# NASSCOM Cyber Security Task Force
# 1st Meeting

May 25, 2015

# Cyberspace – Game Changer

**Increasing Global population** getting online

**Ever Expanding** ~ Growth of Bandwidth and Applications

Increasing Technology & services dependency on cyberspace – **Critical Infrastructure, SMAC, IoT**

**Vulnerabilities** in all platforms and its **Knowledge** available openly

Attacks from **anywhere**; **cheap** to launch

Defense **expensive**; **Attribution** difficult

**Offense dominant**

**Global commons**

A nation's cyberspace is part of the global cyberspace and cannot be isolated to define its boundaries unlike the physical world which is limited by geographical boundaries – land, sea, air and space – **Cyberspace has emerged as the fifth domain which is ever expanding**

# Threat Landscape (Global and India)

| | |
|---|---|
| **Cybercrimes** | • Financial frauds, identity thefts, copyright and trademark violations<br>• McAfee estimate loss of $ 3.7 - 6.9 trillion; banking industry loss upto $ 1.3 trillion |
| **Cyber attacks** | • Attacks on NASA, RSA, IMF, CIA, Sony, Lockheed, Pentagon, Citigroup, Indian Navy, Target<br>• Use of technology & cyberspace by terrorists in 26/11 Mumbai attacks |
| **Critical Infrastructure** | • Attacks on e.g., T3 Delhi; Malwares such as Stuxnet, Duqu, Flame, Shamoon infections<br>• Banks, Telecom network targeted; Cyber hijacking of aircrafts and drones |
| **Cyber Espionage** | • Economic, military and state secrets theft, annual loss of IPRs in excess of $ 1 trillion<br>• Complex malware such as Flame for espionage |
| **Cyber Warfare** | • Cyber attacks on Estonia, Georgia, South Korea and others - military use of cyberspace<br>• Non-state actors used by nation-states for specific aims, Global crime syndicates etc<br>• Nation-states getting into game in big way e.g., Ghostnet, Stuxnet |
| **Social media spawning newer crimes** | • Used for vested interests to initiate movements against states, organize revolutions<br>• Used for spreading terrorism and inducting recruits (ISIS)<br>• Spreading of rumors to create fear in communities - London riots, Northeast exodus |

# Existing Cyber Security Initiatives-India

## Policy Initiatives & Guidelines

- *National Policies on IT, Telecom and Electronics* - 2012
- *National Cyber Security Policy* - 2013
- *Guidelines for Critical Information Infrastructure Protection* -2013
- *National Information Security Policy & Guidelines* - 2014
- *Draft IoT (Internet of Things) policy* - 2014
- *M2M (machine-to-machine) Roadmap document* - 2015

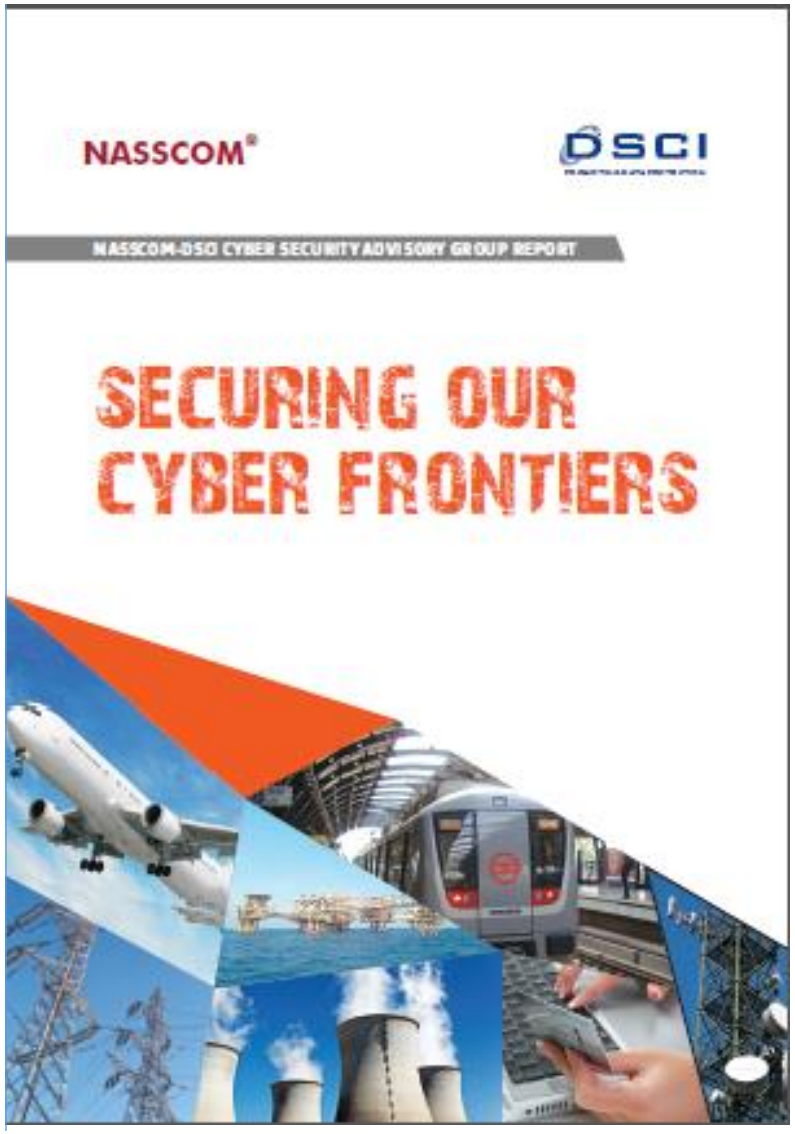
## Regulatory Framework

- *Information Technology (Amendment) Act, 2008*
- Regulatory Guidelines issued by regulators such as
  - *Reserve Bank of India* (RBI),
  - *Telecom Regulatory Authority of India* (TRAI),
  - *Securities and Exchange Board of India* (SEBI),
  - *Insurance Regulatory and Development Authority* (IRDA)

## Institutional Mechanisms

- **DSCI** (Policy, Assurance, Capacity Building and Awareness)
- **JWG** (PPP)
- **NASSCOM-SSC** (Skills)
- **IB-CART** (Information Sharing)
- **ISEA** (Capacity Building and Awareness)
- **Cyber Forensic Lab** (Capacity Building)
- **LITD 17 Committee of BIS** (Standards)

# NASSCOM- DSCI Cyber Security Advisory Group (CSAG) Recommendations - 2012




1. Create a **National Structure for Cyber Security**

2. Design & Implement a **Competency Framework** for building a competent & adequate Cyber Security Workforce

3. Create & maintain **Inventory of Critical Information Infrastructure**

4. Establish a **Centre of Excellence for Best Practices** in Cyber Security

5. Establish a **National Threat Intelligence Centre** (NTIC) for Early Watch & Warning

6. **Build Capacity of LEAs** in Cyber Crime Investigations & Forensics

7. Build **Lawful Interception Capabilities** for balancing National Security & Economic Growth

8. Establish a **Centre of Excellence for Cyber Security Research**

9. Setup **labs for Accreditation** of ICT Products to Manage Supply Chain Risks

10. Establish a **Cyber Command** to defend the Indian Cyberspace

DSCI
PROMOTING DATA PROTECTION

A **NASSCOM®** Initiative

# Indian Security Products Ecosystem

Indian Security Products revenue for 2015 to be around **Rs. 1500 Crore ($ 250 mn)**

↑ 50% in Last 3 years

↑ 70% in Next 3 years

**50 - 80%** of the employee base is in core R&D

More than **60% export**; 80% in some cases

InstaSafe and you're on.

ArrayShield

सी डैक CDAC

TATA

UNIKEN

K7 COMPUTING

SECLORE

Intellinet Datasys Pvt. Ltd.

TATA CONSULTANCY SERVICES

secpod

pawaa SOFTWARE

WIPRO Applying Thought

i7networks Agentless BYOD Discovery & Control

DataResolve Technologies™

ankhorus

NETWORK INTELLIGENCE

Cyberoam

Quick Heal Security Simplified

INORO Technology 4 Masses

PRECISION BIOMETRIC

AMITY UNIVERSITY

Nevis NETWORKS

INDUSFACE Telecom

Secfence TECHNOLOGIES

Trinity Future-In Pvt. Ltd. Securing your Digital World

Cygnet Infotech IT is about you

INNEFU Information Security at its Best

vaultize Unprecedented Protection, Limitless Access

Bhairav

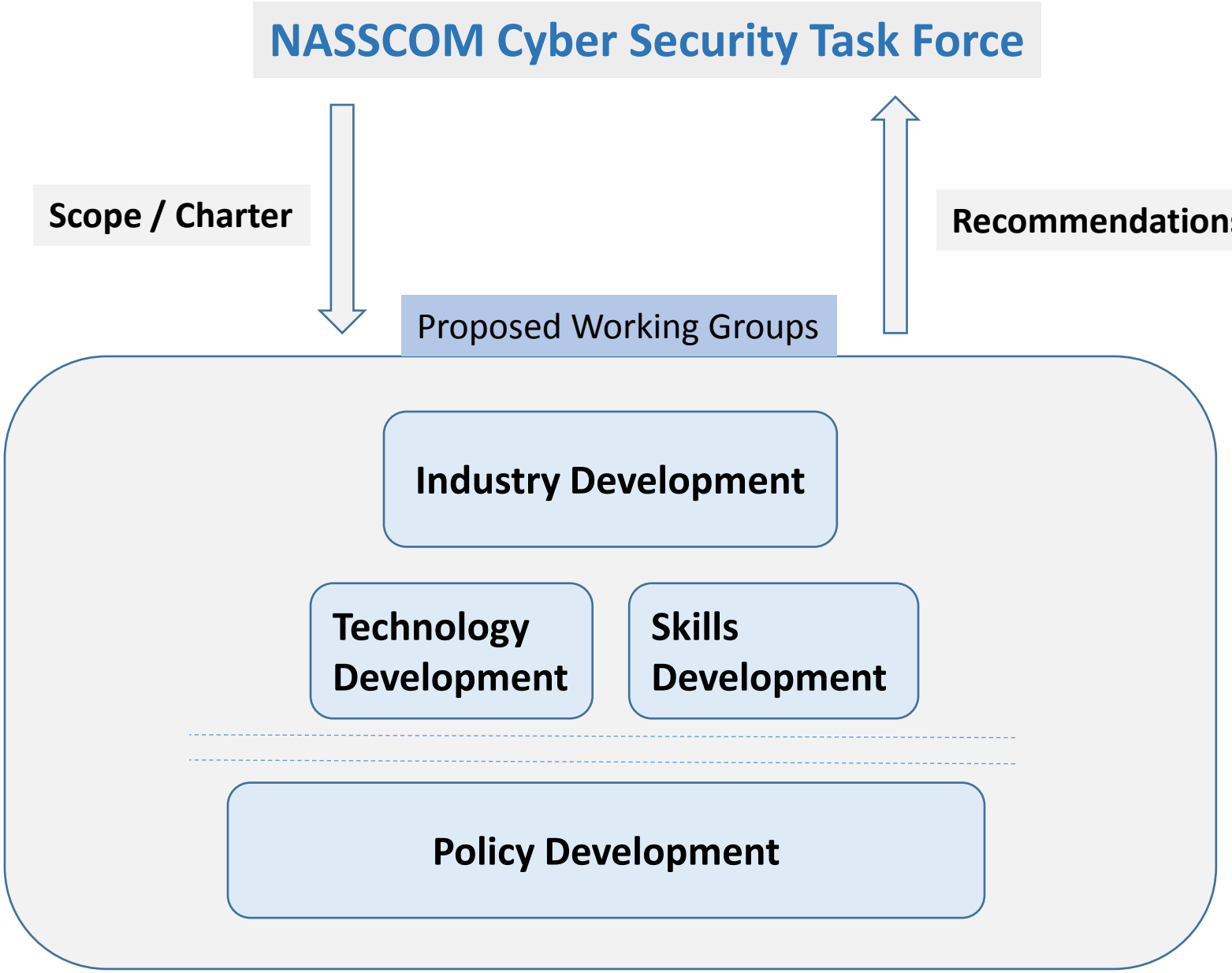
iVIZ intelligent vision

'e Scan

{fix}nix Redefining Security

NEVALES Network Security and Beyond

# CSTF Working Plan




DSCI
PROMOTING DATA PROTECTION

A NASSCOM® Initiative