Information Security & Critical Infrastructure Protection

Presentation to AITEC East Africa ICT Summit
Nairobi, Kenya

By Matunda Nyanchama, PhD, CISSP
Agano Consulting Inc.

Matunda Nyanchama – Short Bio

- Principal Consultant/Director, Agano Consulting Inc. - www.aganoconsulting.com; publisher Nsemia Inc. Publishers – www.nsemia.com); technical author and commentator
- Experience:
  - 14+ years in consulting – IT & IT Security with focus on financial services and security product development
  - 7+ years in telecommunications engineering
- Previous positions
  - Delivery Project Executive/Senior Delivery Program Manager: Managed IT Services, Global Technology services, IBM Canada; sessional faculty (Msc Security Program) University of Ontario Institute of Technology UOIT; Senior Manager of Information Security, Moneris Solutions Inc.; Senior Manager, Bank of Montreal Financial Group; Director, Security Architecture, Intellitactics Inc.; Senior Consultant, Ernst & Young LLP & Executive Engineer, Kenya Posts & Telecommunications Corporation (Kenya)
- Certified Information Systems Security Professional (CISSP)
- Msc. & PhD, Computer Science (UWO), Bsc. Electrical Engineering (UoN, Kenya)
- Contact: mnyanchama@aganoconsulting.com

Agano Consulting Inc. – A profile

- IT Consulting Company
  - Based Canada
  - With “tentacles” in East & South African Regions
- Key focus areas
  - IT consulting – Strategy, Architecture, Information Security & Risk Management
  - IT (specifically Info Sec) Training
  - Strategic Planning for SMB, NGOs
  - Market Research – IT Market Trends
  - Strategic Advice & Strategic Planning
- Sectors
  - Government/Public, Non-Government & Private

Critical Infrastructure

CI include

- *"a number of sectors such as food, water, public health, emergency services, energy, transportation, information technology and telecommunications, banking and finance, and postal services and shipping."* – GAO

US Critical Infrastructure Services
Agriculture and Food
Banking and Finance
Chemical
Commercial Facilities
Commercial Nuclear Reactors, Materials, and Waste
Dams
Defense industrial base
Drinking Water and Water Treatment Systems
Emergency Services
Energy
Government Facilities
Information Technology
Manufacturing
National Monuments and Icons
Postal and Shipping
Public Health and Healthcare
Telecommunications
Transportation Systems

Cyber Security

- Information Security:
  - *Pertains to confidentiality, integrity and availability*

- Cybersecurity
  - *"The defence against attacks on information technology infrastructure."* – GAO
  - *"Safeguarding of computer networks and the information they contain from penetration and from malicious damage or disruption."* - Lewis

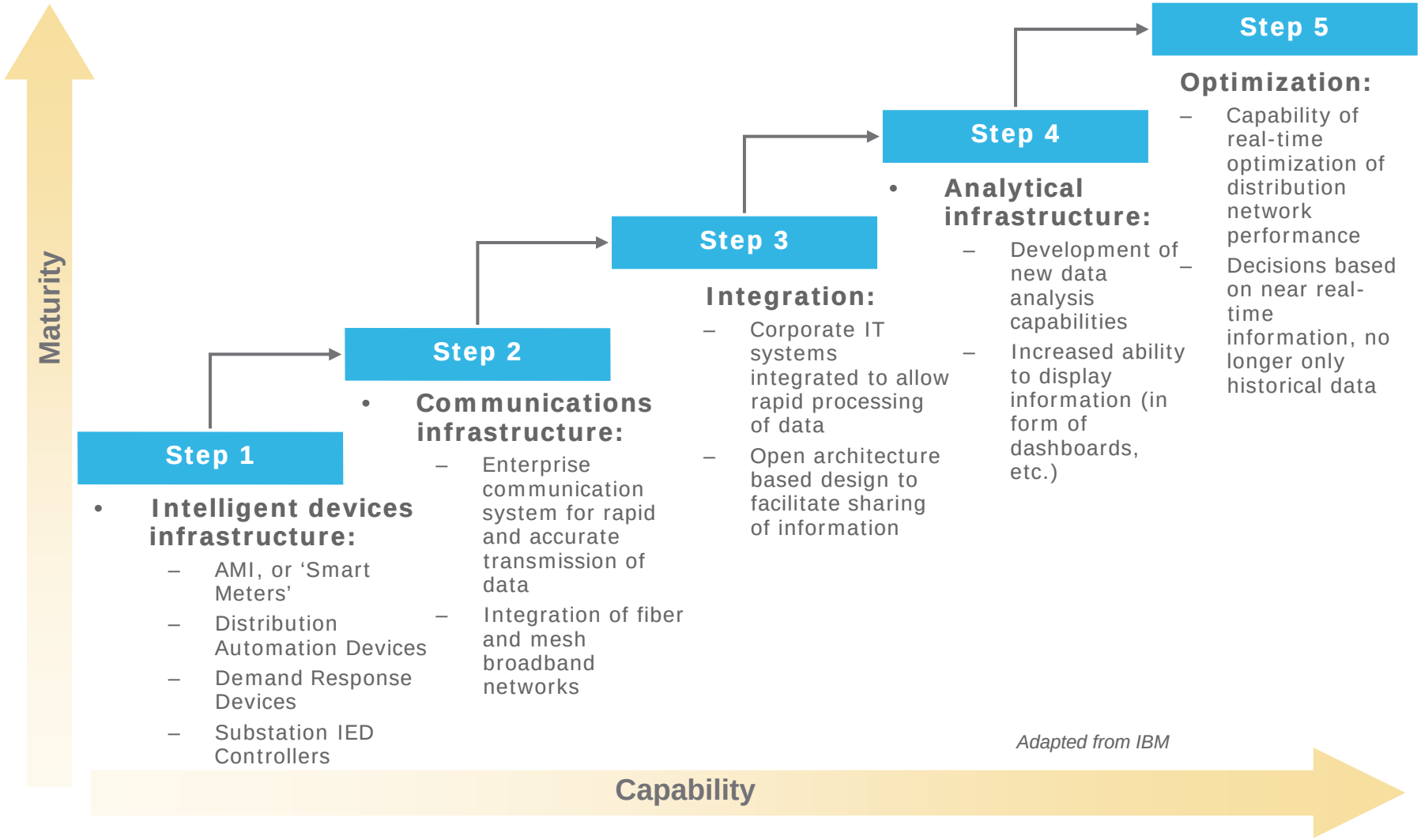
CIs & CyberSecurity

- Critical infrastructures (CIs) increasingly rely on computers and networks for their operations.
  - Example in industry Supervisory Control And Data Acquisition (SCADA) systems are common.

- Many of the CIs networks are also connected to the public Internet; hence face the same risks as do systems on the Internet

- CIs need similar protection as systems on the Internet

Vision of Smart Grid



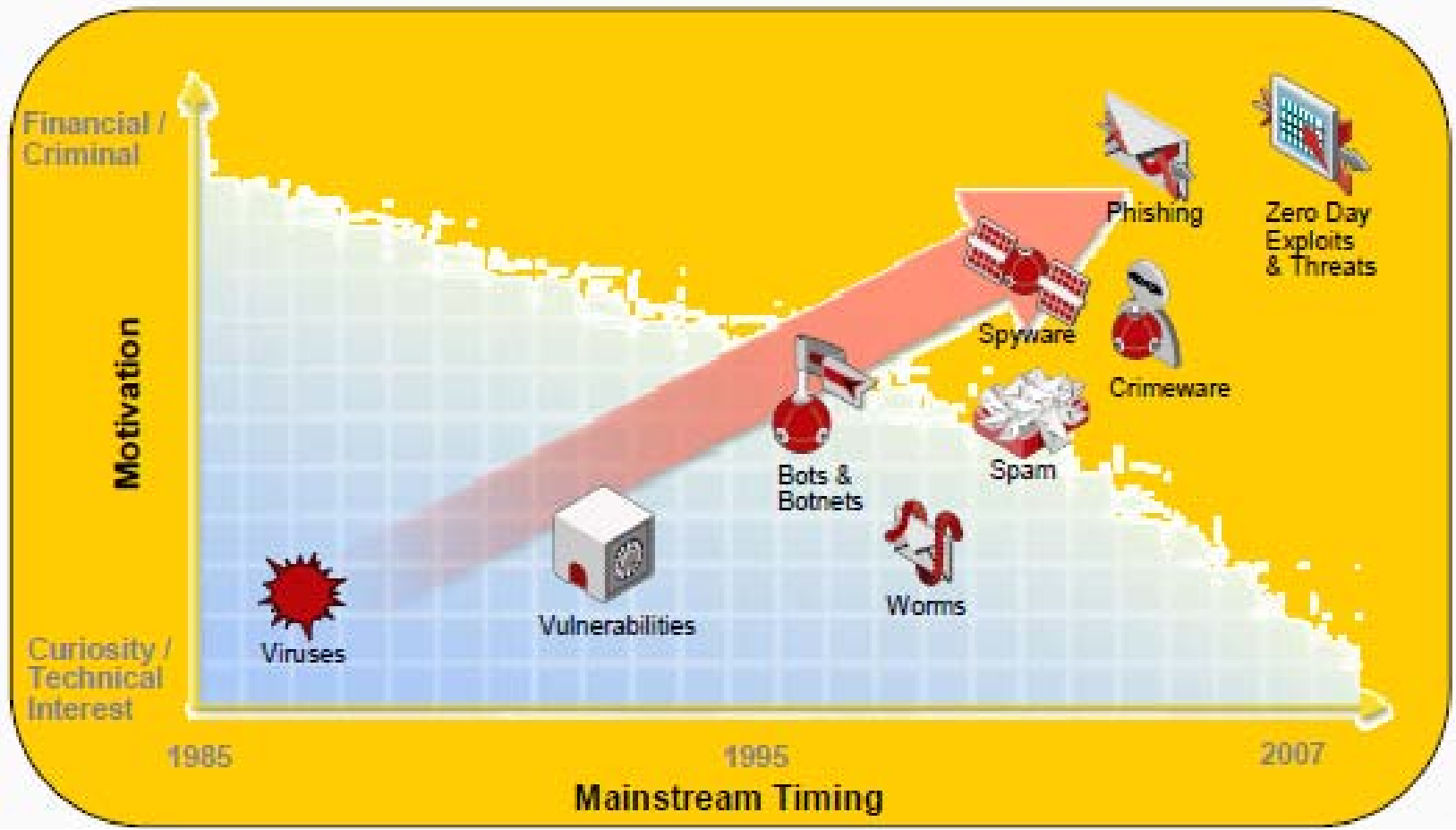
Cyber Threats – The Reality Attacks

- We see proliferation of Information Technology
- Rapid growth and use of the Internet
- Growing number of online transactions
- Today, information systems are essential part of critical infrastructure
- Internet Systems vulnerable target for attack
  - Systems not securely configured
- Attack techniques continue to be sophisticated
- Rapid proliferation of malware

CI Risks

- With connectivity to the Internet CI at risk of attack like any other systems on the Internet
- Attack sources can be anywhere in the world; and not confined to geographical boundaries
- Attack techniques getting more sophisticated and able to mask their behaviour
- Difficult to track attackers

Cyber Threats – Evolving Sophistication



Source: Anil Sagar. *Privacy and Security Countermeasures in e-Governance Projects in India*.

Cyber Warfare Attacks

- Threat (Military & Economic)
  - Espionage
  - Disruption
  - Sabotage

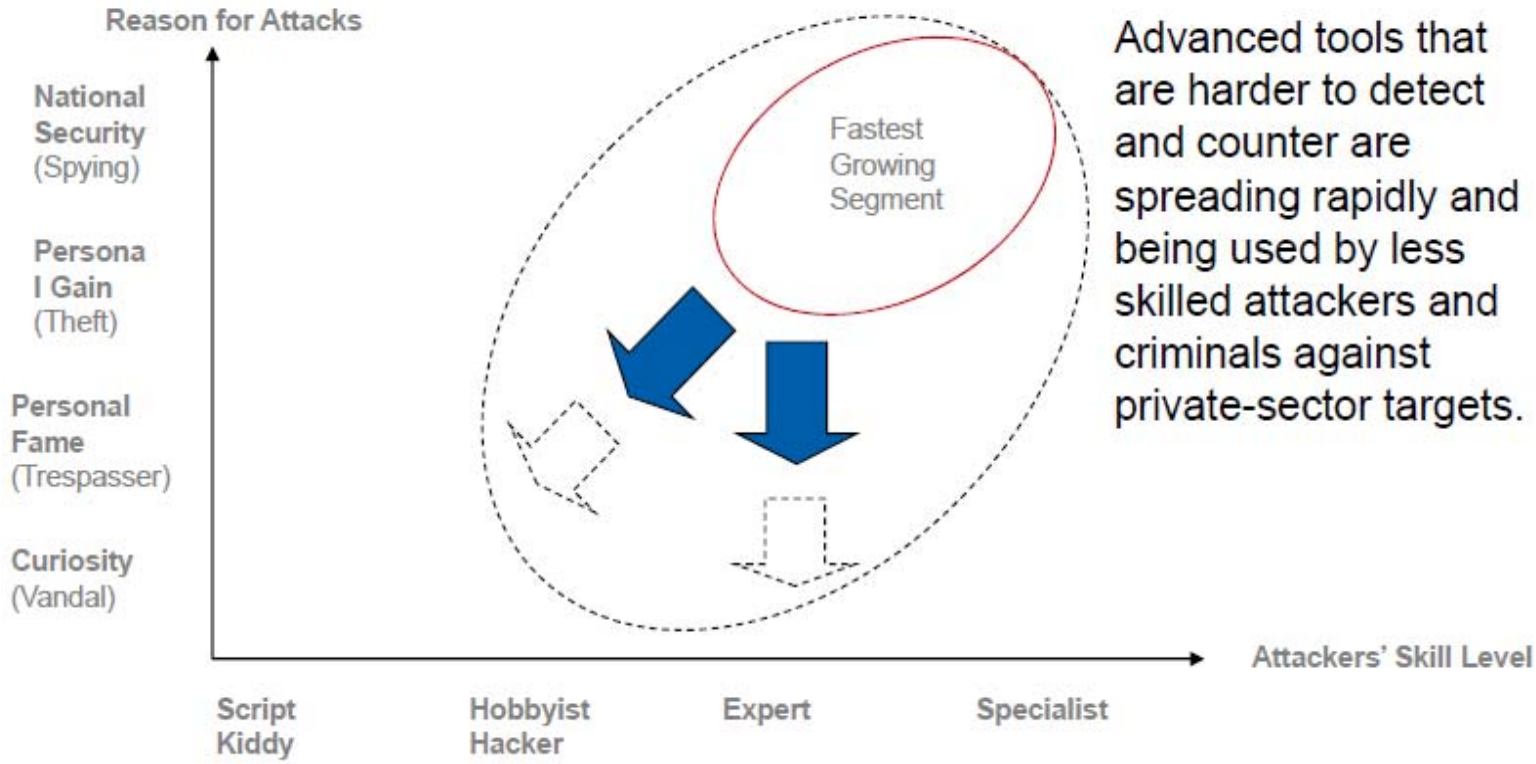
- Organized attacks by
  - States
  - Hacktivists
  - Terrorist groups
  - Criminal groups

Coordinated physical strategies could cripple critical infrastructure

- Cyber tools common, easy to use, inexpensive

Source: Greene: *Cyber Warfare and Implications for National Security*

Expert Tools Used for attacks



Advanced tools that are harder to detect and counter are spreading rapidly and being used by less skilled attackers and criminals against private-sector targets.

Source: Greene: *Cyber Warfare and Implications for National Security*

Modes of Malicious Attack on CI

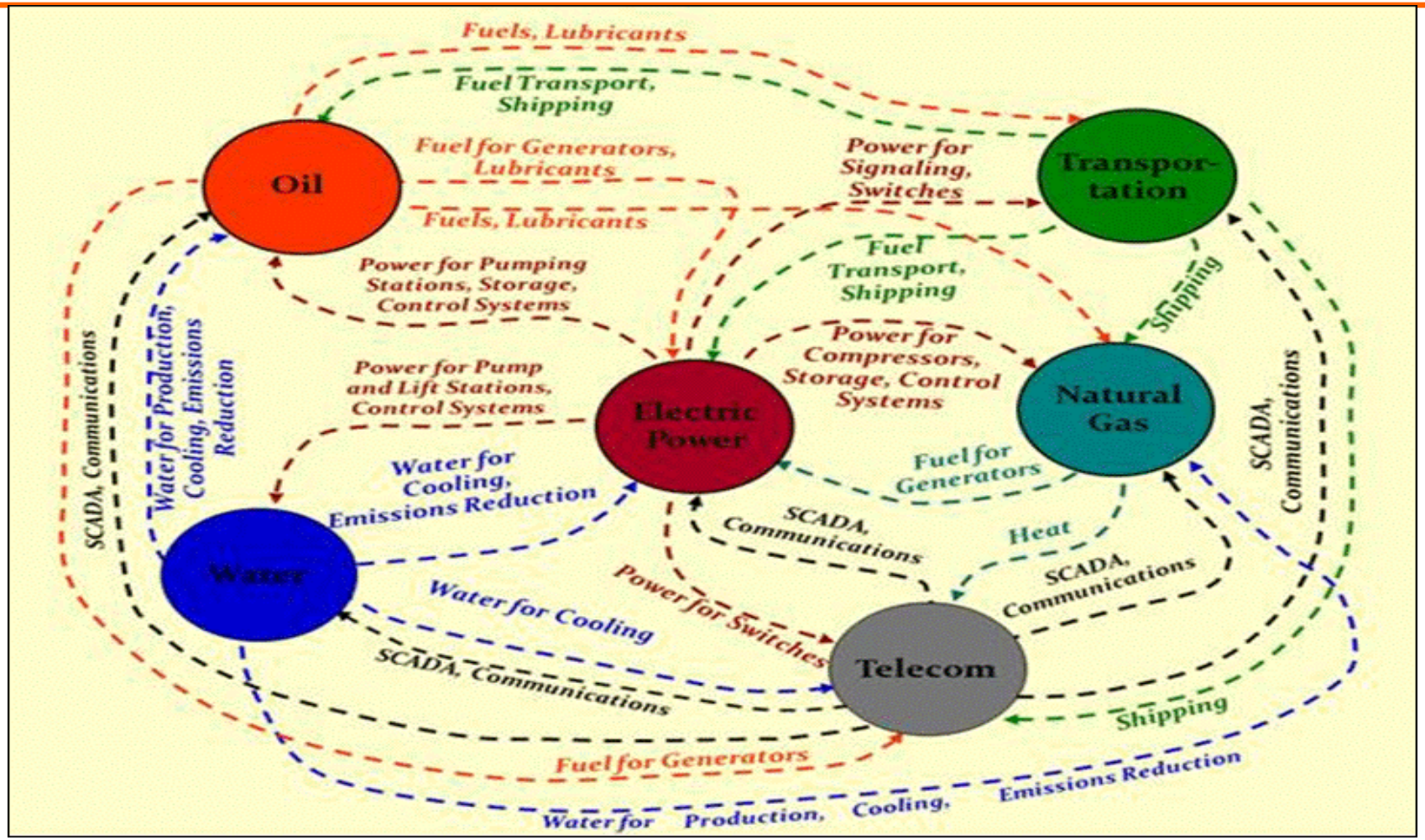
- Attacks upon the system - The system itself is the primary target with ripple effects throughout society;
- Attacks by the system - The population is the actual target, using parts of the system as a weapon;
- Attacks through the system - The system provides a conduit for attacks on other critical infrastructures.

Source: *Performance, Robustness, and Cyber Security of Critical Infrastructure Systems – A Cyber-Physical Systems Research Theme.*

Technology Confluence - Complexity

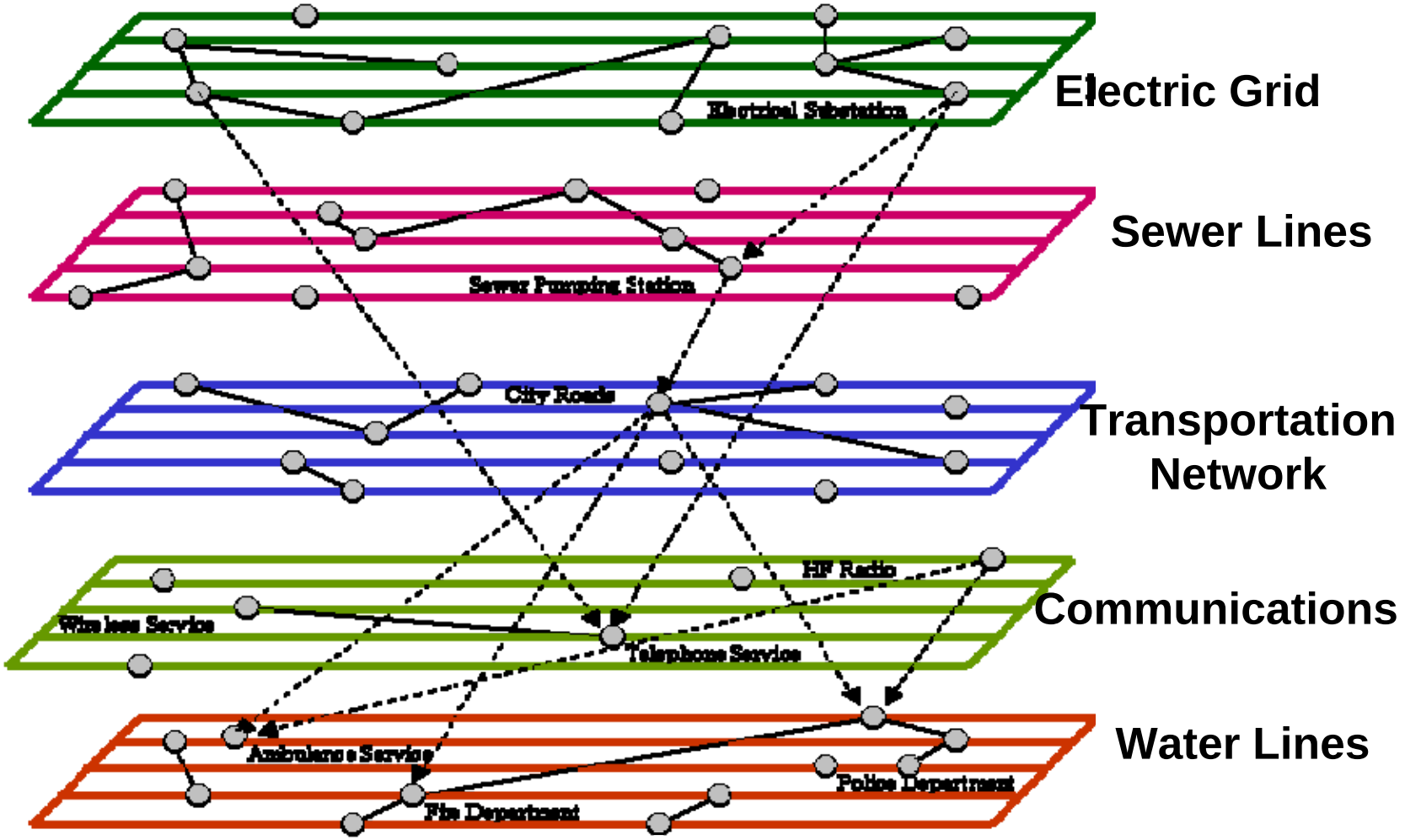
Source: Heller, M (2001). Interdependencies of Civil Infrastructure Systems. *The Bridge*, a publication of the Nation Academy of Engineering. V. $, #31, 2001

Critical Infrastructure Interdependencies



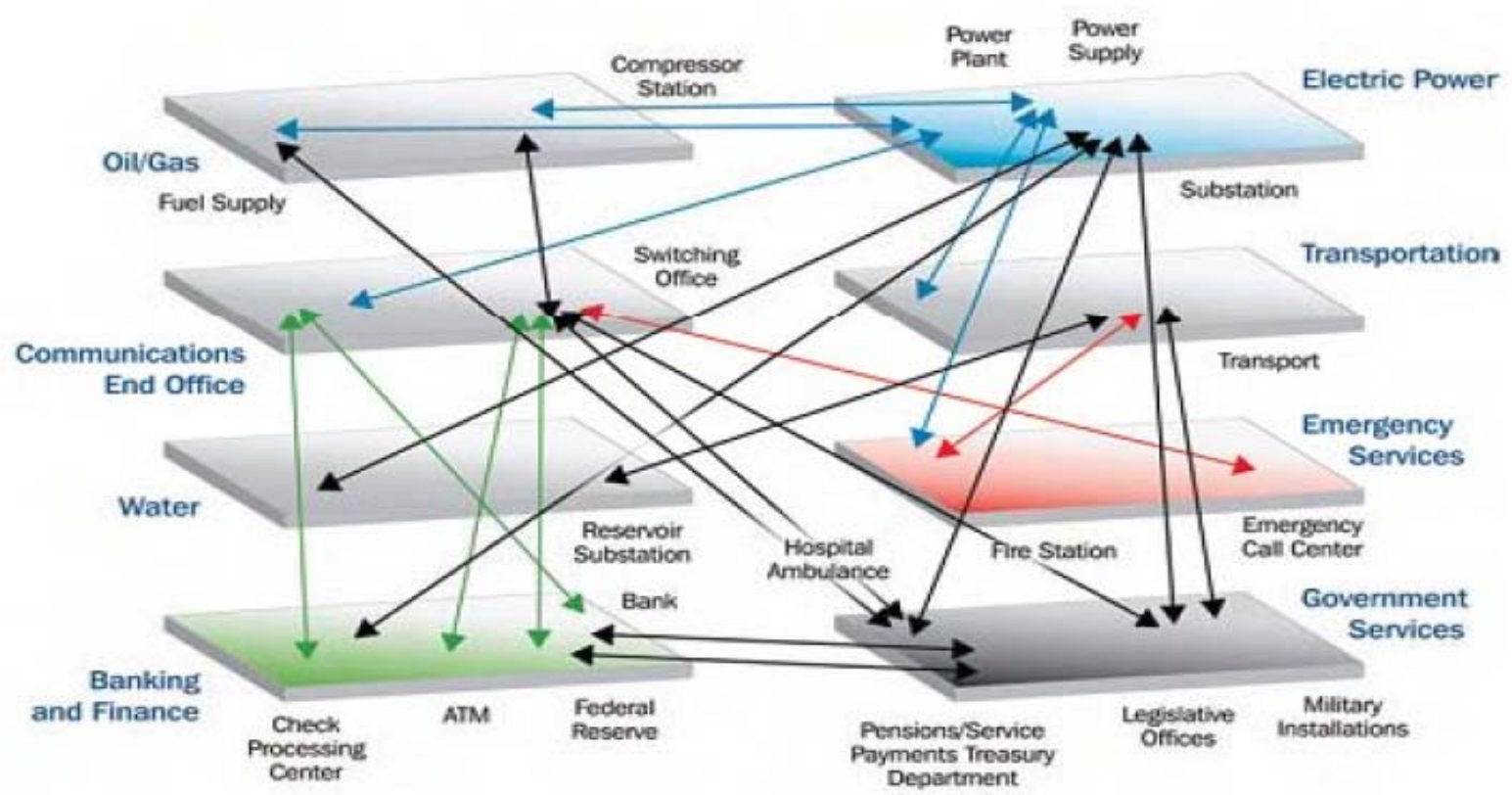
Source: Heller, M (2001). Interdependencies of Civil Infrastructure Systems. *The Bridge*, a publication of the Nation Academy of Engineering. V. $, #31, 2001

Infrastructure Interdependencies



Source: Critical Infrastructure Interdependencies Modeling: A Survey of U.S. and International Research, Idaho National Laboratory

Critical Infrastructure Interdependencies



http://science.nasa.gov/headlines/y2009/21jan_severespaceweather.htm

Critical Infrastructure & National Security

- CI protection enhances national security
- CI Protection *"pertains to activities intended for the protection of a country's cyber & physical public; and private infrastructures that are critical to national security, national economic security, or national public health and safety."* - GAO
- A large % of CIs are owned by the private sector
- Hence public-private partnerships are essential for CI protection.

Overcoming the CI Protection Challenge - I

- Need public-private partnerships
  - Create an authority to coordinate the efforts, e.g. Centre for Critical Infrastructure Protection
  - Would ensure national security by helping reduce vulnerabilities of national infrastructure.
  - Develop clear mandate for the entity, including cyber protection
- Raise education & awareness
- Document CI services and infrastructure
- Adopt a risk assessment approach
  - Remember it is impossible to eliminate risk

Overcoming the CI Protection Challenge - II

1. **Reduce the most substantial risks through centrally-defined standards;**

2. **Provide a shared framework to support cross-sector activity;**

3. **Enhance capacity of infrastructure to absorb shock, through designs that give the CI robustness**

4. **Information Sharing**
   - **Throughout the life of CI**
   - **Improved information sharing and engagement before, during and after emergencies.**

Source: Mat Barber. *Improving the Resilience of Critical Infrastructure to Natural Hazards.*

Sample CI Entity Mandate

1. Develop a national plan for critical infrastructure protection, including cybersecurity.
2. Develop partnerships and coordinate with other federal agencies, state and local governments, and the private sector.
3. Improve and enhance public/private information sharing involving cyber attacks, threats, and vulnerabilities.
4. Develop and enhance national cyber analysis and warning capabilities.
5. Provide and coordinate incident response and recovery planning efforts.
6. Identify and assess cyber threats and vulnerabilities.
7. Support efforts to reduce cyber threats and vulnerabilities.
8. Promote and support research and development efforts to strengthen cyberspace security.
9. Promote awareness and outreach.
10. Foster training and certification.
11. Enhance federal, state, and local government cybersecurity.
12. Strengthen international cyberspace security.
13. Integrate cybersecurity with national security.

Questions

References

- General Accounting Office (GAO – USA) *Cybersecurity for Critical Infrastructure Protection,* May 2004.
- Brent Greene. *Cyber Warfare Implications for National Security and Critical Infrastructure Protection*; Presentation to a Cyber Security Workshop; Christopher Newport University; October 28, 2009
- Samuel A Merrell & James F. Stevens. *The Confluence of Physical and Cyber Security Management.* GOVSEC 2009.
- Anil Sagar. *Privacy and Security Countermeasures in e-Governance Projects in India*. Indian Computer Emergency Response Team. [Accessed on Internet Sept., 2010.]
- James A. Lewis. *Cybersecurity and Critical Infrastructure Protection.* Center for Strategic and International Studies, January 2006
- Performance, Robustness, and Cyber Security of Critical Infrastructure Systems – A Cyber-Physical Systems Research Theme.
- Mat Barber. *Improving the Resilience of Critical Infrastructure to Natural Hazards.*