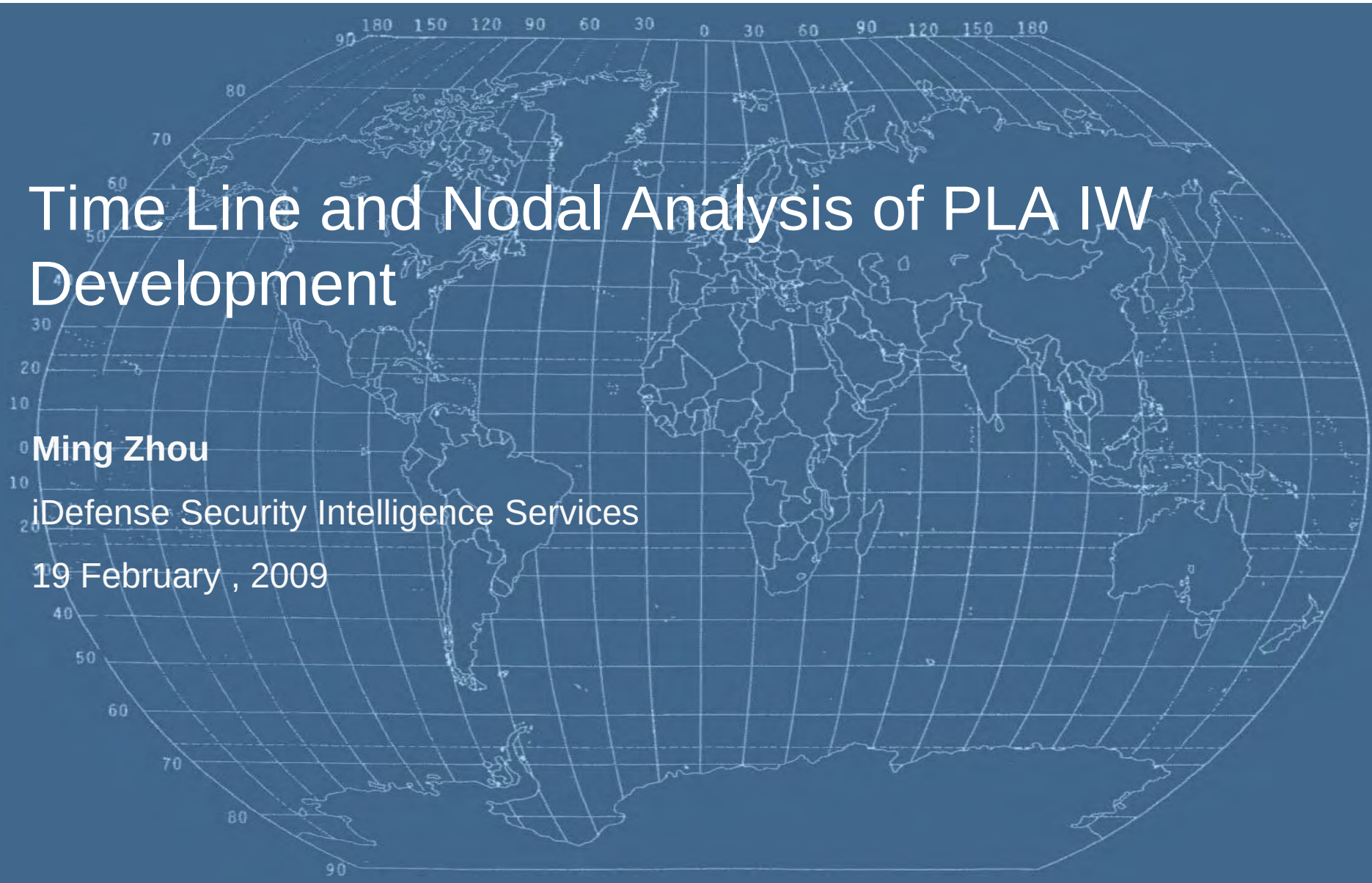
iDEFENSE
Actionable Threat Intelligence



Time Line and Nodal Analysis of PLA IW Development

Ming Zhou

iDefense Security Intelligence Services

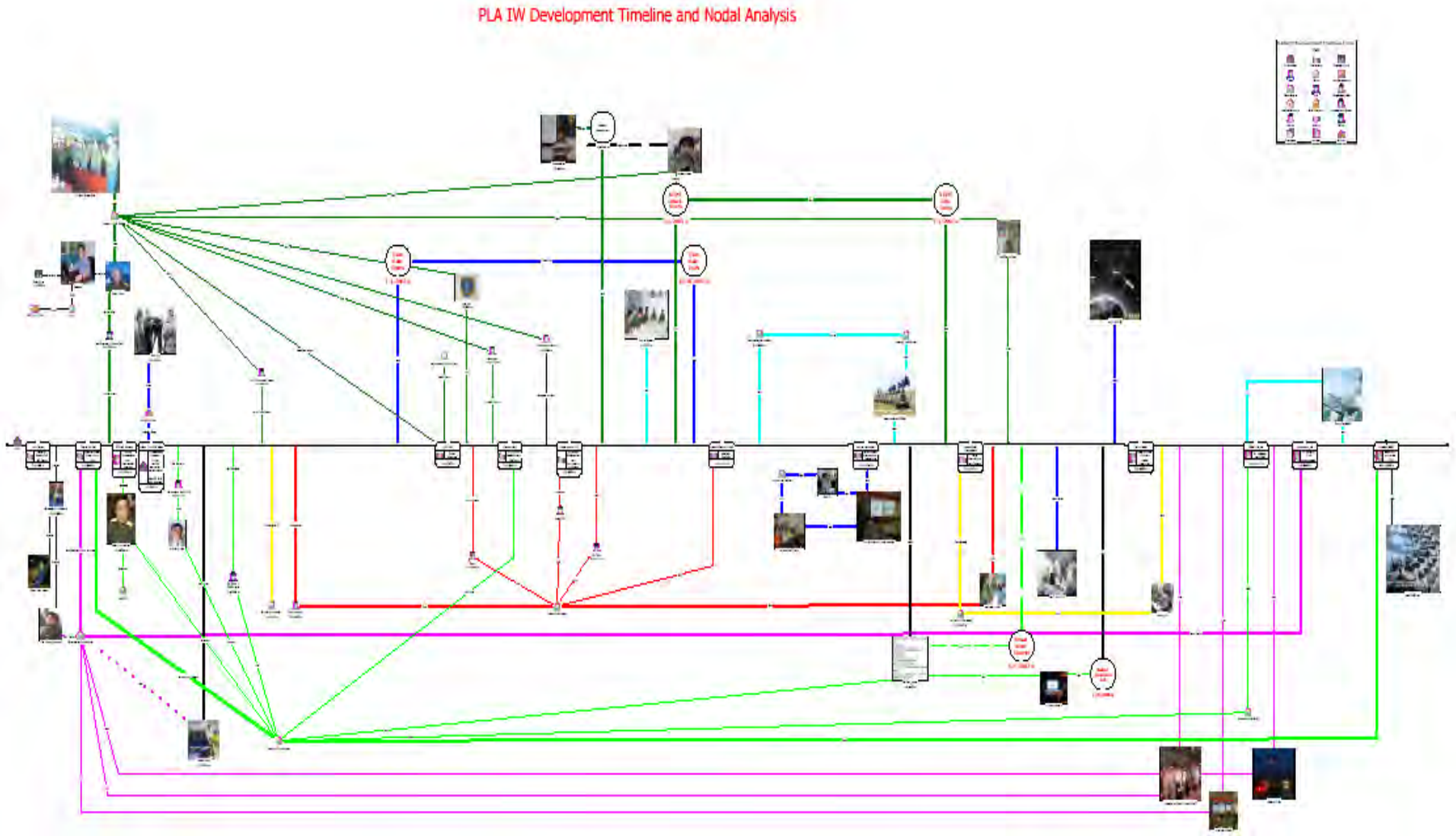
19 February , 2009

Agenda

+ What Have Western Seen?
+ iDefense Research Methodology
+ PLA IW Timeline
+ Deduction and Facts
+ My One Step Leap

iDEFENSE
Actionable Threat Intelligence

Time Line



iDEFENSE
Actionable Threat Intelligence

What Western Have Seen

+ Titan Rain
+ Western governments accusation
+ Sandia National Laboratories
+ Congress Offices
+ DoD Contractors
+ Pentagon
+ Navy
+ NASA
+ Indian Government

iDEFENSE Actionable Threat Intelligence

By Default

+ **PLA!**
+ **PLA?**
+ **PLA {x,y,z…}**
+ **State Sponsor!**
+ **State Sponsor?**
+ **State Sponsor {a,b,c…}**
+ **Gaps...**

iDEFENSE
Actionable Threat Intelligence

Can He Fit the Profile?





iDEFENSE
Actionable Threat Intelligence

Questions before starting

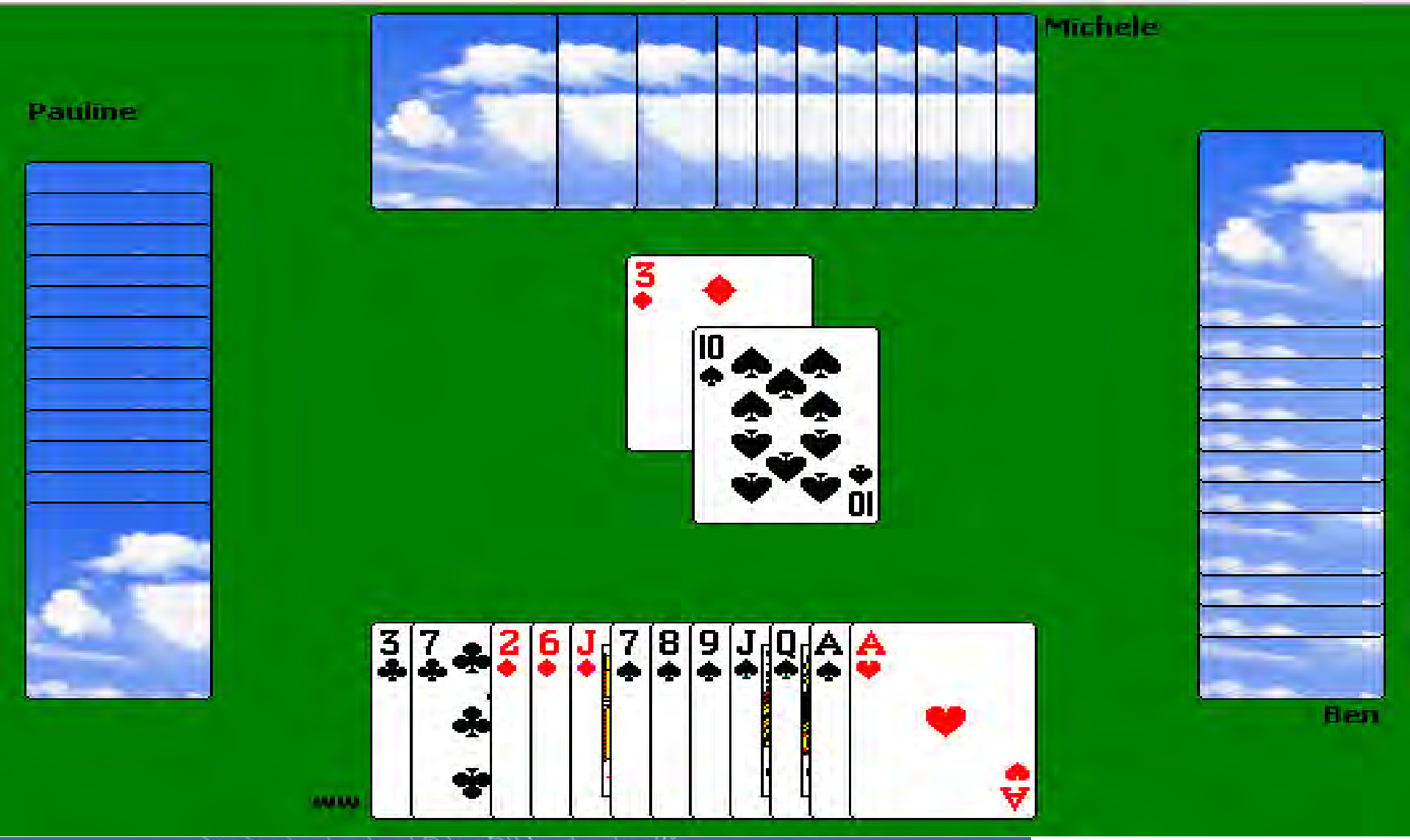
+ Under order?
+ Just for Fun?
+ A Soldier with uniform
+ A Soldier without uniform
+ Several Soldiers with uniform
+ Several Soldiers without uniform

+ **PATRIOTISM , PROPAGANDA**

ACQUIESCENCE

iDEFENSE
Actionable Threat Intelligence

Asymmetric war -Card game



iDEFENSE
Actionable Threat Intelligence

River Rock to New York City



iDEFENSE
Actionable Threat Intelligence

Spot of Cheetah



iDEFENSE
Actionable Threat Intelligence

Methodology

+ Micro to Macro, Macro to Micro,
+ Methodology {Identify, Verify, Validate, Organize}
+ Consistency
+ Continuity
+ Tangible Entities
+ Undeniable published news
+ Cross references

+AND

iDEFENSE Actionable Threat Intelligence

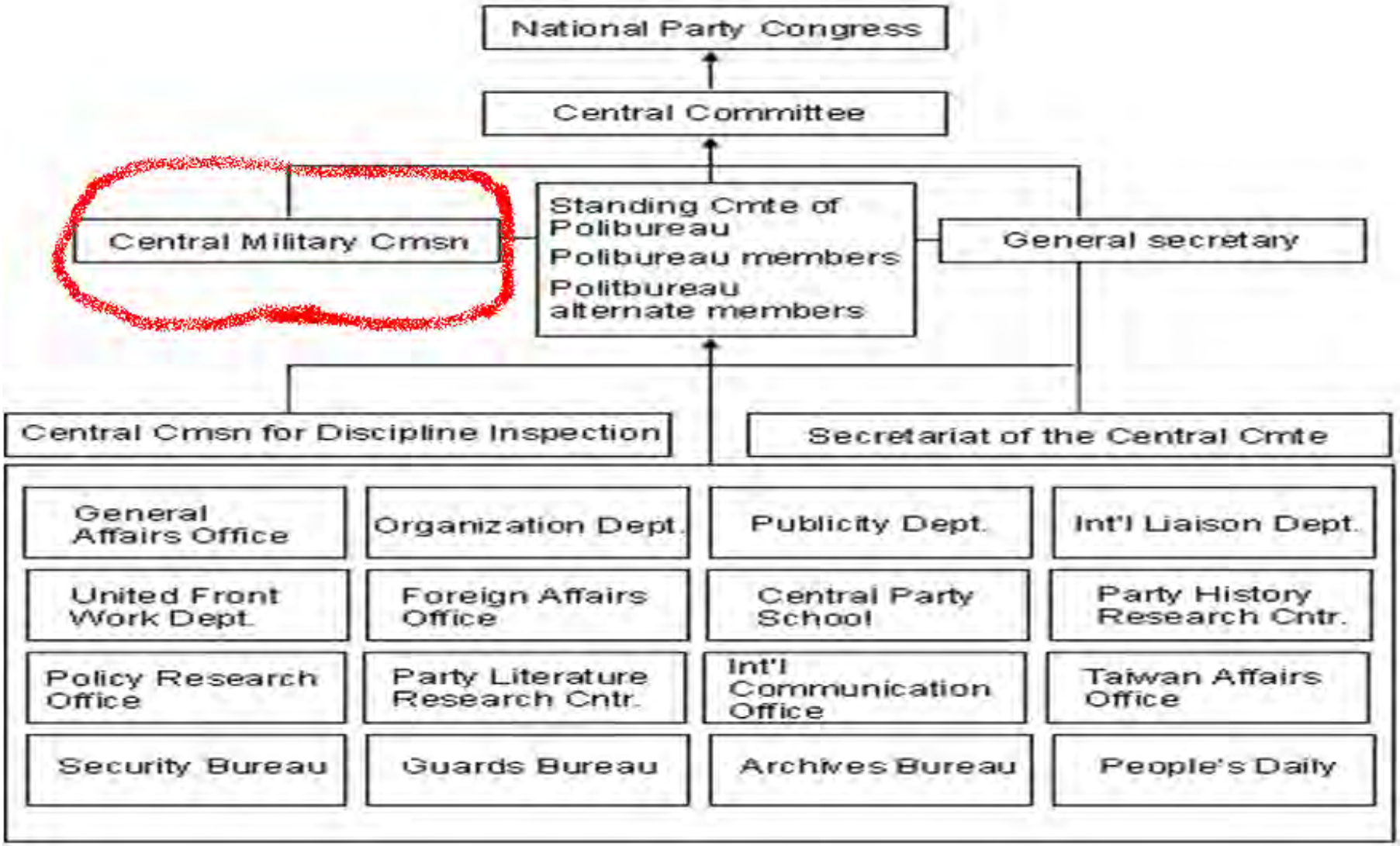
Rules

+ Time
+ Location
+ Unit Code
+ Leader's Name
+ Order Number
+ Designated Function
+ Machine Learning { x, y, z…}

+ OR

iDEFENSE Actionable Threat Intelligence

Hierarchy



iDEFENSE
Actionable Threat Intelligence

Sub Sets

- CMC
  - **General Staff Department (GSD)**
  - **General Political (GPD) Department**
  - **General Logistics Department (GLD)**
  - **General Armament Department (GAD)**
- The GSD is responsible for organizing, leading, and commanding military actions. It is made up of departments for war operations, information, communication, military training, army affairs, mobilization, armament, security, mapping and surveying, foreign affairs, as well as the affairs of the various armed services and arms.

iDEFENSE Actionable Threat Intelligence

PLA Force Structure

- 7 regions (NE, NW, Beijing, E, Nanjing, SE, SW)
- Air force
- Navy
- 2nd Artillery
- Ground Force
  - Active 500,000
  - Armed Police Force 1,500,000
  - Militia 1,000,000

iDEFENSE Actionable Threat Intelligence

Recursively Break down

+ Chinese People's Armed Police Forces (APF) and the Militia.
  - The Militia is a force engaged in continuous preparation and support activities under the leadership of the Party of China
  - It is a component part of the armed forces. Under the command of active military units.
+ A hierarchical subordination relationship is clear. APF is under the direction of the PLA
  - CMC publishes national policy regarding militia management and provides overall guidance;
  - GSD provides management ,
  - PLA regional commanders execute down to the city level through the local APF authorities.
  - The GSD publishes annual training tasks
  - The regional PLA garrisons execute the tasks
  - APF provides the operation units. Equipment and training facilities are supported by different levels of authority.

iDEFENSE Actionable Threat Intelligence

Time Line 1

+ 07/1997, The first PLA Division Chief of Staff training forum, dedicated to studying the Kosovo War.
+ 01/1998, First official net militia unit, 40 professionals
+ 02/1999, Unrestricted Warfare
+ 06/1999, Military started to use HLLP.YAI.
+ 01/2000, Join forces Taiwan War Drill.
+ 12/2000, Gen Xu, GSD promotion.







iDEFENSE
Actionable Threat Intelligence

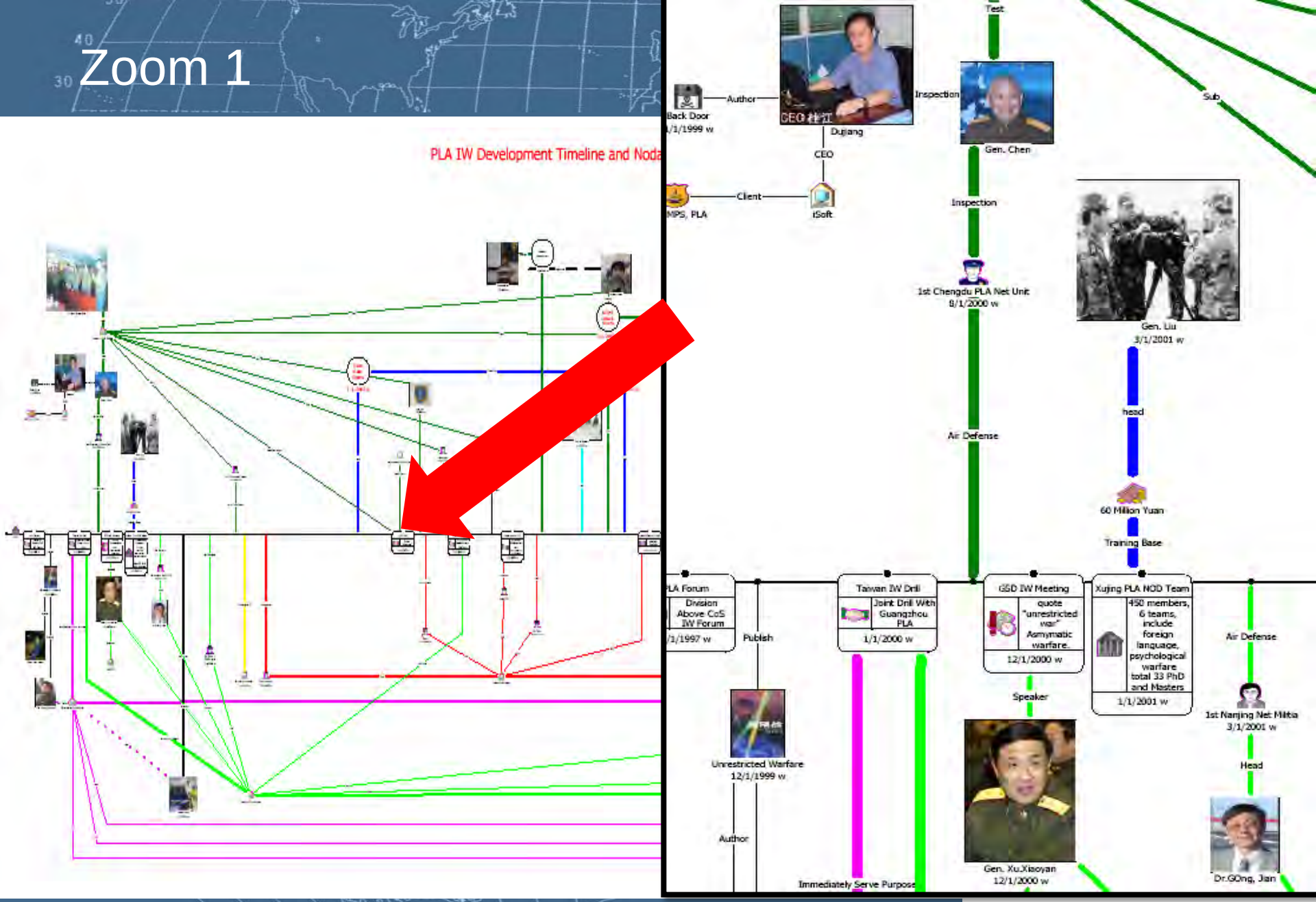
Timeline 2

- 08/2000, First real drill and deployed “Militia Special Net War Training System” for air defense
- 01/2001, Xujing Garrison Training base for 60 Million Yuan
- 03/2001, Air Defense Emergency Alternate Plans, 63 Masters and Professors
- 01/2002, Chongqing and Tianjin exchange and study air defense
- 03/2002, PLA 73685 Unit tests for air defense master switch.
- 05/2002, SW 24/7, 30 minutes response unit
- 05/2002, PLA Gens. Inspect labs.
- 05/2002, Civilian instructors and Trojan “Glacier “



iDEFENSE Actionable Threat Intelligence

Zoom 1



iDEFENSE
Actionable Threat Intelligence

Net Militia Units





iDEFENSE
Actionable Threat Intelligence

Identity





iDEFENSE
Actionable Threat Intelligence

Timeline 3

+ 01/2003, Nanjing PLA outsourcing to University as war time commanding center
+ 04/2003, Senior Net Militia back to mother University to train junior Net Militias.
+ 07/2003, State Own Enterprises as war time commanding centers





iDEFENSE
Actionable Threat Intelligence

Timeline 4

+ 11/2003, PLA Regions new equipments test
+ 12/2003, “Frontier Guard 230” Joint operation for air defense
+ 01/2004, New space surveillance and radar system
+ 03/2004, 9th Order of 2002 and 2003’s 231st document
+ 05/2004, SW Air Defense Officer Institute.
+ 11/2004, Special recruiting in Guangzhou PLA
+ 11/2004, Performance review and appraisal.
+ 12/2004, Training and drill integrate to real war track



iDEFENSE
Actionable Threat Intelligence

Little Stop

+ Air Defense 7 times
+ Directly related 2 times



iDEFENSE
Actionable Threat Intelligence

Timeline 5

+ 04/2005, A large scale emergency order to form Net Militia Units.
+ 04/2005, Multiple Intelligence Units
+ 05/2005, PLA and PAF Universities recruiting
+ 11/2005, National Emergency Drill Structure
+ 05/2006, Air defense drills and exchange
+ 05/2006, NCPH GinWui Rootkit.

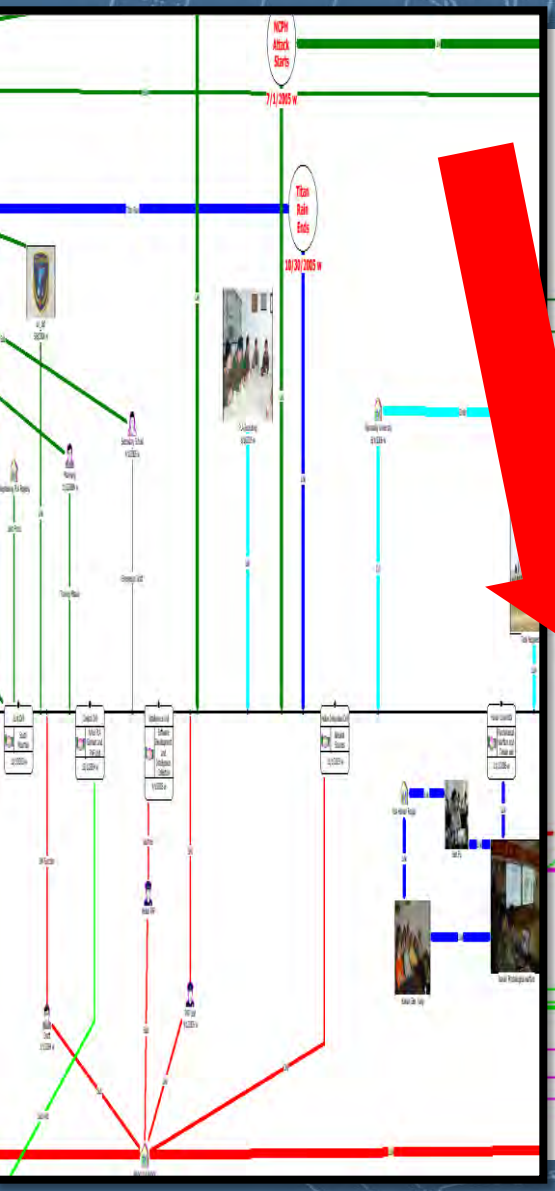


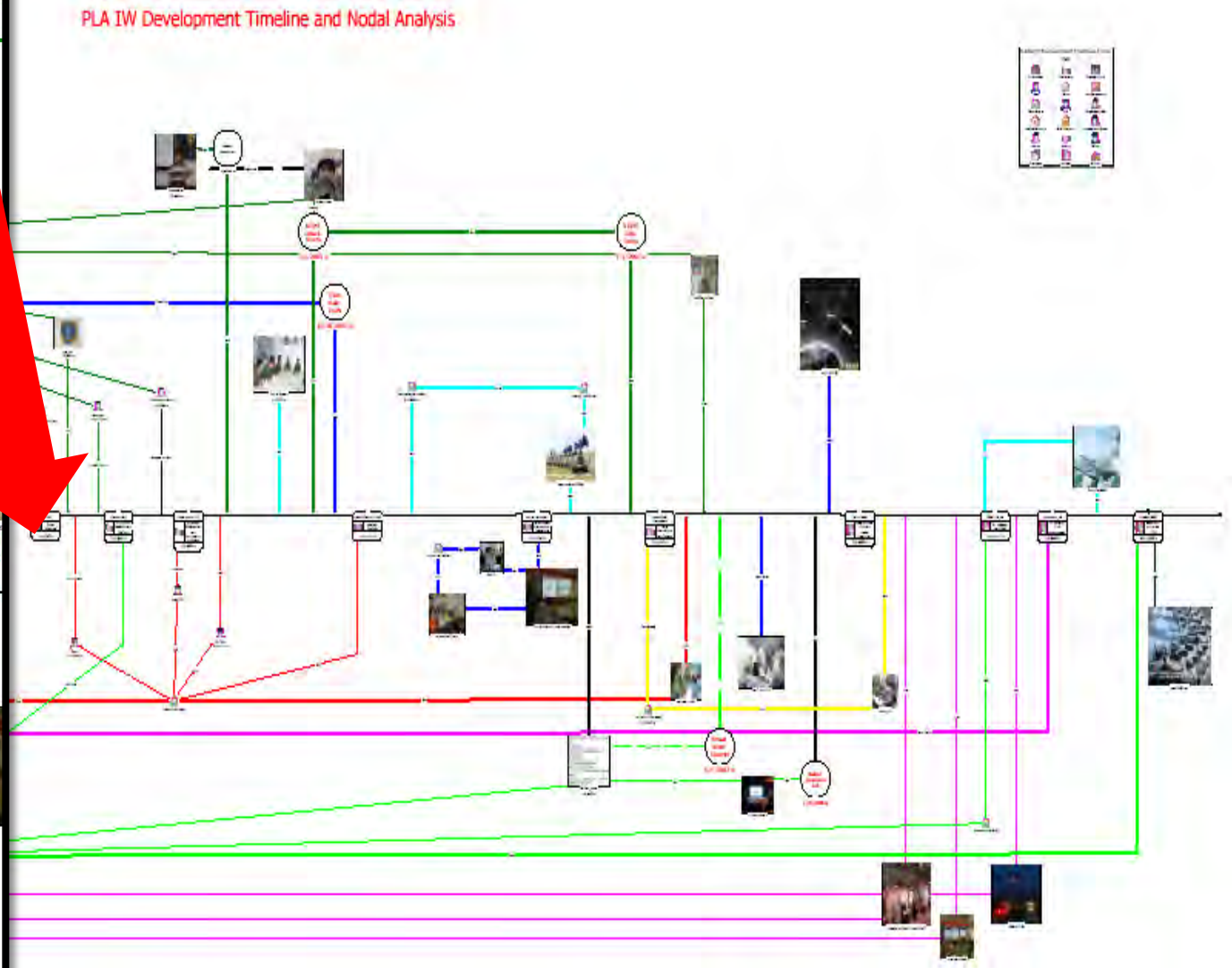




iDEFENSE
Actionable Threat Intelligence

Zoom





iDEFENSE
Actionable Threat Intelligence

Timeline 6

- 11/2006, Large scale online Psychological warfare against Taiwan
- 05/2007, Shanghai in the air defense game
- 07/2007, Wuhan in the air defense game
- 07/2007, Guangzhou PLA set “100 mile off shore”
- 08/2007, Electromagnetic protection solution
- 11/2007, Bring in Complicate Electromagnetic Environment concept





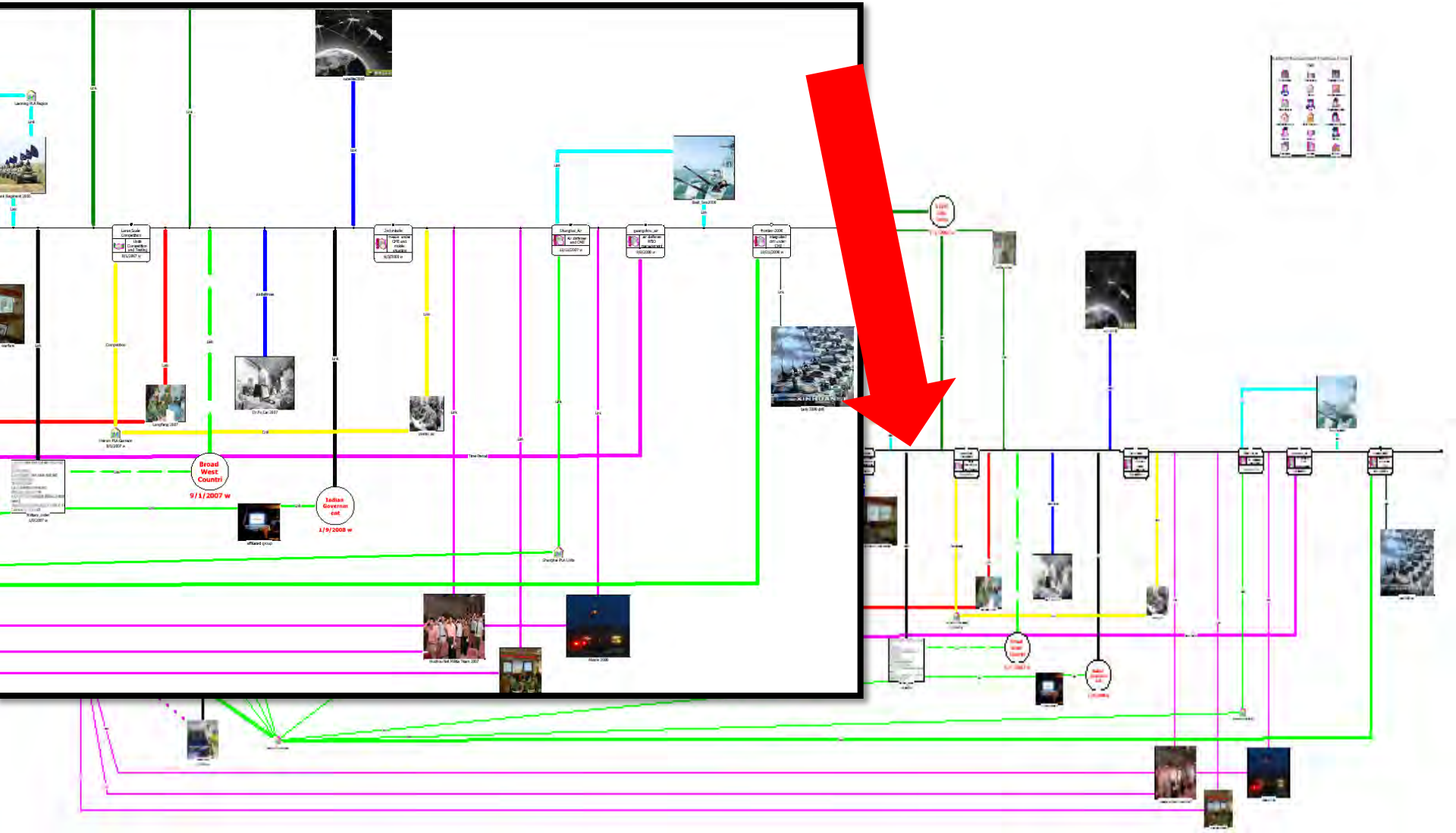
iDEFENSE
Actionable Threat Intelligence

Timeline 7

- 09/2007, Tank Regiment 1000 Mile maneuver CEE Drill
- 12/2007, Purchase “Helicopter” related Information
- 01/2008, PLA Shenyang Drill for Trojans to change logistic requirements and data to cause confusion. Then EMP destroyed motherboard wireless function modules, landlines and finally radio stations.
- 09/2008, Guangzhou Deployed KS-1 Missile with Net Militia Units.
- 09/2008, 2nd Artillery, the largest drill in history and new standards
- 10/2008, 35 satellites cover surrounding
- 10/2008, Tank Regiment “Front Line 2008” live ammunition CEE Drill
- 01/2009. East Sea Fleet drill CEE

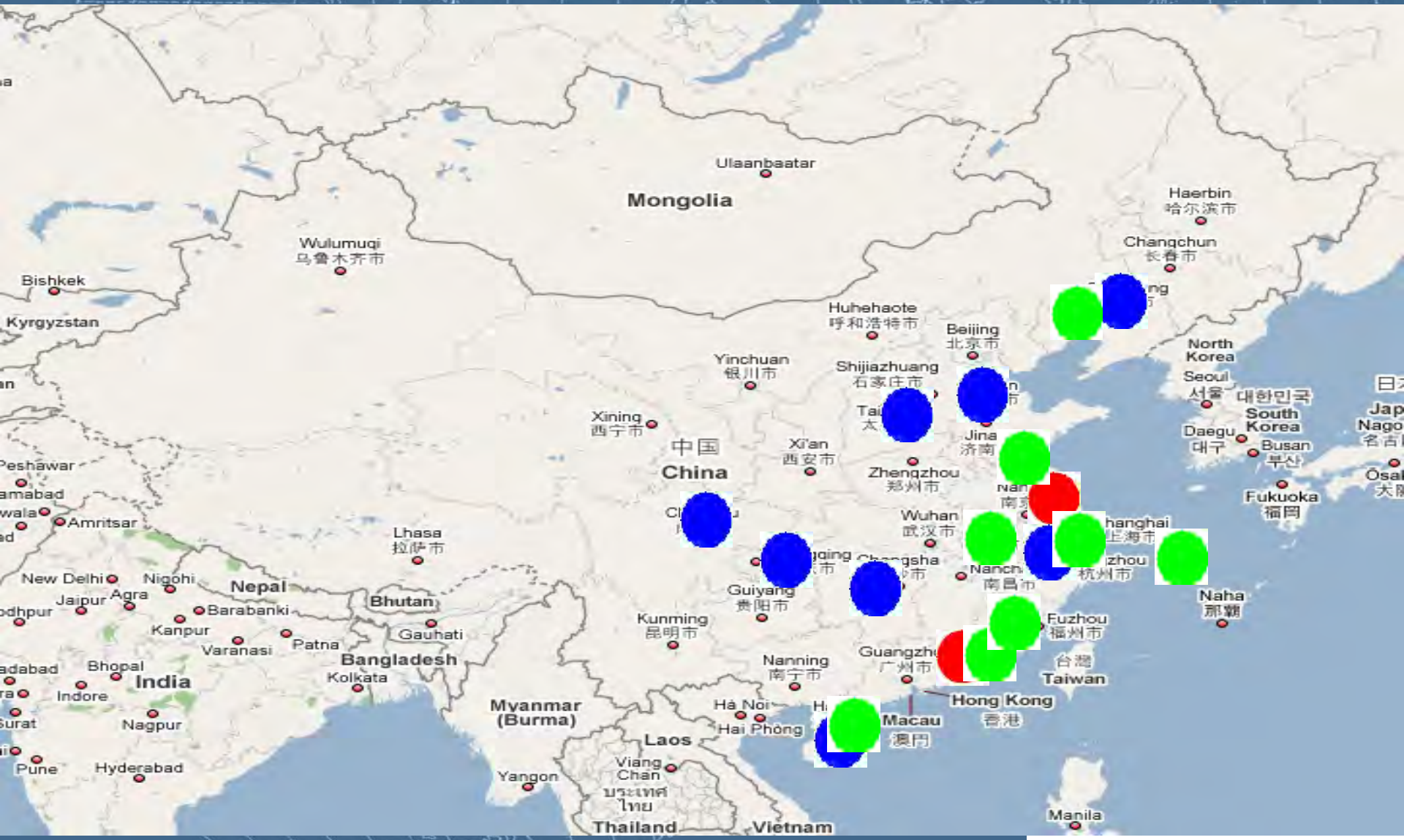
iDEFENSE Actionable Threat Intelligence

Zoom 2



iDEFENSE
Actionable Threat Intelligence

Activities Stage Map



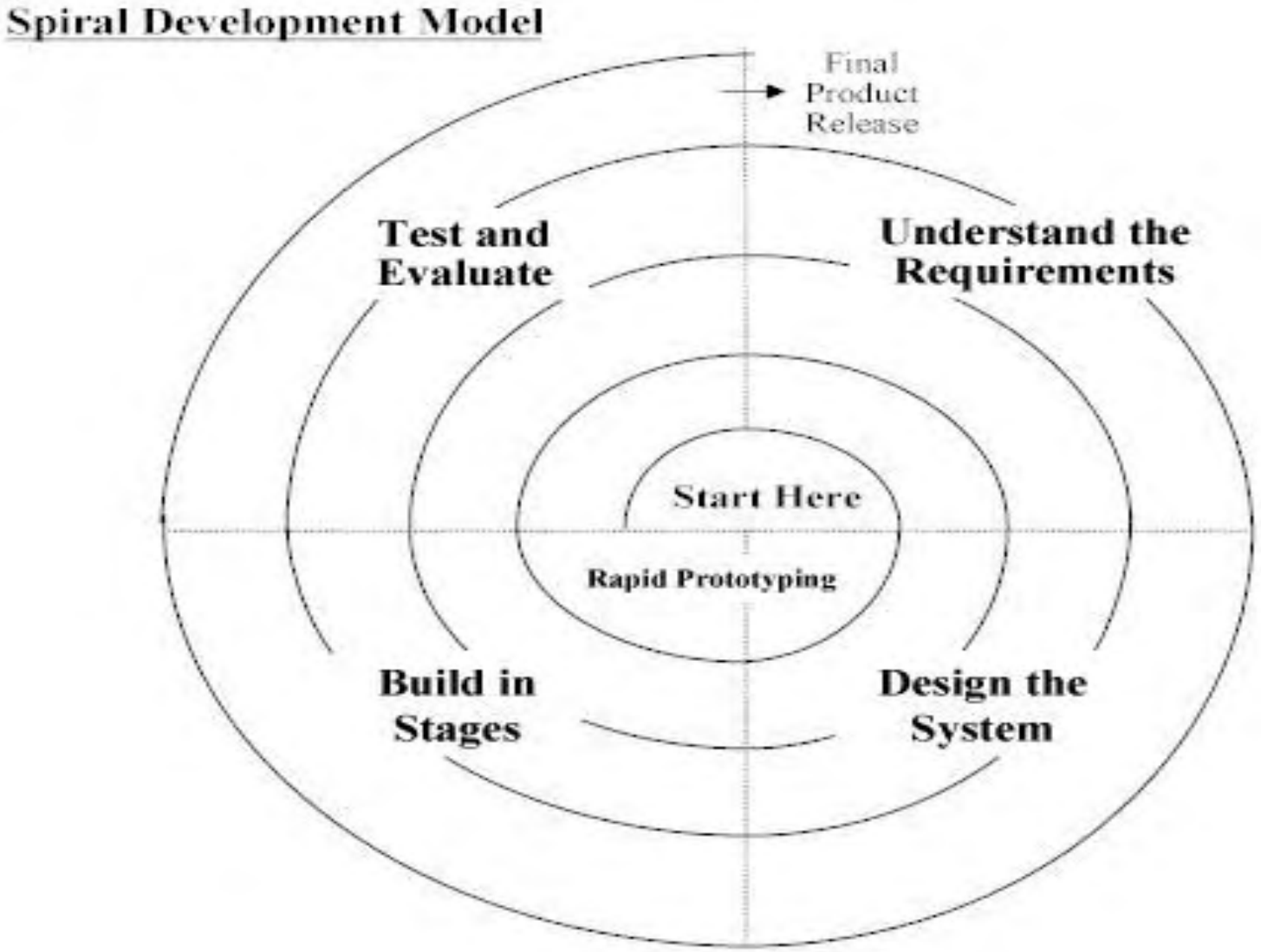
iDEFENSE
Actionable Threat Intelligence

Product development Stages

+ Strategic Planning → Time Line1
+ Research → Time Line 2
+ Product Define→ Time Line 3
+ Project management → Time Line 4
+ Industrialization → Time Line 5
+ Implementation → Time Line 6
+ Dissemination → Time Line 7
+ New Circle of Preparation for CEE

iDEFENSE Actionable Threat Intelligence

Different stages



iDEFENSE
Actionable Threat Intelligence

Spiral Model

+ Quick Prototype →Taiwan
+ Requirements → Stage 2
+ Design the System→ Stage 3
+ Build in → Stage 4,5
+ Test → Stage 6,7
+ Release →Back to the initial focus



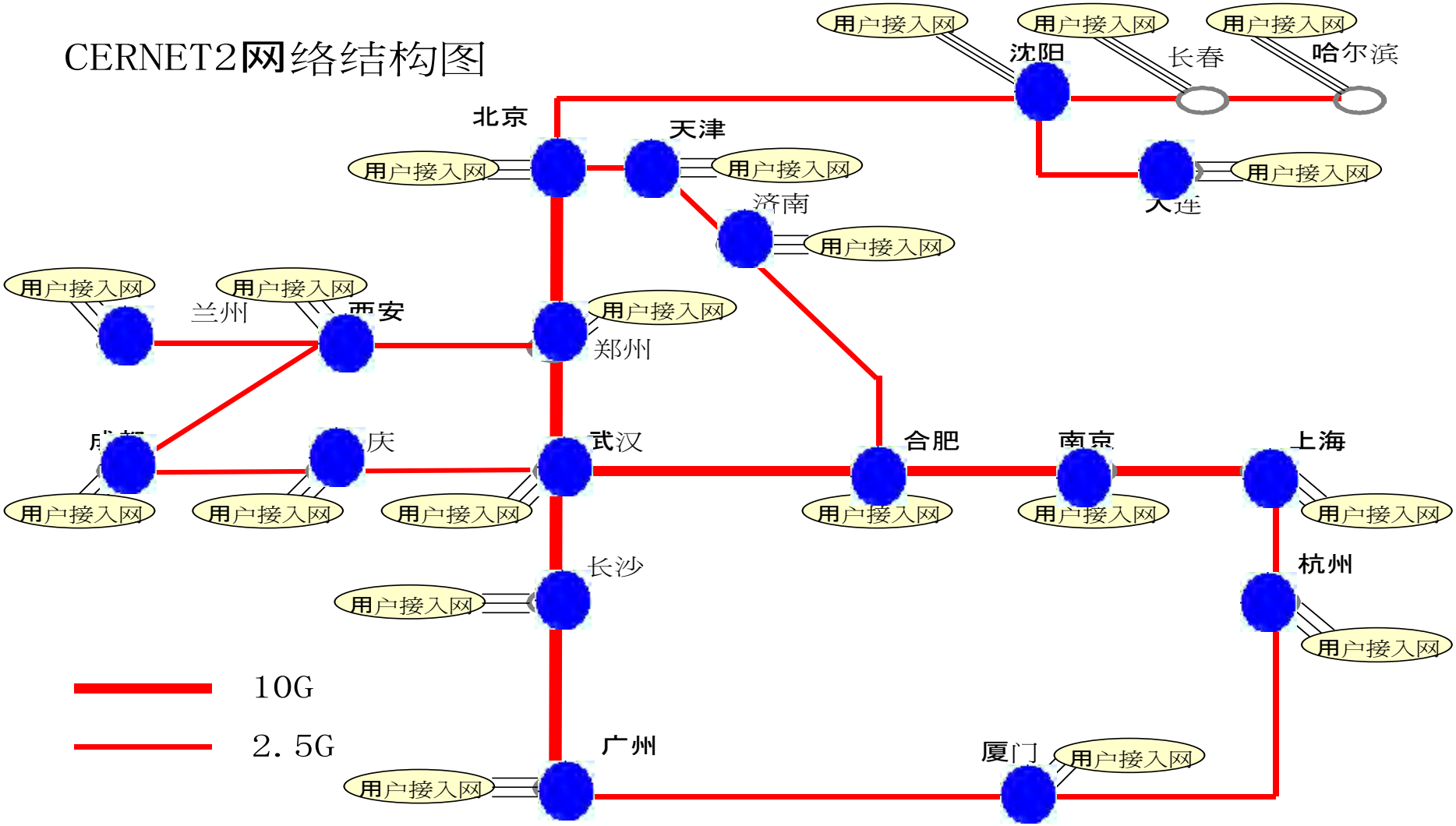
iDEFENSE
Actionable Threat Intelligence

Facts List

+ PLA is guiding and tasking Net Militia Units and civilian companies.
+ PLA has developed large scale national cyber emergency drill
+ All activities are based on physical infrastructure…CERNET.
+ PLA IW focus was air defense, recently shift to Operate under CEE
+ From inland to coast line
+ From person to business to national level structure
+ From civilian research to official order
+ From land to ocean to space
+ From virtual to tank to missile
+ **Taiwan was the initial issue, is and still will be**
+ **PLA IW module is complete.**

iDEFENSE Actionable Threat Intelligence

Operate on CERNET



iDEFENSE Actionable Threat Intelligence

Taiwan War Map-Head Off Operation



iDEFENSE
Actionable Threat Intelligence

Followings are just my OWN observations

+ 90 % information from OSINT
+ 10% Reliable sources
+ Remember : Investigator + AI Robot Thinking + Tank Sable Penetration+ Disney kitchen man

+ Takes Passion, Domain Expertise, Neutral Thinking, Efforts and Time to Digest

iDEFENSE Actionable Threat Intelligence

107 mm Rocket



iDEFENSE
Actionable Threat Intelligence

Simulation



iDEFENSE
Actionable Threat Intelligence

Diesel AIP



Chinese Defence Today (www.sinodefence.com)

iDEFENSE
Actionable Threat Intelligence

300 km Anti-Ship Missile



iDEFENSE
Actionable Threat Intelligence

South Sea Fleet is Preparing for “After Nuke”



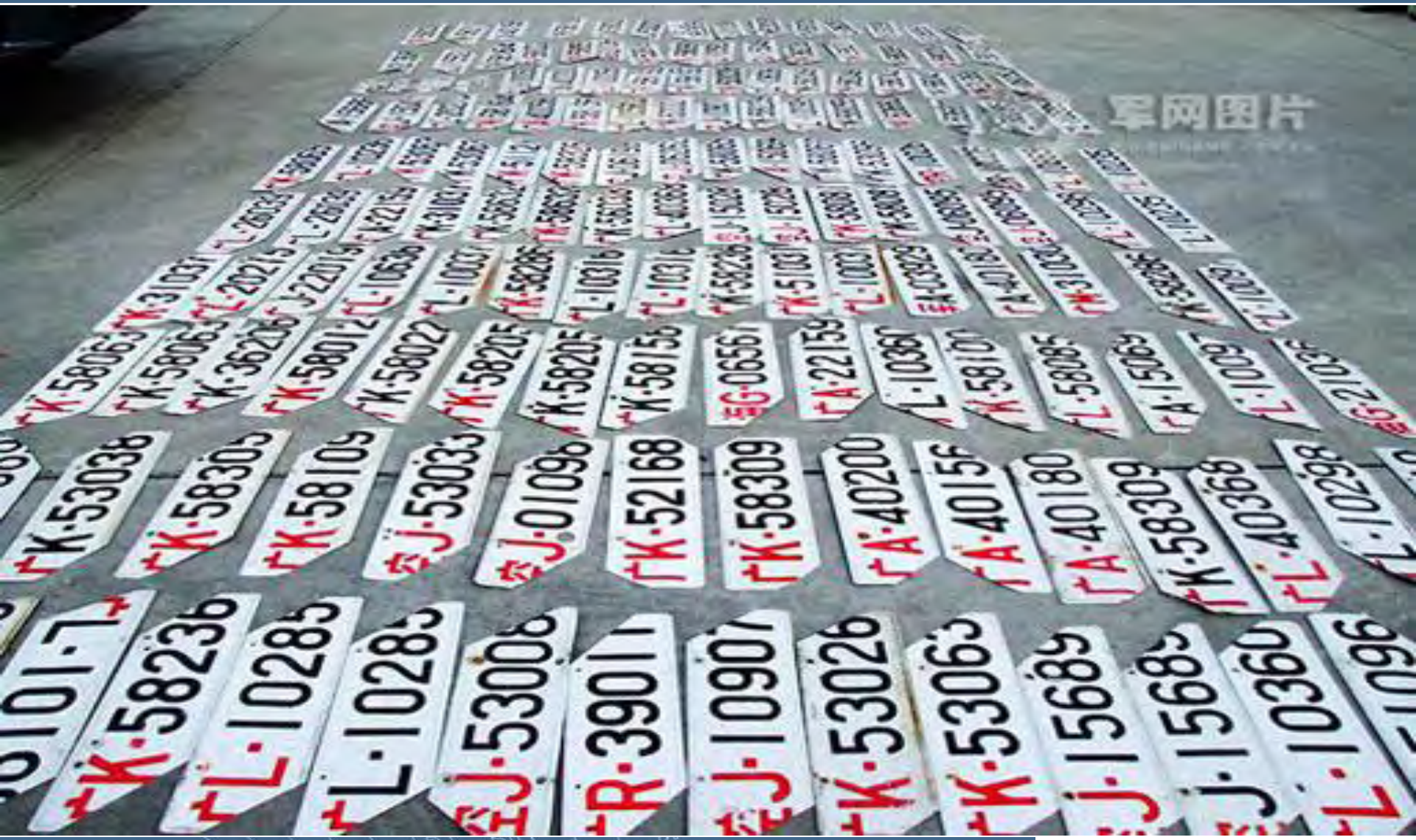
iDEFENSE
Actionable Threat Intelligence

South Sea and Deep Inland Combined Drill



iDEFENSE
Actionable Threat Intelligence

Guangxi and Guangzhou Logistic Support Chain



iDEFENSE
Actionable Threat Intelligence

WiMax On the Top of Everest



iDEFENSE
Actionable Threat Intelligence

Xiao Tian



iDEFENSE
Actionable Threat Intelligence

2010, 35 satellites



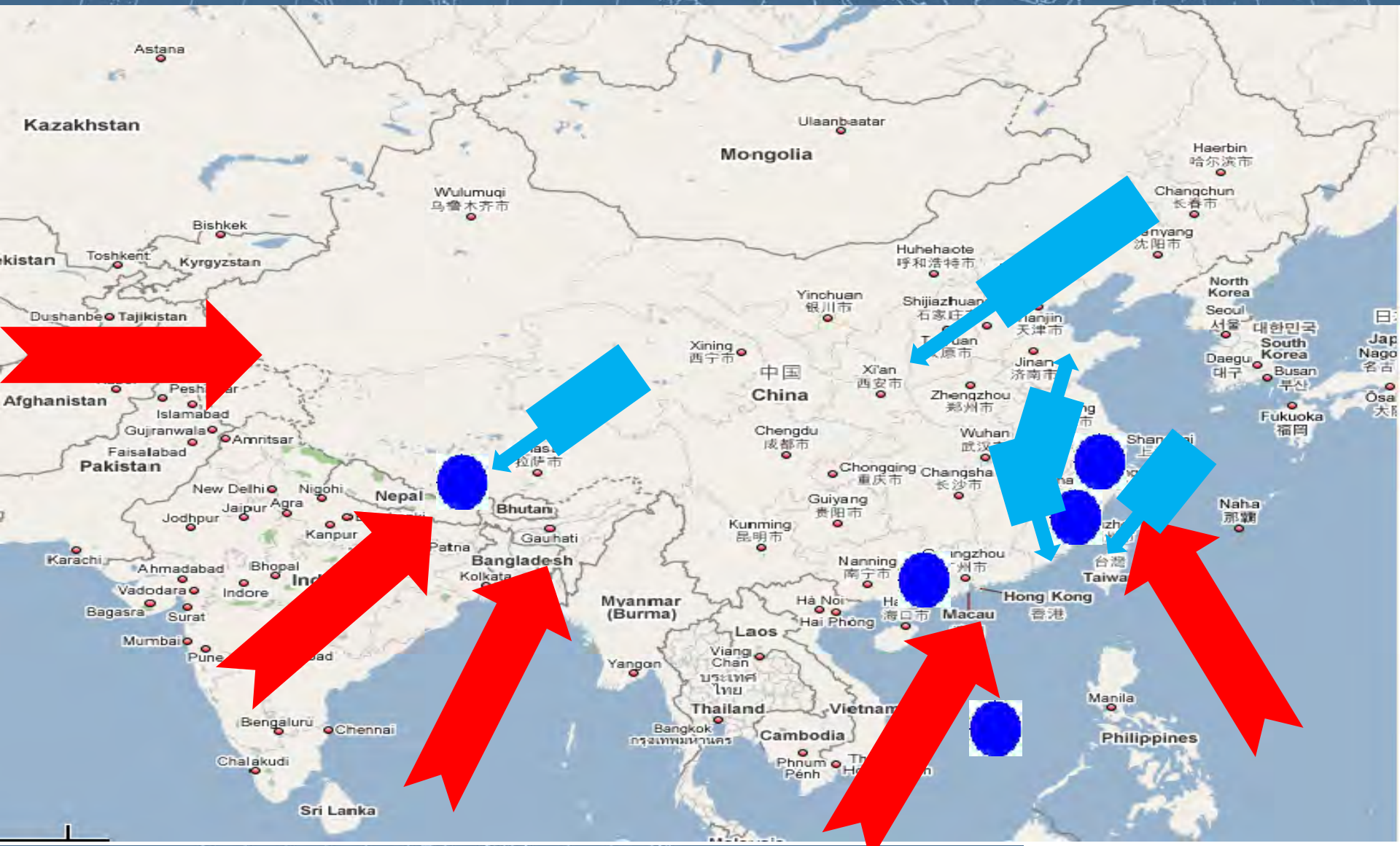
iDEFENSE
Actionable Threat Intelligence

2010-2011 Space Station



iDEFENSE
Actionable Threat Intelligence

35 Satellites Cover Zone (E70-145, N5-55)



iDEFENSE
Actionable Threat Intelligence

Another Time Line

+ “…China has no real war since 50 years ago, soldier needs real practicing…” General (S)
+ Air Defense School Student: From O-2 to O-3, O3-O4, O-4 to O-5.
+ Heritage foundation research : 2025 pacific area 5:1 submarine
+ Aircraft carrier 2020
+ Imbalance between men and women: 40 Million extra bachelors 2020.

+ Another 10 years.

iDEFENSE Actionable Threat Intelligence

My Hypothesis

+ **IF (Taiwan War Break out)**
+ **Then (what China will most likely face)**
  - Cyber (Propaganda, Economic, Media, Penetration , Psychological)
  - Space (Satellite)
  - Air (Regular strike , Airborne and landing, Electronic warfare)
  - Ocean (Pacific Fleet)
  - Land (Direct Force Insertion, “Back Stabbing”)
+ **So**
  - Great Firewall,
  - IPV6
  - .CN Root Domain
  - Satellite Quick Launch
  - Air Defense, CEE
  - More Diesel Submarines
  - Satellite Cover zone
  - Indian

iDEFENSE Actionable Threat Intelligence

Question



EFENSE
tionable Threat Intelligence