more has been done is anyone's guess, but the media and everyone is calling this war

BUT
No one is dead yet

Is This War !

< cyber >

< / war >

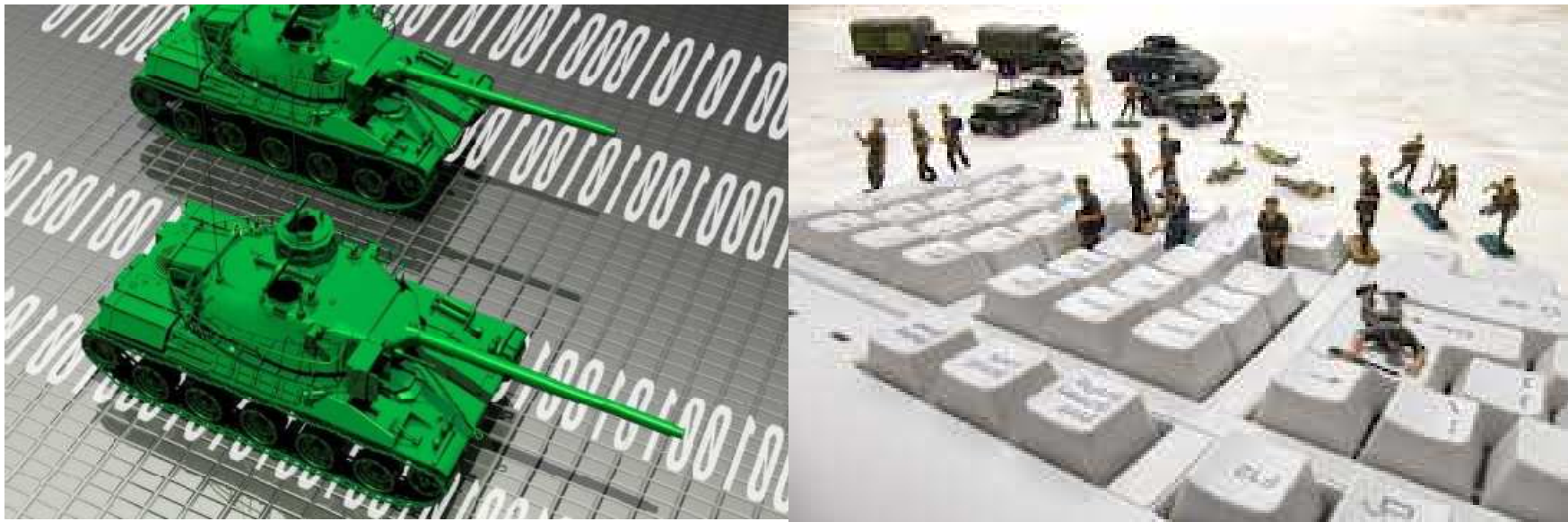
A Paradox

because no one knows what it is

Just like it's parent 'The Internet'

The concept of cyberwar is flawed and meant to confuse everyone except the people who started this subterfuge

Search the internet and this is the type of images you get for cyberwar



Tanks, grenades, jawans clambering on keyboards and binary roads !

Is This is also War

- Website Defacements
- Ransomware
- Rumor via Social Media leading to terror situations
- Micro-finance / crowd sourcing
- Elearning jihadis and terrorists

And This Too...

- Anonymous attacks on banks, media, government infrastructure
- 000's of attacks per minute on Asian Games or Olympic Games

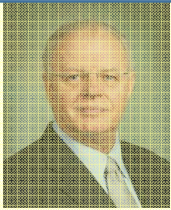
Not Wanting to Confuse You

Or duck the actual topic.

The last few slides were not put in to bring any confusion but to highlight the confusion in the domain and to question “experts” who have yet to do their homework

Actually, Cyberwar will
depend on

who is defining WAR –
defence personnel, hacker
community, mango-people,
government, academics ...



Howard Schmidt,
ex Cyber Security
Co-ordinator for
the White House.

No definitions for Cyberwar!

"We really need to define this word because words do matter. Cyber war is a turbo metaphor that does not address the issues we are looking at like cyber espionage, cyber crime, identity theft, credit card fraud.

"When you look at the conflict environment - military to military - command and control is always part of the thing.

"Don't make it something that it is not," Mr Schmidt told reporters.

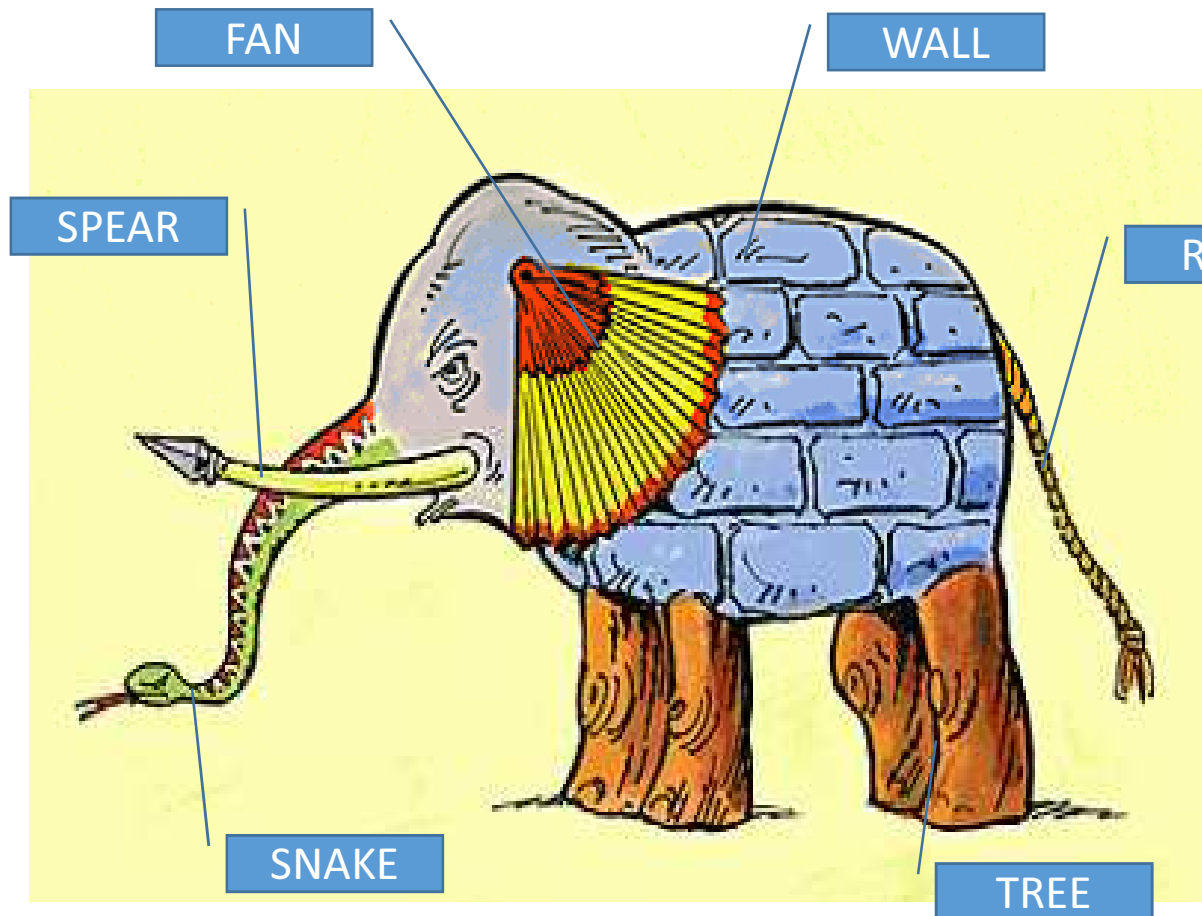


Bruce Schneier,
Chief Security
Officer for BT

"What we are seeing is not cyber war but an increasing use of war-like tactics and that is what is confusing us. We don't have good definitions of what cyber war is, what it looks like and how to fight it,"

<http://www.bbc.co.uk/news/technology-12473809>

Defining Cyberwar or Internet



It was six men of
Indostan To learning
much inclined

Who went to see
the Elephant
(Though all of them
were blind),

That each by
observation Might
satisfy his mind

http://www.uen.org/Lessonplan/downloadFile.cgi?file=28910-2-36017-Blind_Man_elephant.ppt&filename=Blind_Man_elephant.ppt

Now... Lets talk about ...

- What is war – then, now, ahead
- Cyberwar (what's that!), **Estonia and Stuxnet** – eye openers or game changers
- India Under Attack
- India Preparedness Scenario
- Conclusions / The Bottom Line

Estonia

Neither in 2007 nor today are there any internationally accepted definitions on the subject of cyber defense and security

What one nation considers a "cyber attack" might appear more like a "cyber war" to another or even a simple "cyber crime" to a third.

Estonia (pop. 1.3 m)

- In 2007 the country faced a large scale attack by about 1 million botnet
- Almost all government functions are over the internet – voting, parking, banking, identification
- And this was shutdown for the country
- They are NATO members but no one knew what was happening and it was termed as a war later
- The country has free wifi as they consider net access as a basic human right
- The plan is to make internet as available as electricity
- Euro 384m project “EstWin” to provide 100 megabits / sec for every citizen by 2015

Stuxnet

Stuxnet's existence became known in June 2010

Target : Iran Nuclear Facility



HOW STUXNET WORKED



1. infection

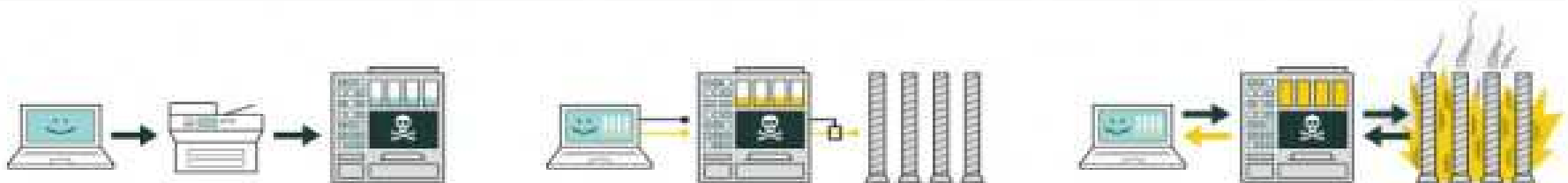
Stuxnet enters a system via a USB stick and proceeds to infect all machines running Microsoft Windows. By brandishing a digital certificate that seems to show that it comes from a reliable company, the worm is able to evade automated-detection systems.

2. search

Stuxnet then checks whether a given machine is part of the targeted industrial control system made by Siemens. Such systems are deployed in Iran to run high-speed centrifuges that help to enrich nuclear fuel.

3. update

If the system isn't a target, Stuxnet does nothing; if it is, the worm attempts to access the Internet and download a more recent version of itself.



4. compromise

The worm then compromises the target system's logic controllers, exploiting "zero day" vulnerabilities—software weaknesses that haven't been identified by security experts.

5. control

In the beginning, Stuxnet spies on the operations of the targeted system. Then it uses the information it has gathered to take control of the centrifuges, making them spin themselves to failure.

6. deceive and destroy

Meanwhile, it provides false feedback to outside controllers, ensuring that they won't know what's going wrong until it's too late to do anything about it.

Stuxnet worm and Flame malware represent “a spectacular failure for our company and the antivirus industry in general””

- Mikko Hyppönen, Chief Research Officer, F-Secure

Stuxnet Repercussion

Obama Order Sped Up Wave of Cyberattacks Against Iran

By
Pub

W
sec
sys
sig
cy

Print | Leaflet | Feedback | Share »

US Defense Secretary warns of “Pearl Harbor” cyber attack by Iran

By Niall Gre
15 October

In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back


Published: October 23, 2012 | 105 Comments


In a spee
Leon Pan
in the Mid
equivalen
bombardi


(Page 2 of 2)


After analyzing the software code from the Aramco attack, security experts say that the event involved a company insider, or insiders, with privileged access to Aramco’s network. The virus could have been carried on a USB memory stick that was inserted into a PC.

 FACEBOOK

 TWITTER

 GOOGLE+

 SAVE

 EMAIL

. Ba

A

Budgets

- Pentagon Five-Year Cybersecurity Plan Seeks \$23 Billion
- The Iranian government has reportedly invested \$ 1 billion to develop and build out its own cyberwar capabilities
- Estonia is the most cyberaware nation- provides free education to students in Cyber Security undergrad/post-grad programs + free net....

Now... Lets talk about ...

- What is war – then, now, ahead
- Cyberwar (what's that!), Estonia and Stuxnet – eye openers or game changers
- **India Under Attack & Preaparedness Scenario**
- Conclusions / The Bottom Line

India

- Budget == secret bad word
- Capability == Fragmented
- Capacity == Lots of noise
- Organization == chaotic
- Future Plan == Future! Duh! It's top secret
- Core Cybersecurity Strategy == knee jerks based on ignorance or pompousness

Our Strengths (official stand)

- IT Act and various amendments
- National Cyber Security Policy
- Crisis Management Plan
- CERT, NTRO and 60+ organizations and agencies
- Oversight thru' Clause 49, UID, NPR,

Reality Check

- IT Act and various amendments
- National Cyber Security Policy
- Crisis Management Plan
- National Critical Infrastructure Policy
- RBI, SEBI, TRAI/DOT and other regulations

Reality Check

- Multiple data breaches at PMO, MEA among other agencies over the years
- Use of free email services despite revelations of NSA's Prism program
- Knee jerk directive against use of public emails in the absence of ANY alternative (Brazil Post has set up free email services)

Reality Check

- UID weaknesses and NPR
- CCTNS
- Non starter
- CERT, NTRO and 60+ organizations and agencies – Fragmented, internal politics, progress is (not) shared

A Small Digression

Prompted by the last point about
60+ organizations / agencies
operating in the country

Organization Soup



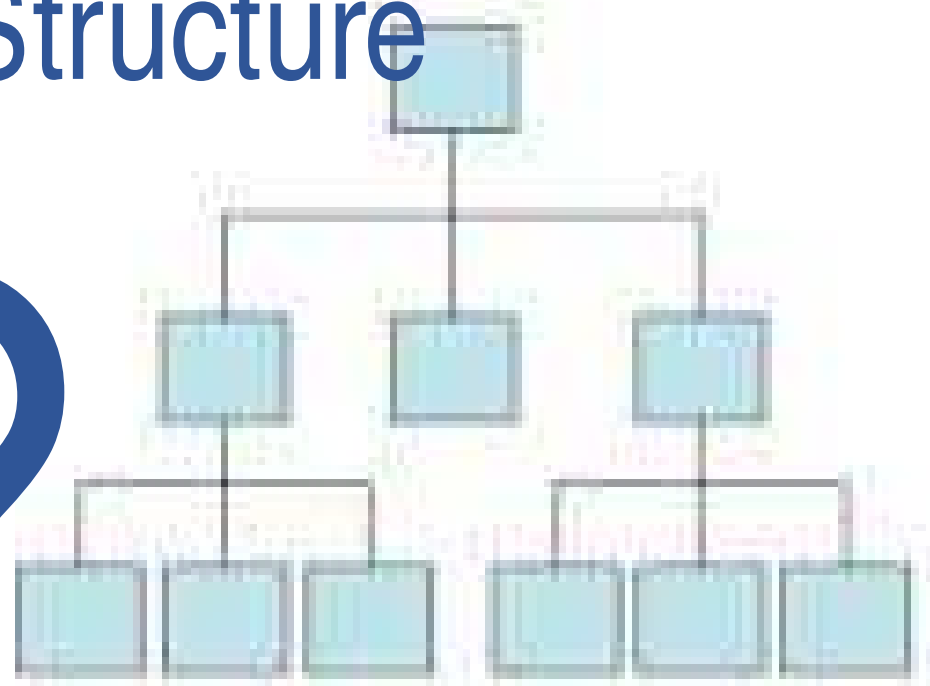
WESEE	General Weapons and Electronics Systems Engineering Establishment
DIARA	Defense Information and Research Agency
DIA	Defence Intelligence Agency
	Special Operations Command
	Strategic Forces Command
	CERT-Navy
	CERT-Army
	CERT-AirForce
	Cyber Operations Centre (NTRO with Armed Forces)

CERT-In	Computer Emergency Response Team
CHCIT	Cyber and Hi-Tech Crime Investigation and Training Center
NIC	National Informatics Center
NTRO	National Technical Research Organization
	Cyber Regulation Advisory Committee
NCSC	National Cyber Security Commissioner
	Cyber Coordination Center
CMS	Central Monitoring System
NCSF	National Cyber Security Framework
	Cyber Security Board
	Cyber Security Board - Cyber Security Coordinators
NCCC	National Cyber Coordination Centre
NSCS	National Security Council Secretariat
NCCC	National Cyber Coordination Centre
NSAB	National Security Advisory Board
	National Information Security Authority
NCIIPC	National Critical Information Infrastructure Protection Committee

What Org Structure



What We Have



What We Need

Organization Soup



CDRC	Cyber Defence Research Centre, Jharkhand
	Cyber Suraksha Cell, Gujarat
	Special Operations Group, Gujarat
	Cyberdome, Kerala Police
DSCI	Data Security Council of India
IISc	Indian Institute of Science, Bangalore
ISAC	Information Sharing and Analysis Centre
CSI	Computer Society of India
	Deccan Hackers
	Indian Cyber Army
	National Security Database
IDRBT	Institute for Development and Research in Banking Technology
IBA	Indian Banks Association
RBI	Reserve Bank of India
	CBI's Bank Securities and Fraud Cell

	National Intelligence Board
SSTCG	Strategic Security Technology Coordination Group
MAC	Multi Agency Centre
	Joint Cipher Bureau
	Scientific Advisory Group
	Indian Statistical Institute
	Cipher Committee
	Scientific Advisor to Raksha Mantri
	Telecom Security Council of India
NATGRID	National Intelligence Grid
CCTNS	Crimes and Criminal Tracking Network and System
NCTC	NCTC was to weld together multiple intelligence databases:
NJDG	National Judicial Data Grid
TETC	Telecom Testing and Security Certification Centre
TRAI	
DOT	

Our Score = 60+

- The country should have been on the top of the Cyber capability index worldwide
- We would not having this conference.. Rather ... the topic would have been different
- Nations and individuals would have to think twice to face up to us – no website defacements or data breach

What We Have

- To respond to an attack by air the Air Force is called, on land it is the Army and the Navy at sea

Who do we call upon for an attack through the internet



- How do 60+ agencies coordinate with each other
- How can a planned response be launched in the absence of a central coordinator....



“The good news”

**Worldwide – other
countries are no better**



"SECURE THE BUILDING"

THE ARMY WILL POST GUARDS AROUND THE PLACE.
THE NAVY WILL TURN OUT THE LIGHTS AND LOCK THE DOORS.
THE MARINES WILL KILL EVERYBODY INSIDE AND SET UP A
HEADQUARTERS.
THE AIR FORCE WILL TAKE OUT A FIVE-YEAR LEASE WITH AN
OPTION TO BUY.

OK... We Return to Our
Presentation

Reality Check

- R&D and PPP are good terms used in policies and meetings
- Advisories (invariably) speak a foreign language
- Lack of statistics or authentic surveys so anyone says anything

Now... Lets talk about ...

- What is war – then, now, ahead
- Cyberwar (what's that!), Estonia and Stuxnet – eye openers or game changers
- India Under Attack & Preparedness Scenario
- **Conclusions / The Bottom Line**

Are we ready for cyberwar?

CERTAINLY NOT!

THE BOTTOM LINE

WHY NOT!

You May Ask

Where are the policies and strategies which will guide our nation in the event of a cyberwar?

What is our budget allocation?

Who is spending money wisely?

Where is the money being spent?

Have you seen one (critical) PSU with genuinely good practices which are adopted by the organization?

THE BOTTOM LINE

WHAT CAN WE DO

Speak to the people we know in Government and get them scared

Kick the people who say they have the best systems in place (be careful you do not kick the wrong one)

Understand and accept that risks and threats from technology are part of life and we have to change

Contribute our effort strongly to making things better in our own small way

THE BOTTOM LINE

Al Qaeda's own "country" for 2013: Northern Mali



Fighters from Islamist group Ansar Dine stand guard during a hostage handover in the desert outside Timbuktu, Mali, on April 24, 2012. / AP PHOTO/FILE

4 Comments / Shares / Tweets / Stumble / Email More +

MOPTI, MALI | Deep inside caves, in remote desert bases, in the escarpments and cliff faces of northern Mali, Islamic fighters are burrowing into the earth, erecting a formidable set of defenses to protect what has essentially become al Qaeda's new country.

They have used the bulldozers, earth movers and Caterpillar machines left behind

Leaving
you with
some
food for
thought

European Parliament switches off Wi-Fi after hacker breaks into politicians' emails

BY ROB VAUGHN POSTED 27 NOV 2013 AT 10:21AM

CYBERCRIME 0 TAGS WI-FI



The European Parliament has switched off its public Wi-Fi system after an anonymous hacker broke into the personal emails of several Members of the European Parliament (MEPs) from outside the building, using only a laptop.

French news outlet [Mediapart](#) quotes the anonymous hacker as saying, "it was child's play," and that his attack required only "a few bits of knowledge that everyone is capable of finding on the internet." The attacker was also able to access email accounts owned by IT staff.

Follow Us



Automatically receive new posts via email:

Type your email address

FeedBurner

Leaving
you with
some
food for
thought

HOT TOPIC

BANKING MALWARE



18 OCT 2013

17 New IBM system adds "robust" security to smartphone banking and shopping

15 OCT 2013

16 Stop, thief! Five new tricks used by cybercriminals - and how to stay safe

20 SEP 2013

15 Can't keep a bad man down: "Shylock" Trojan returns to attack U.S. banks

Cyberwar is a chimera, a figment of imagination which is yet to be defined and we have to be careful of watmongers and sabre rattlers!

The need is to secure our infrastructure which is where all attention must be focussed

Leaving you with some food for thought

Thank You

Head Office:

FB-05, NSIC Software Technology Park Extn,
Okhla Industrial Estate,
New Delhi-110020,
T: +91-9650894671
F: +91-11-26322980
E: contact@pyramidcyber.com

Mumbai Office:

308 Orbitz Premises
Chincholi Bunder Road
Malad West
Mumbai 400064

T: +91.9769890505

E: dinesh.bareja@pyramidcyber.com



Pyramid
www.pyramidcyber.com

Dinesh O. Bareja,

CISA, CISM, ITIL, BS7799, Cert IPR, Cert ERM



- Professional Positions

- Pyramid Cyber Security & Forensics (Principal Advisor)
- Open Security Alliance (Principal and CEO)
- Jharkhand Police (Cyber Security Advisor)
- Indian HoneyNet Project (Co Founder)

- Professional skills and special interest areas

- Security Consulting and Advisory services for IS Architecture, Analysis, Optimization..
- Technologies: SOC, DLP, IRM, SIEM...
- Practices: Incident Response, SAM, Forensics, Regulatory guidance..
- Community: mentoring, training, citizen outreach, India research..
- Opinioned Blogger, occasional columnist, wannabe photographer

Contact Information



dinesh@opensecurityalliance.org



@bizsprite



<http://in.linkedin.com/in/dineshbareja>



+91.9769890505



dineshobareja



dineshobareja

References

<http://socialmediastrategiessummit.com/blog/relevance-strategic-inflection/>

Acknowledgements & Disclaimer

Various resources on the internet have been referred to contribute to the information presented. Images have been acknowledged (above) where possible. Any company names, brand names, trade marks are mentioned only to facilitate understanding of the message being communicated - no claim is made to establish any sort of relation (exclusive or otherwise) by the author(s), unless otherwise mentioned. Apologies for any infraction, as this would be wholly unintentional, and objections may please be communicated to us for remediation of the erroneous action(s).

Thank
You