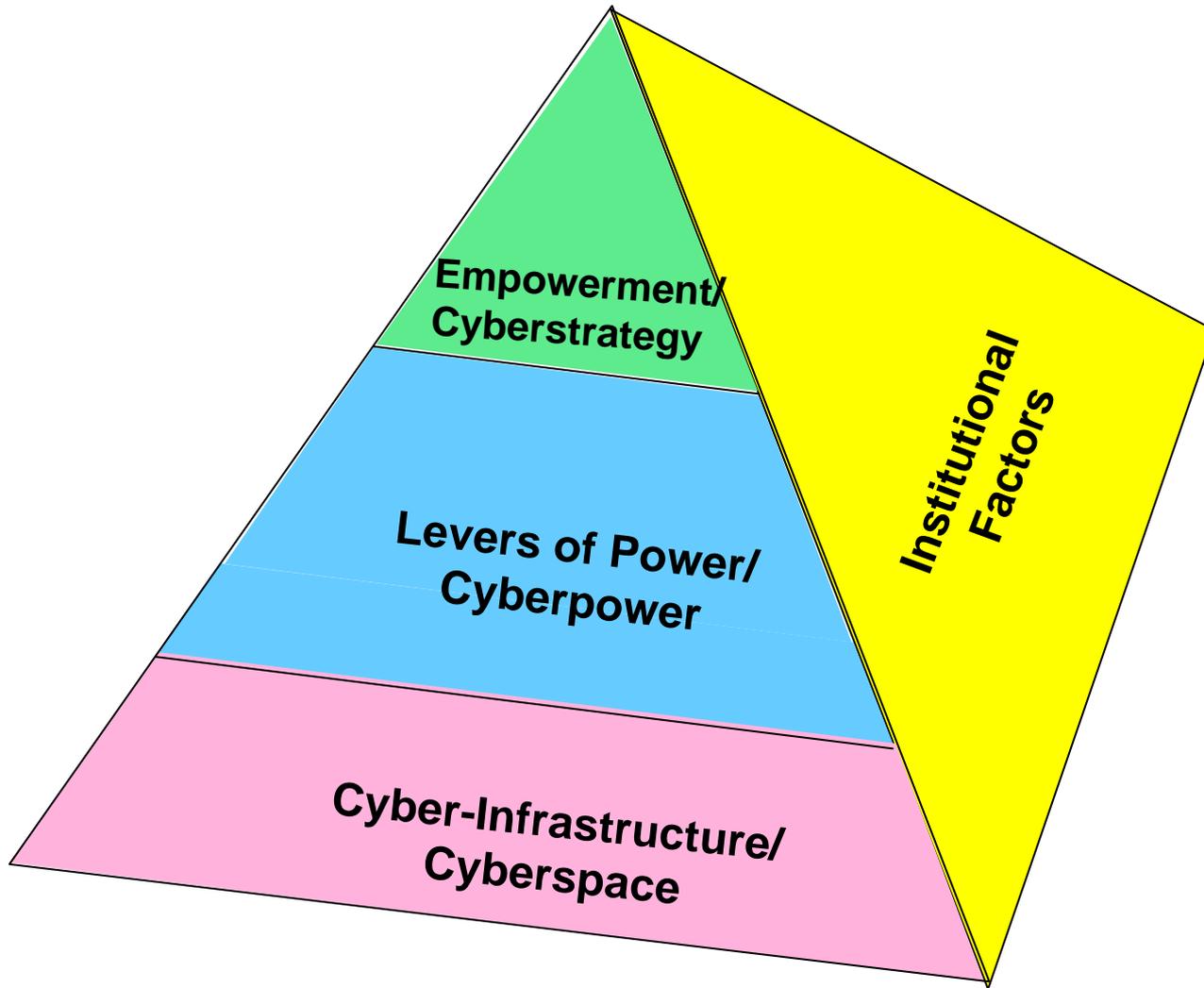


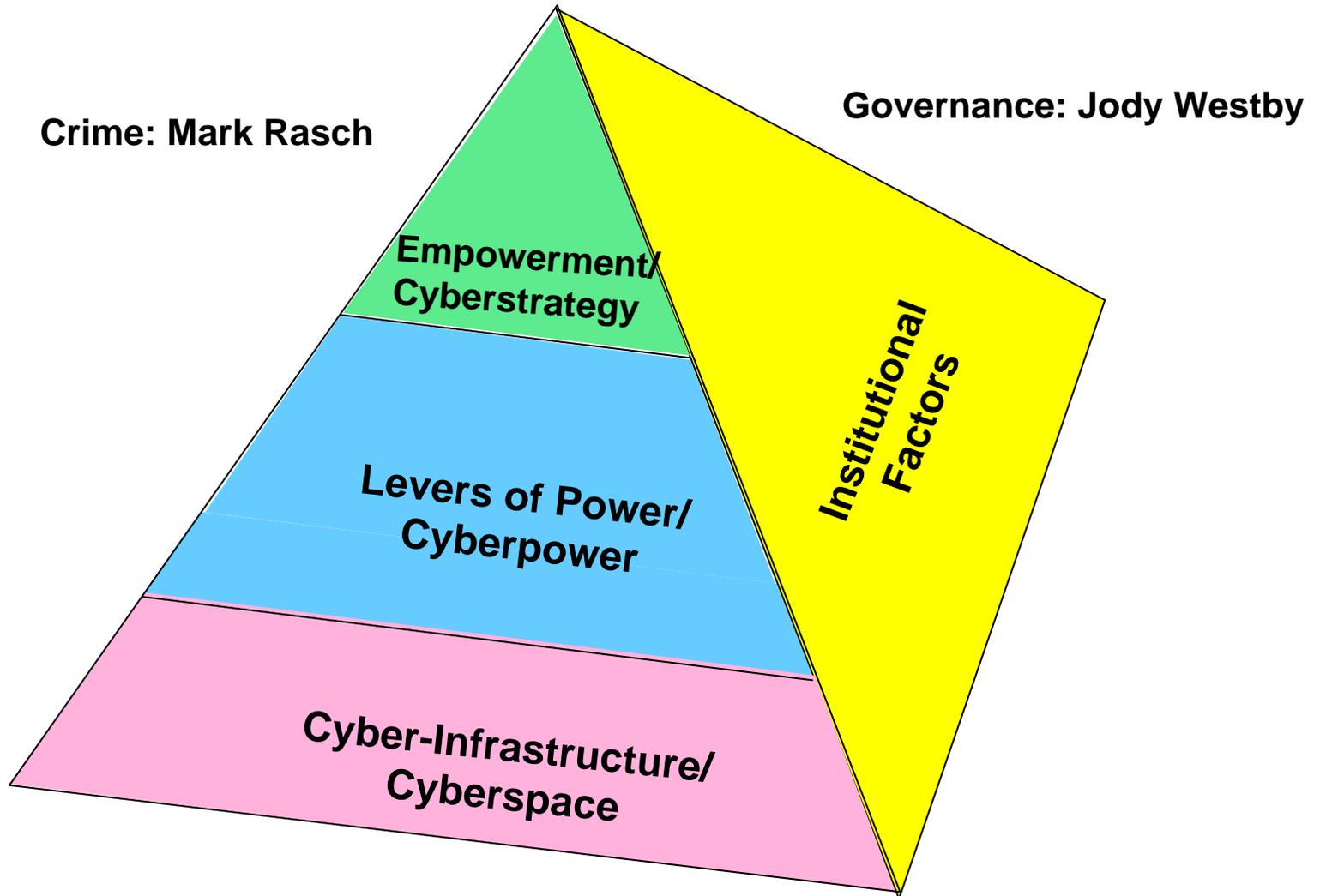
Panel 1 --
The International Challenges of
Crime, Security, and Governance:
Context

April 29, 2009

Framework



Framework: Panel 1



Framework: Panels 1-6+

Governance: Jody Westby

**Panel 3: Critical Cyber
Infrastructure Protection**

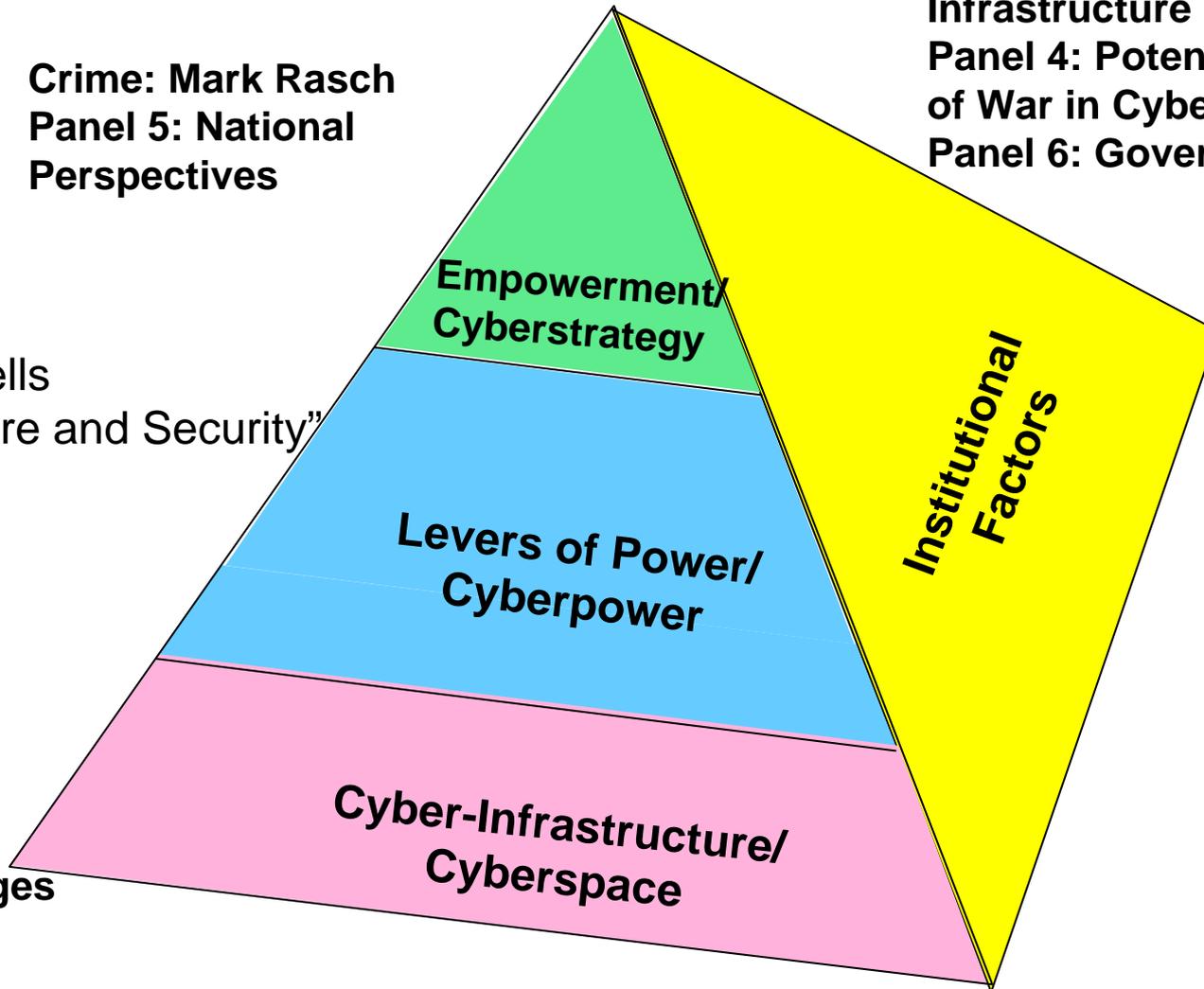
**Panel 4: Potential Thresholds
of War in Cyberspace**

Panel 6: Governance Initiatives

Crime: Mark Rasch
**Panel 5: National
Perspectives**

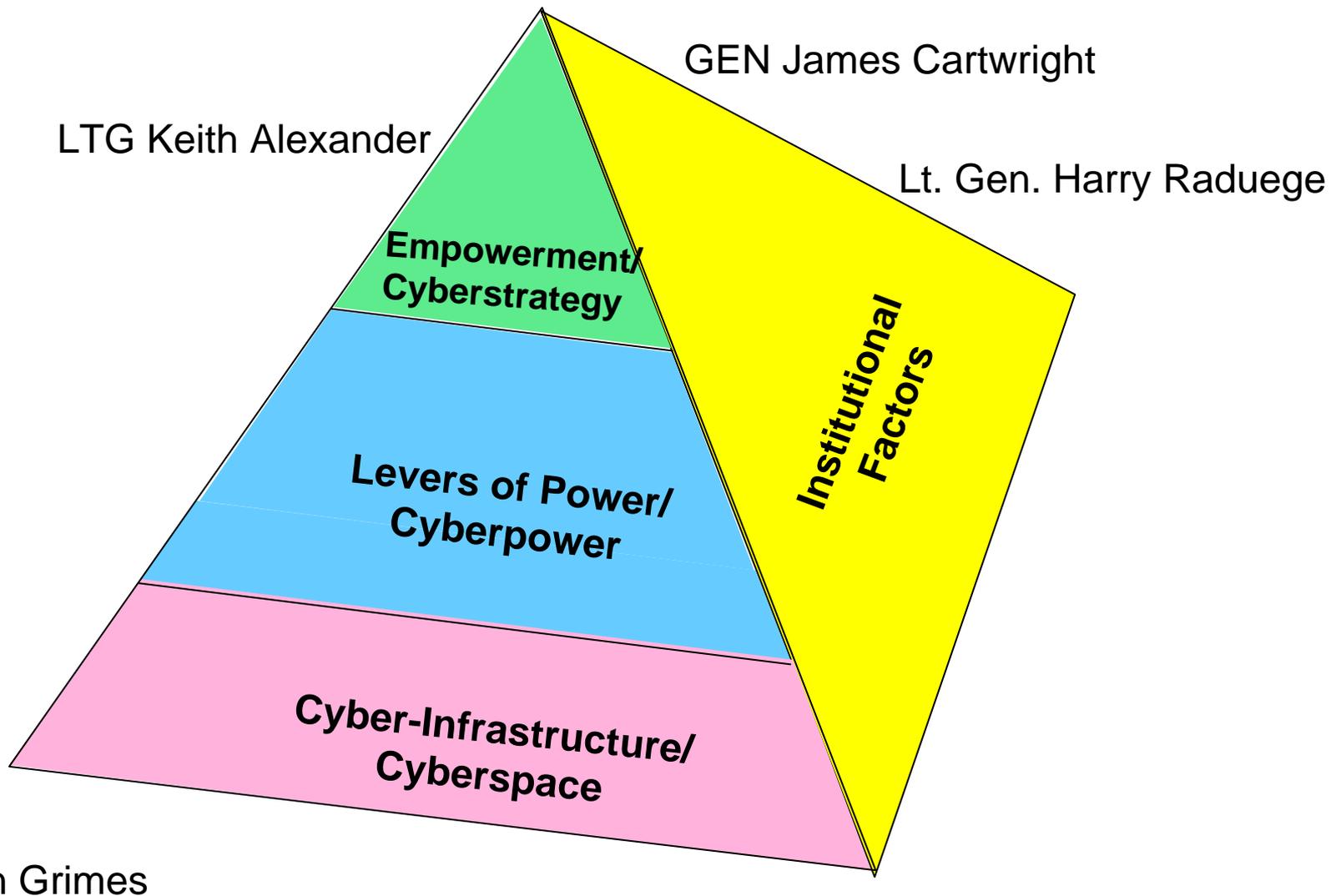
Drapeau & Wells
“Social Software and Security”

Security:
Ed Skoudis
Rich Baich
Panel 2:
Policy Challenges
In Defending
Against Cyber
Attacks



Back-up

Conference Framework: Key Speakers





Security in Cyber Space

How Good Is it?

By Ed Skoudis
InGuardians Co-Founder



Security in Cyber Space

- A sufficiently determined, but not necessarily well-funded attacker can break into almost any modern organization
 - Gaining control of critical systems within the organization
 - Exfiltrating sensitive information
 - Acting for sufficient periods of time unnoticed to damage that organization
- Besides enterprises, the problem is worse for consumers
 - Over 250 million accounts compromised in 2008, according to Verizon's annual report
 - At its peak, the 2008/2009 Conficker worm infected over 3 million machines
 - The bad guys are awash in stolen credit card numbers
 - They commit fraud on only small percentage of the accounts they hold



Why Is This So? Vulnerabilities

- Increased attack surface
 - Client-side exploitation
 - Browsers (IE and Firefox), document rendering programs (Adobe, Word, Excel), media players (Real Player, Windows Media Player), program execution environments (Java Runtime Environment)
 - Wireless (almost) everywhere
 - Wifi and bluetooth, among others
 - Webification of most applications
 - Web 2.0 – Content posted by millions now widely distributed
 - SQL Injection
 - Cross-Site Scripting
 - Such attacks can be combined together

More Why Is This So?

Repeated Mistakes



- We're not learning from the mistakes of the past
 - Buffer overflow vulns still prevalent
 - Misconfigurations abound
 - Comprehensive patching processes remain elusive
 - New languages and environments to run them are embedded in nearly everything
 - General-purpose computer systems are hungry to run code...
 - ...and attackers are happy to provide it

Why Is This So?

Asymmetry and Botnets



- Computer attackers have always benefited from the fact that they only need to find one way in, while the “good guys” need to block almost every avenue in...
 - ...or at least police every entry point
- A crucial asymmetry in offense vs. defense...
 - Making attackers’ jobs easier than defenders’
- The asymmetry is also present in costs:
 - Write and distribute a worm for a few hundred dollars
 - Defending against or cleaning up a worm attack is much more costly
- Plus, with the rise of botnets, the attackers increasingly have computer firepower that matches or even exceeds the target organization



Conclusion

- Sorry I could not paint a cheerier picture
 - But, we have to call 'em as we see 'em
- The good news: Security is improving...
- The bad news: Attacker's techniques for finding flaws, exploiting them, and monetizing their attacks are increasing far more quickly
- The balance increasingly shifts in the attacker's favor



State of Cyber Governance

Jody R. Westby, Esq.
National Defense University
April 29, 2009

www.globalcyberrisk.com

Internet Governance: Definition

Definition of Internet Governance:

The development and application by Governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programs that shape the evolution and use of the Internet.

Working Group on Internet Governance, June 2005 Report



Internet Governance: Key Issues

- **Internet Governance Forum (IGF)** – Outcome of WSIS; multi-stakeholder policy dialogue
- **ICANN – IANA** agreement leaves Verisign in charge of putting data into root; political lightning rod; conspiracy theories about USG, ICANN has USG approved staff, Verisign is USG butler (Proposal to IANA, approved, IANA tells NTIA, NTIA tells Verisign)
- Governance of Internet by UN v U.S. – Berlusconi & G8 Agenda
- Driven by developing countries -- Infrastructure development perceived as governance issue v. investment, liberalization issues
- **U.S. v ITU** agenda – cybercrime should not be considered
- **Bottom Line:** US National & Economic Security Issues v. Developing Countries' Goals
- **Reminder:** China's independent network provides national security through redundancy

3



THANK YOU!

Jody R. Westby

4





An Industry Perspective on Cybersecurity Challenges

Rich Baich, CISSP, CISM
Deloitte & Touche LLP

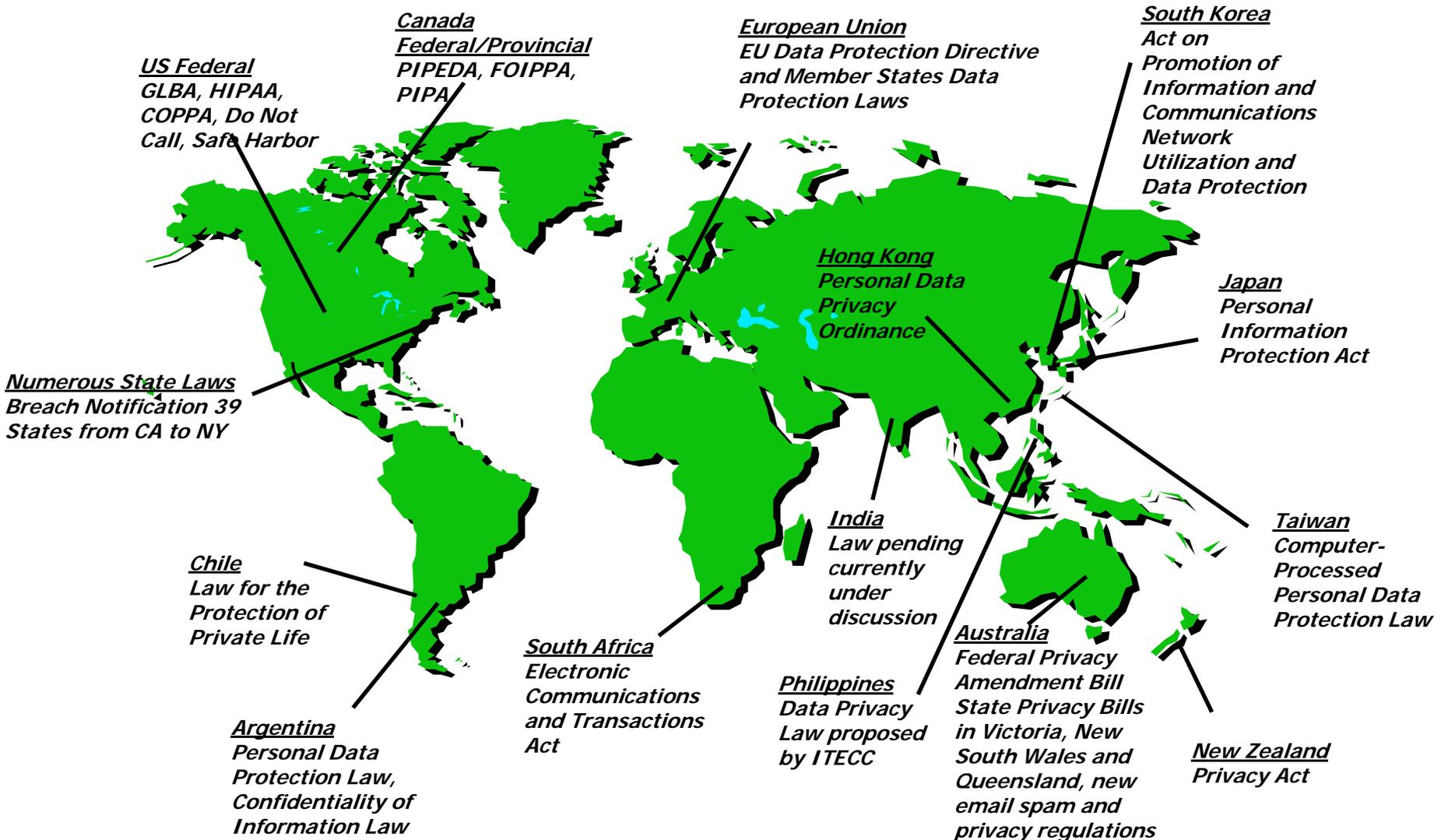
April 29, 2009

Seemed Like a Good Idea at the Time...



Hilda Schrader Witcher
078-05-1120

Global Response: Proliferation of Privacy and Data Protection Laws & Regulations



What is Risk ?

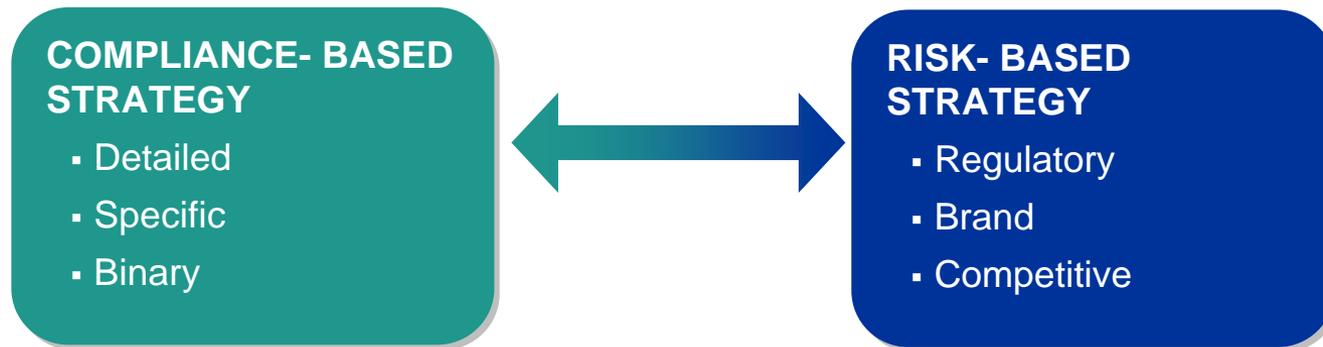
$$V + T + AV \times P^* = Risk$$

<u>Vulnerability</u>	<u>Threats</u>	<u>Asset Value</u>	<u>Risk</u>
<i>Insecure Software</i>	<i>External</i>	<i>Intellectual</i>	<i>Business Disruption</i>
<i>System Failure</i>	<i>Threat</i>	<i>Property</i>	<i>Corporate Liability</i>
<i>Social Engineering</i>	<i>Man-Made</i>		<i>Shareholder Confidence</i>
<i>Geography</i>	<i>Natural</i>		<i>Customer Trust</i>

** Probability of occurrence*

Compliance vs. Risk-Based Approach

The approach to solving data protection-related issues ranges between adopting a compliance strategy to a risk-based strategy:



Advantages of the risk-based approach:

- Free the company from reactionary cycles
- Allocate scarce resources efficiently and according to level of threat
- Deliver value as quickly as possible

It's up to you.



Be Proactive. Be Prepared.



CAN WE SECURE THE CLOUD? SANCTUARIES ON SERVERS SHARED BY LEGITIMATE ACTIVITIES



Michael R. Nelson
Visiting Professor, Internet Studies
Communication, Culture and Technology Program
Georgetown University

Conclusions

- We are entering the third phase of the Internet
 - As profound as the World Wide Web
 - The next 2-3 years will define the Next Generation Internet
- Standards and business practices are shaping the Net as much—or more—than law and regulation
- The Internet revolution is less than 15% complete
- Preventing abuse of this new infrastructure will require:
 - Building security into the technical standards and architecture
 - More openness and interoperability not less
 - Need to create coalitions between different stakeholder groups



Cloud Computing

Academic grids as a prototype of the cloud

Amazon, Google, Microsoft building huge data centers and offering online apps

Amazon's Elastic Compute Cloud

Gmail – “the entry drug for cloud users”

Flickr, YouTube, Salesforce.com

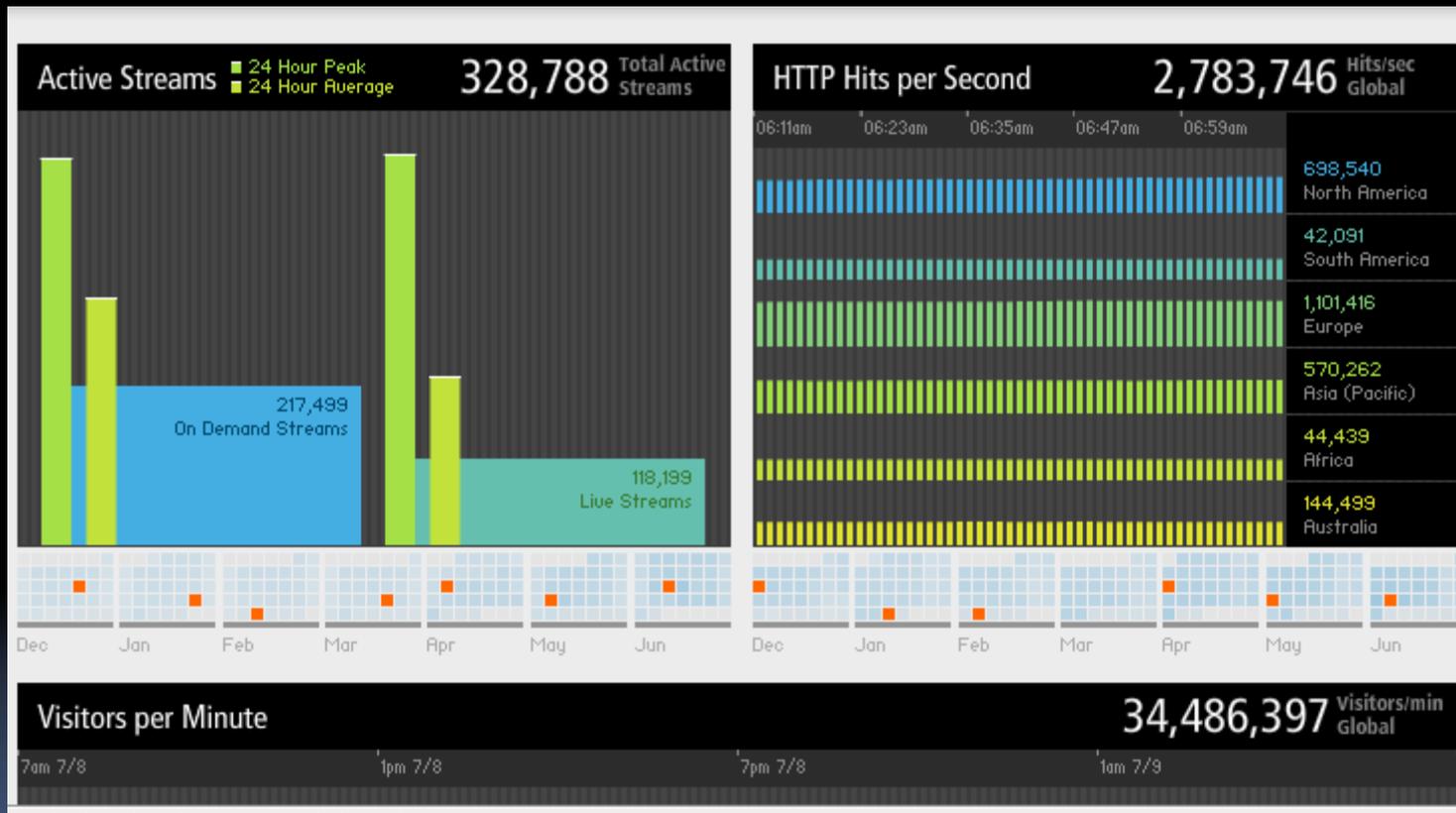


Online back-up

Akamai delivers 15-20 percent of Internet traffic

BOINC grids more powerful than supercomputers

Akamai - Visualizing the Internet



http://www.akamai.com/html/technology/visualizing_akamai.html

THE WALL STREET JOURNAL

WSJ.com

PAGE ONE | MARCH 26, 2009, 4:08 A.M. ET

The Internet Industry Is on a Cloud -- Whatever That May Mean

By GEOFFREY A. FOWLER and BEN WORTHEN

Ever since Google Inc. Chief Executive Eric Schmidt publicly uttered the term "cloud computing" in 2006, a storm has been gathering over Silicon Valley.

Companies across the technology industry are jockeying to associate themselves with clouds. Amazon.com Inc., better known for peddling books online, began selling an Elastic Compute Cloud service in 2006 for programmers to rent Amazon's giant computers. Juniper Networks Inc., which makes gear for transmitting data, dubbed its latest project Stratus. Yahoo Inc., Intel Corp. and a handful of others recently launched a research program called OpenCirrus.

While almost everybody in the tech industry seems to have a cloud-themed project, few agree on the term's definition.

"I have no idea what anyone is talking about," said Oracle Corp. Chief Executive Larry Ellison, when talking about cloud computing at a financial analyst conference in September. "It's really just complete gibberish. What is it?" He added: "When is this idiocy going to stop?"



In its broadest sense, cloud computing describes something apparent to anybody who uses the Internet: Information is stored and processed on computers somewhere else -- "in the clouds" -- and brought back to your screen.

But no two clouds, apparently, are alike. A company's backroom mass of servers and switches is cloudlike. So are social-networking sites like Facebook Inc., or the act of buying a book on Amazon. Some clouds, like Google's email service, Gmail, are public. Others, like corporate networks, are closed to outsiders.

Part of the problem, say observers, is that the tech industry has become bogged down in jargon. Companies have long pushed the likes of "network-distributed parallel processing," often packaged as "solutions" that are "end-to-end" and "scalable." Cloud sounds much nicer.



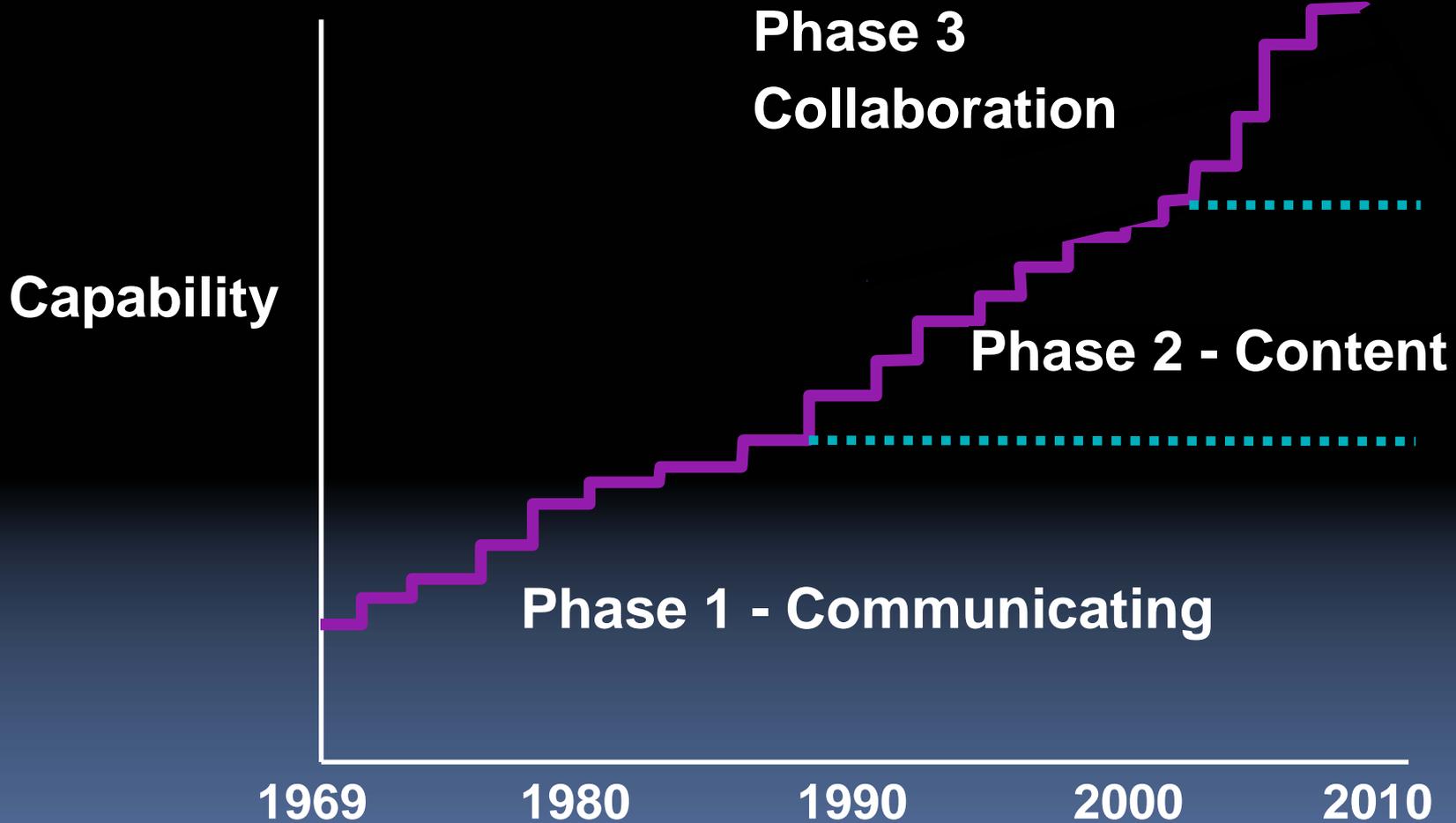
Cloud Computing as “Game Changer”

Why it matters:

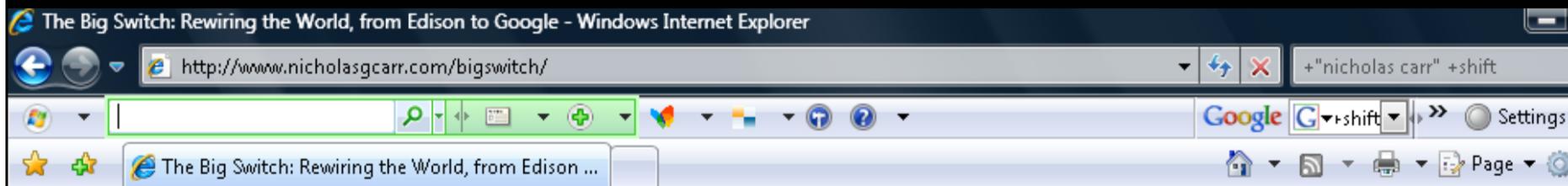
This is the 3rd phase of the Internet

This is the 3rd phase of COMPUTING

The Third Phase of the Internet

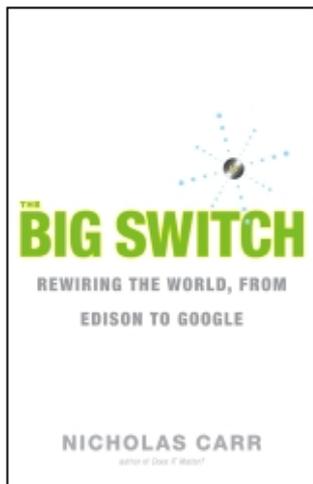


“The Big Switch” by Nicholas Carr



HOME | BLOG | THE BIG SWITCH | DOES IT MATTER? | DIGITAL RENDERINGS | ARTICLES | SPEAKING

nicholas g carr



Excerpts:
["Where did the computer go?"](#)
["Among the dynamos"](#)
["A spider's web"](#)

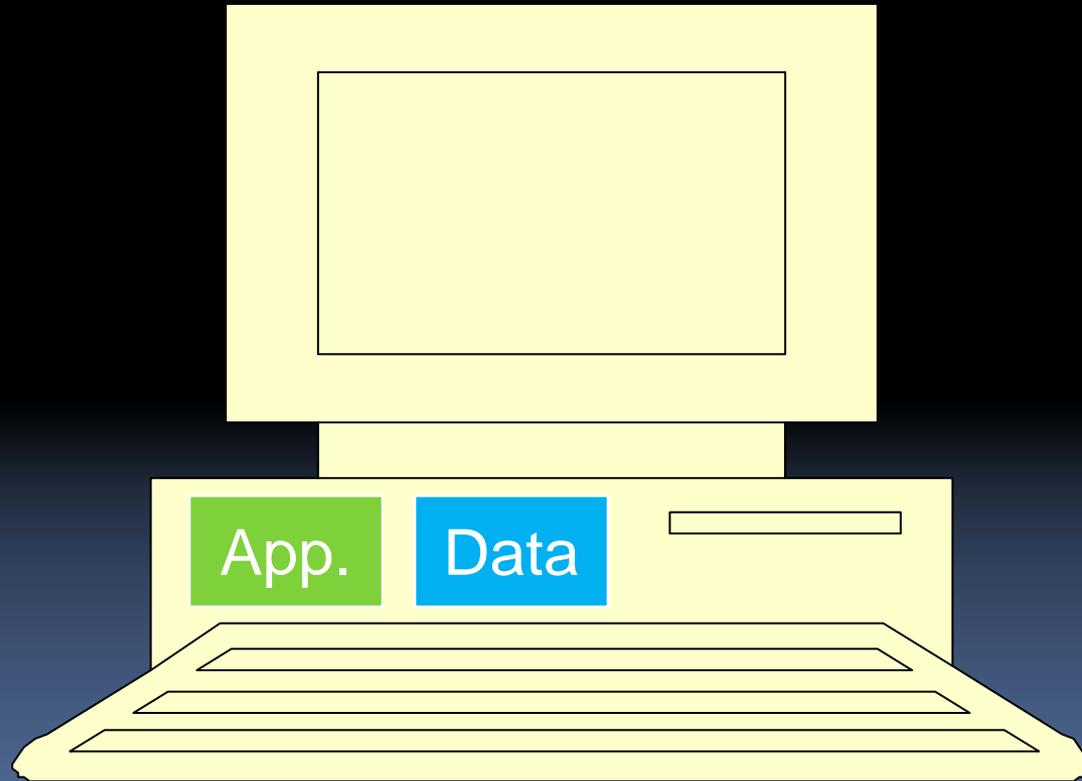
THE BIG SWITCH

a Wall Street Journal bestseller

His last book shook up the high-tech industry. Now, Nicholas Carr is back with The Big Switch, a sweeping and often disturbing look at how a new computer revolution is reshaping business, society and culture.

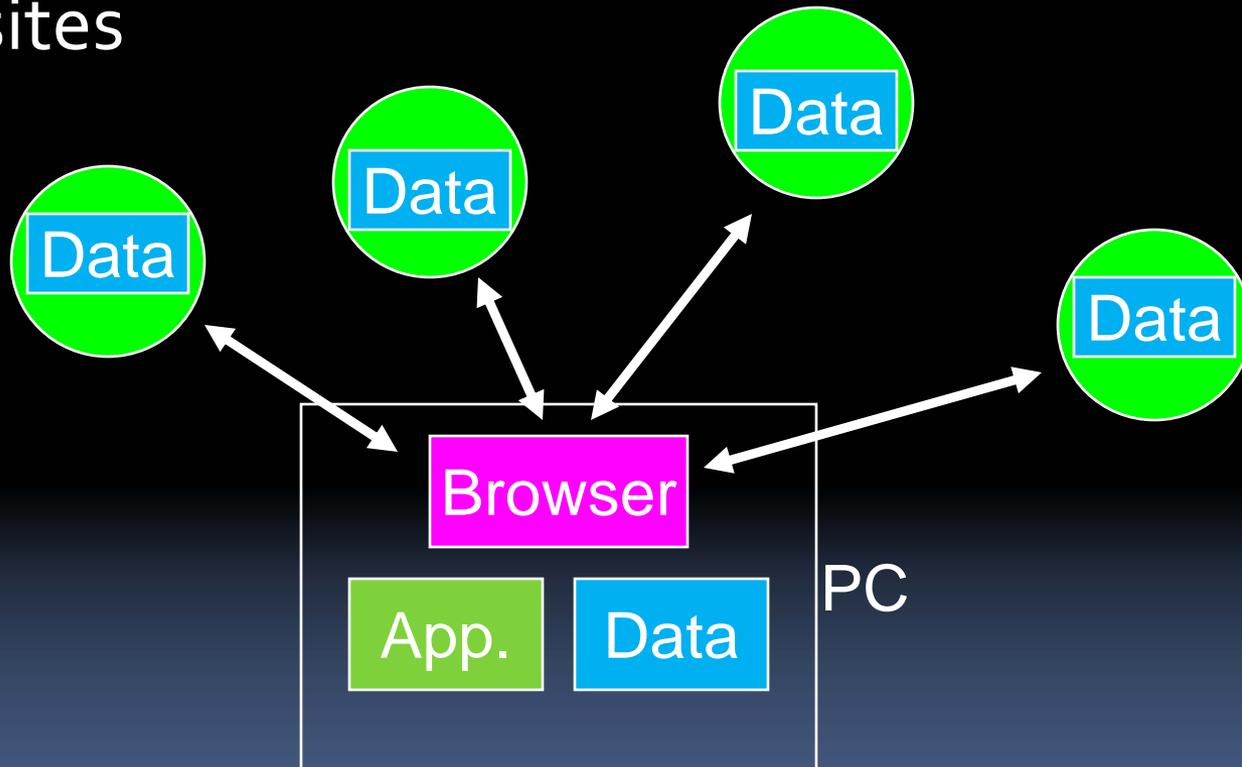
A hundred years ago, companies stopped generating their own power with steam engines and dynamos and plugged into the newly built electric grid. The cheap power pumped out by electric utilities didn't just change how businesses operate. It set off a chain reaction of economic and social transformations that brought the modern world into existence. Today, a similar revolution is under way. Hooked up to the Internet's global computing grid, massive information-processing plants have begun pumping data and software code into our homes and businesses. This time, it's computing that's turning into a utility.

Phase One – Stand Alone Computer

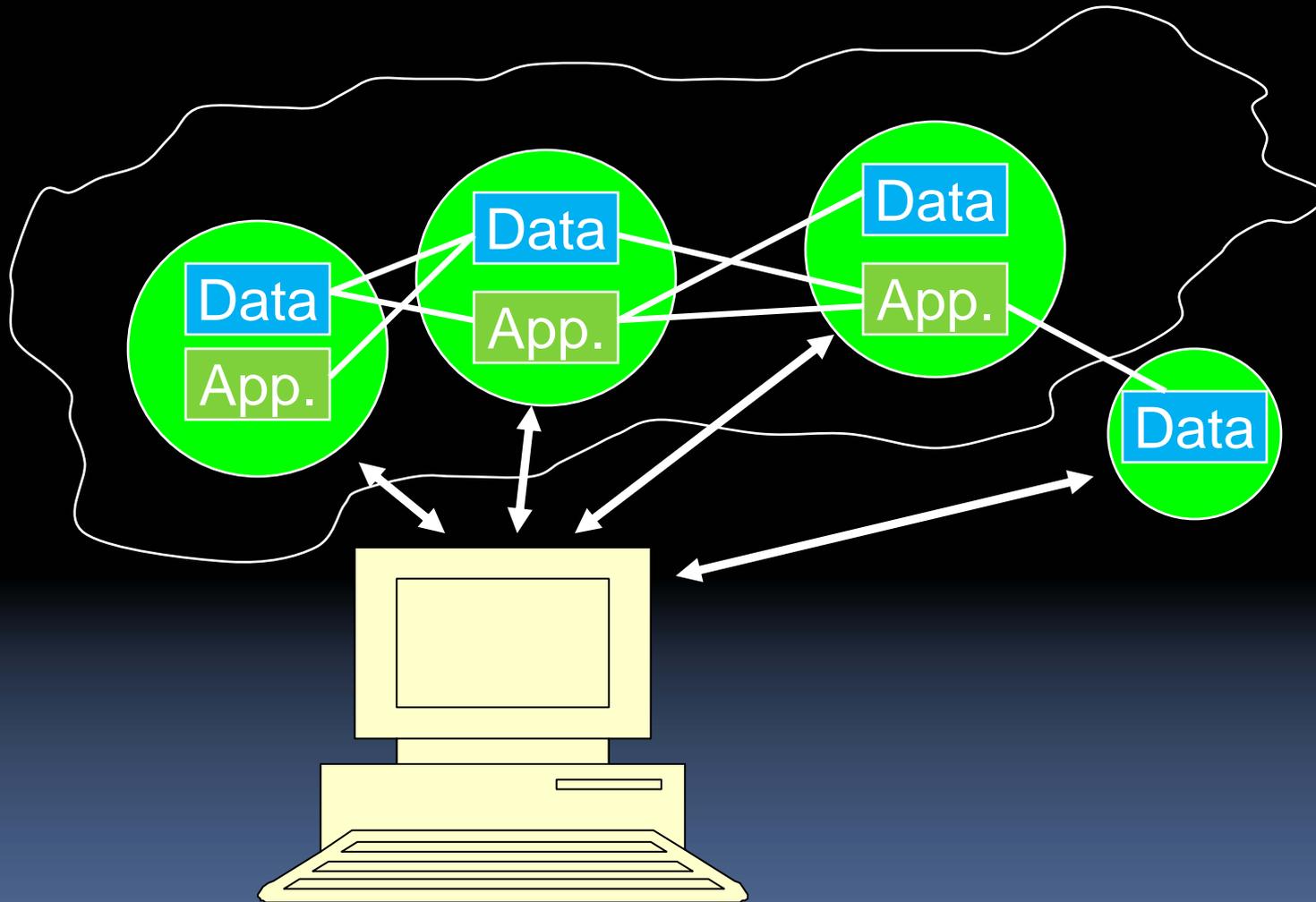


Phase Two – The Web

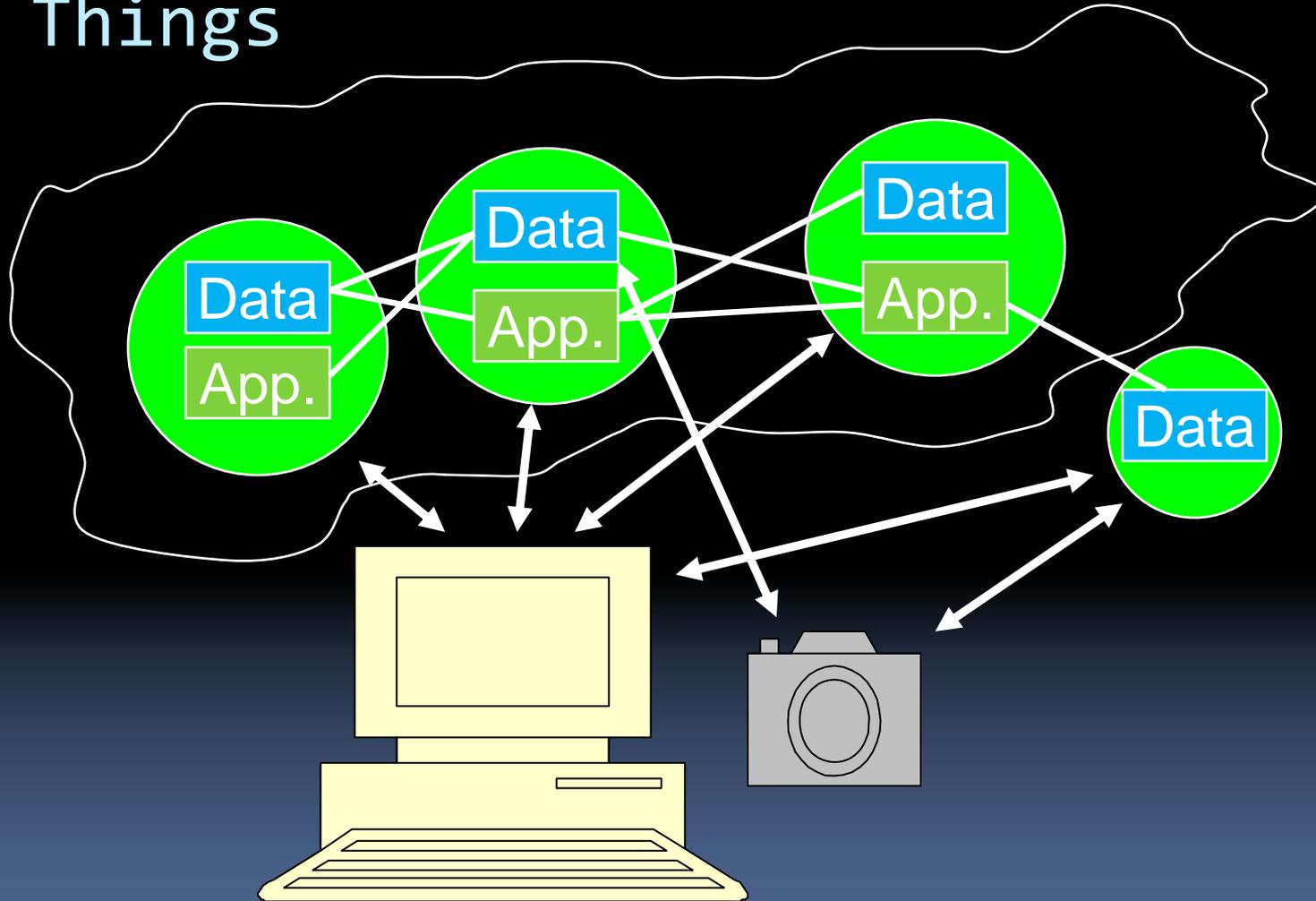
Web sites



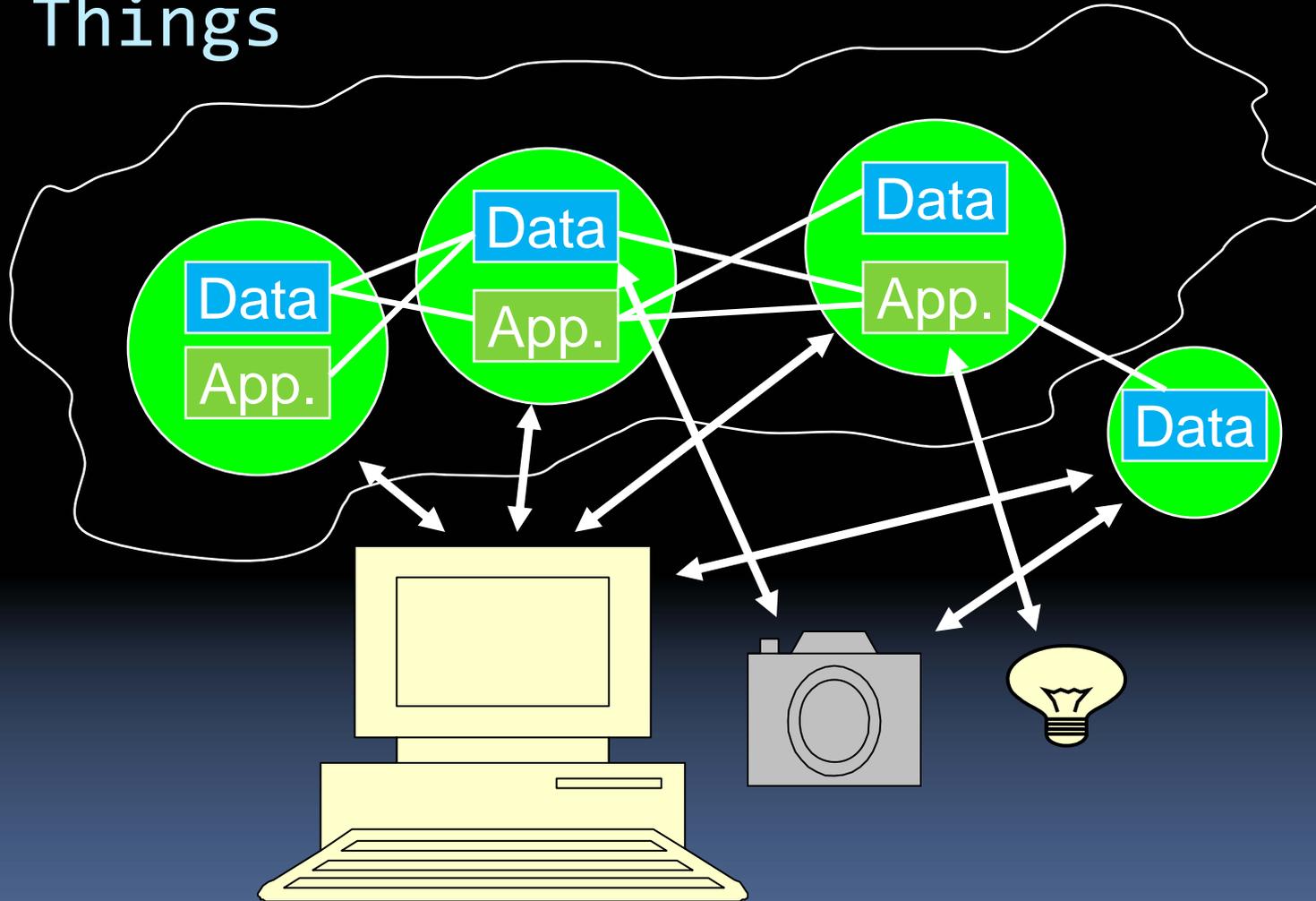
Phase Three – The Cloud



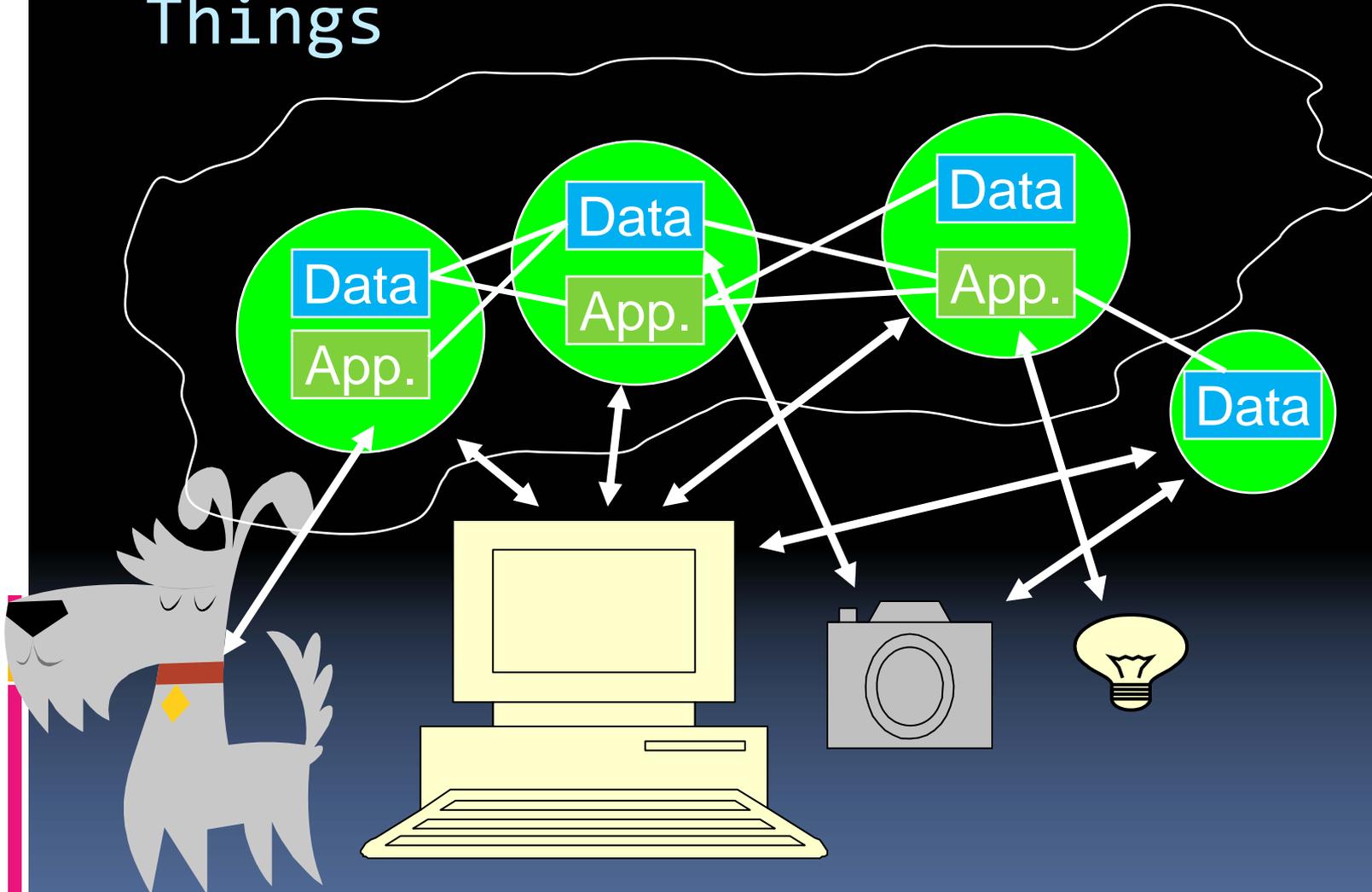
The Cloud + The Internet of Things



The Cloud + The Internet of Things

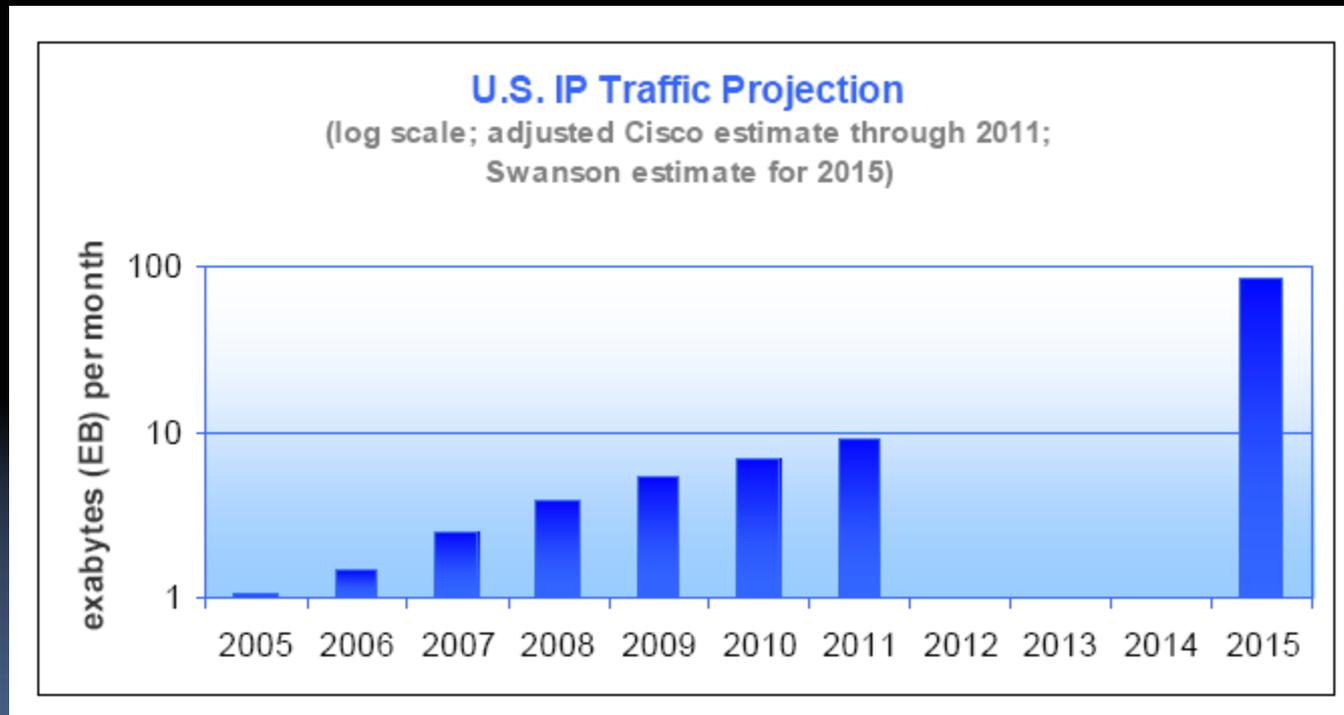


The Cloud + The Internet of Things



Estimating the Exaflood

(Swanson and Gilder, 2008)



What's in the Exaflood?

Rough estimate of annual U.S. IP traffic, by application, circa 2015

Movie downloads and P2P	100 exabytes
Video calling and virtual windows	400 exabytes
“Cloud” computing / remote backup	50 exabytes
Internet video, gaming, virtual worlds	200 exabytes
Non-Internet “IPTV”	100 exabytes, or more
Business IP traffic	100 exabytes
Other (phone, Web, e-mail, photos, music)	50 exabytes
total	1,000 exabytes = 1 zettabyte



BIG, Hairy Audacious Prediction #1

Within 5 years, 80% of all computing
and storage done worldwide could
happen “in the cloud”



Less Hairy Audacious Prediction #1

Within 5 years, 80% of all computing
and storage done worldwide could
happen “in the cloud”

(But it might take 10 years)



BIG, Hairy Audacious Prediction #2

Within 5 years, 100 BILLION devices
and sensors could be connected to
the Net



Less Hairy Audacious Prediction #2

Within 5 years, 100 BILLION devices
and sensors could be connected to
the Net

(But it might take 10 years)

Why Not?

- Technical
 - Agreement and adoption of key standards
 - IPv6, DNSsec, IPsec, Grid standards
- Business practices
 - Cooperation around open standards vs. proprietary lock-in; open source software
- Culture
 - Users have to learn to “trust the cloud”
 - CIOs and their teams have to adapt to new roles
- Policy

Updating policies for the Cloud

- Privacy
 - Search warrants, wiretapping in the Cloud?
- Transparency
- Online copyright
- Liability for cloud service providers
 - Who's responsible for Illegal activities?
 - Security breach legislation updated?
- International data flows
- Competition policy



Three Possible Futures

1. The Clouds Scenario
2. The Cloudy Skies Scenario
3. The Blue Skies Scenario

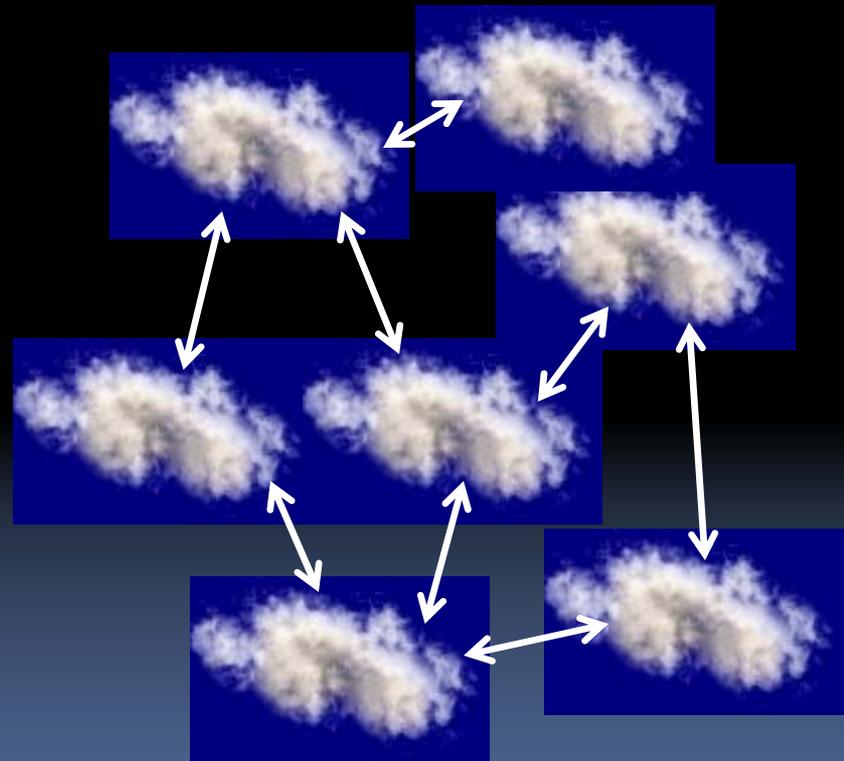
The Clouds Scenario

- Different, distinct, proprietary clouds
- Non-interoperable standards
- The cable television network business model; bottlenecks and monopolies



The Cloudy Skies Scenario

- Distinct clouds
- Interconnected
- Cloud applications aren't interoperable
- Little common middleware (e.g. no single sign-on)
- Lots of missed opportunities



Blue Skies Scenario

- A “cloud of clouds” like the network of networks
- Truly interoperable clouds services
- “Mix and match”
- Common middleware
- Seamless
- Almost infinite opportunities



Sky's the Limit!!

What Will Users Want?

- Lower Costs; More Competition and Choice
- Reliability
 - 0% downtime
 - Recovery of data
- Assurance of Security and Privacy
 - Of data
 - Of usage logs
- Transparent processes and audits
- Bill of Rights globally

What Will Everyone Want?

- Effective law enforcement—globally
- Protection against the “bad guys”
 - Terrorist videos
 - Collaboration and virtual worlds
 - Caches of stolen content (credit card data, IPR)
 - Denial of Service Attacks



Other interests

- Content owners – pay per view
- Repressive governments - control
- Telecom network providers – growth
- Cloud service providers – lock-in



Steps towards reconciliation?

- Open, interoperable authentication
- Open standards and open source middleware for the cloud >> Blue Skies scenario
- Immutable audits built in
- Encryption, anonymity built in
- Bill of Rights built in

TRUST AND ON DEMAND: ENABLING PRIVACY, SECURITY,
TRANSPARENCY, AND ACCOUNTABILITY IN DISTRIBUTED SYSTEMS

M. R. Nelson, M. Schunter, M. R. McCullough, and J. S. Bliss, TPRC, 2005



1) Privacy Notice



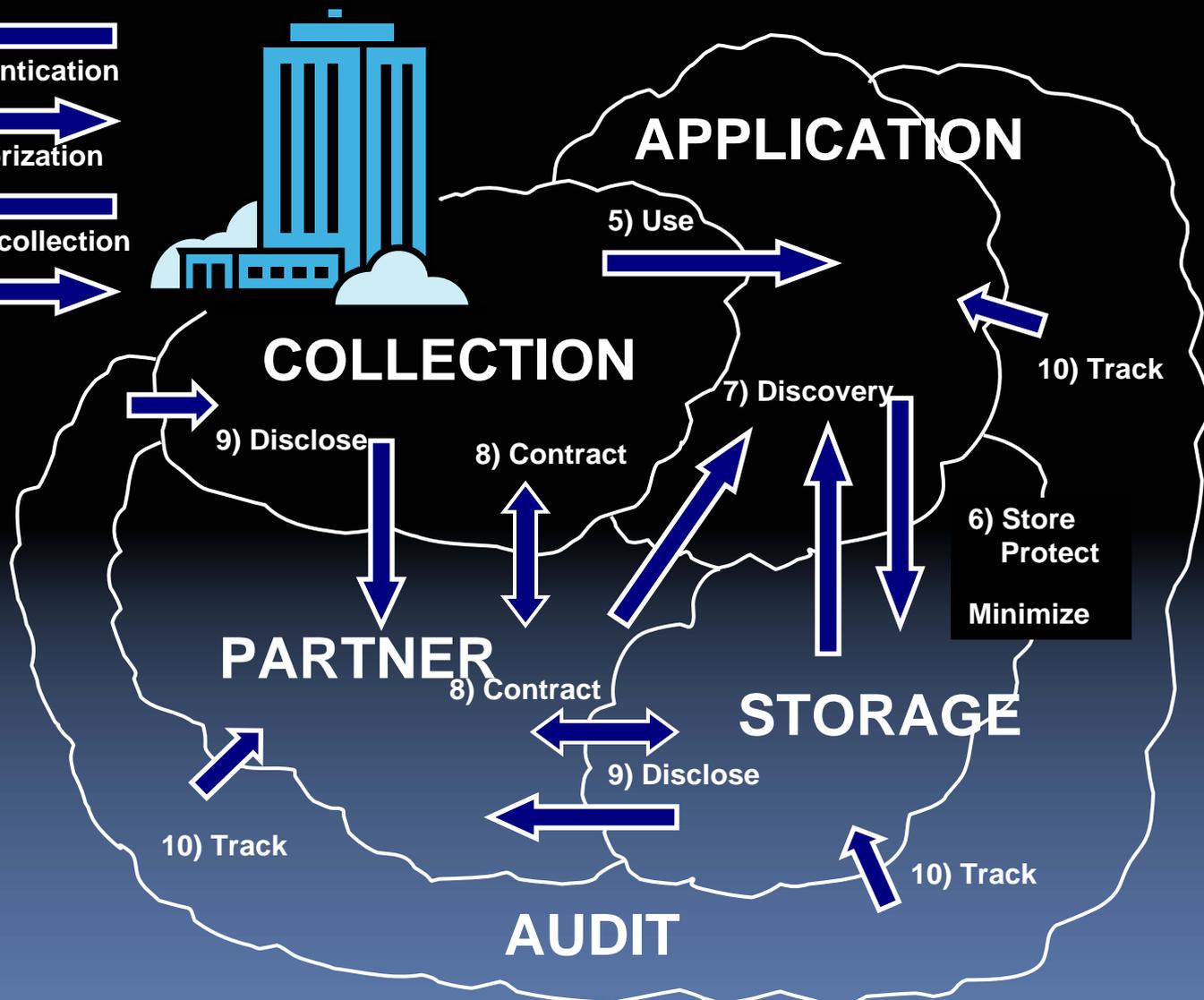
2) Authentication



3) Authorization



4) Data collection



Possible Futures





Conclusions

- The Internet Revolution will be as disruptive as the printing press, but:
 - Much faster
 - Totally global
 - More unpredictable
- We have 2-3 years to create the right framework for the Cloud
- When in doubt, empower the user!

Challenges in International Cyber Security

NDU Conference, 29 April 2009

Defining Responses to Cyber Incidents: Legal Frameworks

Maeve Dion

Center for Infrastructure Protection
George Mason University School of Law

Think. Learn. Succeed.



Defining Responses to Cyber Incidents

Jurisdictions for Response

Criteria for Action / Decision

Frameworks for Criteria Definition

Mapping Jurisdictions (Situational Awareness)

Think. Learn. Succeed.



Slide 2:

Overview:

Focus of this presentation is on national security thresholds in peacetime: not conflicts management or armed conflict.

Jurisdictions for Response

Swine Flu

- Hospital / Clinic
- State Health / HS
- Federal Health / HS
- International: WHO
- Quarantine Authorities
- Intelligence Community
- Law Enforcement
- Foreign Policy

Cyber Incident

- Corporation / Agency (network / system security)
- Federal HS ('cyber-related' incident of national significance)
- Military (conflict mgt, armed conflict)
- IC, LE

Think. Learn. Succeed.



Slide 3:

Jurisdictions for Response

Depending on the severity and scope of a cyber incident, various jurisdictions may respond (business/corporate security, LE, IC, state dept, military, etc.).

Compare to **health incident (H1N1/swine flu)**

- Hospital/Clinic
- State Health & Homeland Security Offices
- Regional Coordination & Cooperation
- Federal Health & Homeland Security Offices
- World Health Organization
- Quarantine Authorities
- Intelligence Community (e.g., if cause of health incident was unknown; maybe malicious? threats?)
- Law Enforcement (malicious? evidence?)
- Also, there is a role for Foreign Policy / State Department, balancing policy and economic considerations regarding travel advisories, etc.

For a health incident, each of these jurisdictions **has criteria/thresholds for action/decision.**

For Cyber Incidents, there are **no similar frameworks** for each jurisdiction's criteria/thresholds for action/decision.

Criteria for Action / Decision

Military (conflict mgt, armed conflict)

Federal HS (NRF)

- ESF #2, Cyber Incident Annex, NPTS
- Criteria:
 - ESF #2 activated “when a significant impact . . . is expected or has occurred”
 - Cyber Incident Annex procedures “are implemented when . . . a cyber-related Incident of National Significance is imminent or underway”

Think. Learn. Succeed.



Slide 4:

Criteria for Action / Decision

Military (conflict management, armed conflict) analysis will be discussed by another panelist. It is important to note that an armed attack determination is sort of the ultimate in response, and is a **situation that's actively avoided by malicious actors** – they want to stay below that threshold in order to limit military involvement in response.

Federal Homeland Security / National Response Framework

Emergency Support Function #2 – Communications, and the NRF Cyber Incident Annex, support the National Plan for Telecommunications Support in Non-Wartime Emergencies. For NRF Cyber Incident Annex: “Procedures . . . are implemented when it is determined that a cyber-related Incident of National Significance is imminent or underway.” ... “The Cyber Incident Annex outlines the provision of Federal cyber incident response coordination among the Federal departments and agencies and, upon request, State, tribal, local, and private-sector entities in response to any incident induced by cyber means (e.g., significant cyber events, technological emergencies, and Presidentially declared major disasters and emergencies that threaten, disrupt, or cripple communications and IT services or degrade other essential infrastructures).” ... “DHS/Federal Emergency Management Agency (FEMA) activates ESF #2 when a significant impact to the communications infrastructure is expected or has occurred” .. Under ESF #2 / NRF Cyber Incident Annex implemented, the interagency response process includes NCRGC, IC-IRC, JTF-GNO, etc.

There are **no delineated criteria for determining levels of response/protocol escalation** (contrast with criteria used by doctors, state health/HS offices, WHO, etc., in health incident). There is no clearer definition of a ‘cyber-related’ incident of national significance.

What are the criteria for this? Are we OK with “we’ll know it when we see it?”

NOTE: Any **cyber-related Incident of National Significance will likely be an incident of INTERNATIONAL significance**. What’s the importance of having the criteria recognized in the international arena as valid criteria? E.g., earlier panel – what’s internationally recognized as “sufficient evidence” of attribution for different levels of response (State Dept pressure vs. military pressure).

Criteria for Action / Decision

Corporation / Agency

- Block / wall-off bad traffic / equipment
- Switch to back-up systems
- Implement full COOPs
- Communicate w/ colleagues
- Communicate w/ customers
- Communicate w/ govt

Think. Learn. Succeed.



Slide 5:

Criteria for Action / Decision (continued)

At a lower level, there are examples of internal network security (corporations, agency, etc., in 'best case scenario') criteria for response. A corporation has criteria for deciding when to merely unplug one buggy computer and re-route data/processes, versus switch the whole network to the back-up system to debug the main system. There are stages of a business's continuity of operations plans, only some of which may need to be implemented depending on the requisite level of response to the scope/severity of the disaster/incident. These decisions are made based upon facts, criteria, and **pre-determined thresholds of decisionmaking**. A business may have criteria of when to communicate network degradation/damage to customers. There are state laws which may require entities to communicate notification of data breaches. These all are based on **some criteria at which the threshold for communication or notification** have been met.

Much of this decisionmaking and criteria-setting is properly the purview of the corporation. Except for when the system/asset is vital to U.S. homeland security/national security.

E.g., for vital systems/assets, what are the criteria for reporting incidents or vulnerabilities? To whom is it shared? Does the U.S. government have a clear understanding of the voluntary vs. mandatory (regulated) status of information sharing?

Note that for internal network security, there is no national (or international) perspective regarding threats/vulnerabilities – that's properly the responsibility of Government. Who is responsible for situational awareness of potential cyber incidents of national consequence – throughout the whole phase of consideration (not just when it reaches the point of 'we know it when we see it') --? [comment on IC vs DHS; calls for higher position in White House].

Frameworks for Criteria Definition

Identification of Criteria

Map Response Decisions to Criteria (decision tree)

Legal Frameworks

- National
 - Cyber Crimes
 - Conflict Management / Armed Conflict
- International
 - Law of the Sea, Outer Space, Satellites, Telecommunications
- FICS initiative

Think. Learn. Succeed.



[transition from prior slide:] AND beyond military, Federal HS/NRF, and Corporation/Agency, what are the criteria for other potential jurisdictions for response in the context of a cyber incident? Example: State department decision-making (foreign policy pressure)?

Slide 6:

Frameworks for Criteria Definition

First Step: **Identify the Criteria** with which we'll be making our decisions. Second Step: **Map the various options/decisions** of Response to the criteria. Note that the criteria may be different within jurisdictions (e.g., IC vs LE), based upon the data required (by law, policy, custom, etc.) to make the decision. Some decisions may require activity across jurisdictions (which may thus require additional criteria/data sets in order to justify cooperation across jurisdictions). There may be various criteria/requirements for foreign/international assistance or cooperation.

Some scholars are looking at **existing legal frameworks to help identify criteria & map responses** (e.g., national crimes under the Computer Fraud & Abuse Act, the law of the sea, international agreements regarding outer space or telecommunications). BUT these do not necessarily help, for example, in determining the criteria for incident reporting to Homeland Security/National Security entities; or the escalation criteria for implementing the NRF Cyber Annex and ESF #2; or any other HS/NS decision-making jurisdiction outside of the context of armed conflicts/conflict management.

Another approach is the FICS initiative [see next slide 7].

FICS

Frameworks for International Cyber Security

Criteria

- Is there a military response?
- Is there a foreign relations response?
- Is there a law enforcement response?
- Is there a regulatory response?
- Is there a corporate response?
- Is international assistance / coordination required?
- Is there an IC response?

Think. Learn. Succeed.



Slide 7:

Frameworks for International Cyber Security (FICS)

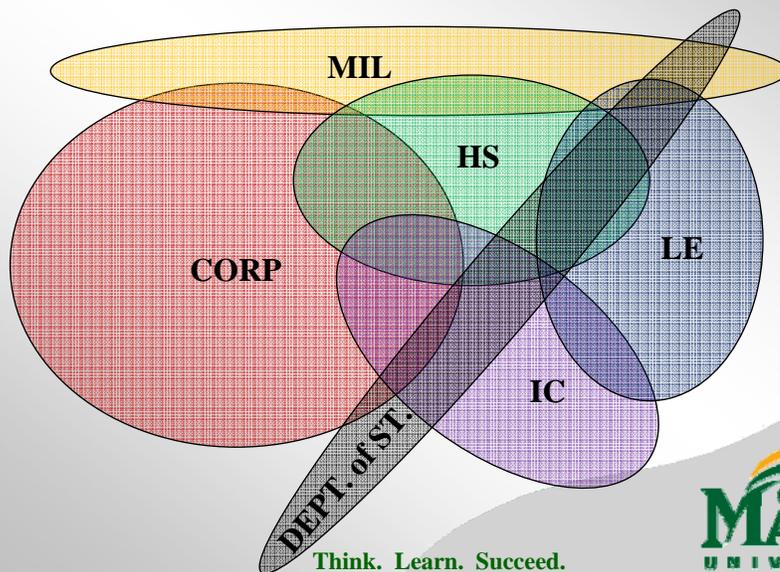
This initiative is a cooperative effort among faculty at GMU CIP, NDU, NPS, Army Command & Staff College, and the NATO-accredited Cooperative Cyber Defence Centre of Excellence. This group regularly consults with other scholars, policy-makers, businesses, emergency response & defense personnel, etc., so that the FICS initiative provides useful, operational tools, in addition to the policy/theory that underlies the decisionmaking.

The FICS initiative is looking at a **Framework for determining Military Response** – the Schmitt Analysis – which identified 7 qualitative criteria for determining how military coercion differs from other kinds of coercion (e.g., diplomatic or economic) in regard to information operations. The FICS researchers are planning to take a similar approach to the other jurisdictions to identify qualitative criteria for response/coercion during cyber incidents. [see questions on slide 7]

Ideally, this initiative will help to develop tools to assist in quantitative decisionmaking as well. E.g., automated decisionmaking rule sets built into distributed networks for inter-jurisdictional cyber incidents – i.e., for basic-level decisions (not major decisions involving human judgment) of information sharing, alerts, etc.

We hope to approach NSF with a funding proposal this summer.

Mapping Jurisdictions (Situational Awareness)



Slide 8:

Mapping Cyber Jurisdictions (Situational Awareness)

This was sketched at the most recent FICS workshop.

- Is this even useful? Will it help to visualize the jurisdictions, help to determine criteria?
- What should it look like?
- What are the conflicts?
- What are the grey areas?
- What are the needs for international collaboration? Who has the lead?

SAVE THE DATE

**Frameworks for International Cyber Security:
A Legal & Policy Conference**

9-11 September 2009

Tallinn, Estonia

Organizers:

Center for Infrastructure Protection, George Mason

NATO-accredited Cooperative Cyber Defence
Centre of Excellence

Think. Learn. Succeed.



Registration information coming soon to www.ccdcoe.org

Sponsorship opportunities are available.

Center for Infrastructure Protection

Maeve Dion

Think. Learn. Succeed.



NATO's Perspective on Cyber Defence

Major General Koen Gijsbers
ACOS C4I, Dutch Army
Allied Command Transformation

**ALLIED
COMMAND
TRANSFORMATION**

A new day ahead. A new way ahead.

23 APRIL 2009



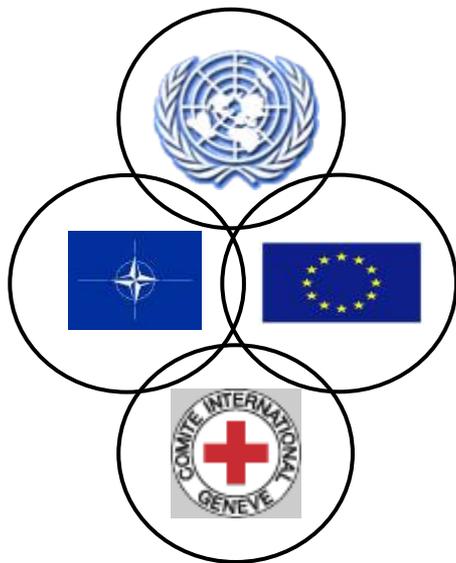
The Cyber Challenge



- **Assured access to reliable information**
- **Attacks against critical infrastructure**
- **Increasing sophistication of potential adversaries – nations, non-nation state actors, organised crime, and empowered individuals**
- **Lack of international agreements**
- **Global security issue**
- **Hybrid threat with fractured responsibilities**



The Cyber Challenge For NATO



- **NATO has not agreed to whether a cyber attack is an Article 5 “attack”**
- **Increased vulnerability due to expeditionary operations**
- **Complex array of cyber defence responsibilities within Alliance nations**
- **Requirement to operate alongside and with International Organizations**
- **No single actor who can “see” the cyber threat - or link Alliance cyber defence capabilities**



Cyber Defence Efforts in NATO



- **Strategy**
 - Strategic Cyber Defence
 - International Cooperation / Coordination
- **Operations**
 - Cyber Defence Exercises
 - Training and Awareness
- **Organization & Resources**
 - NATO Computer Incident Response Capability
 - Cyber Defence Management Authority
 - Cooperative Cyber Defence Centre of Excellence



Cyber Defence Efforts in NATO – What's Next



- **New Strategic Concept: Delineate cyber defence roles of NATO and Nations**
- **Expand NATO's cyber defence capability**
- **Implement cyber events into military exercises**
- **Coordinate & implement national best practices through the cyber defence Centre of excellence**
- **Field a Command & Control reference capability – Stress / attack the NATO reference system for vulnerabilities**





Key Challenges

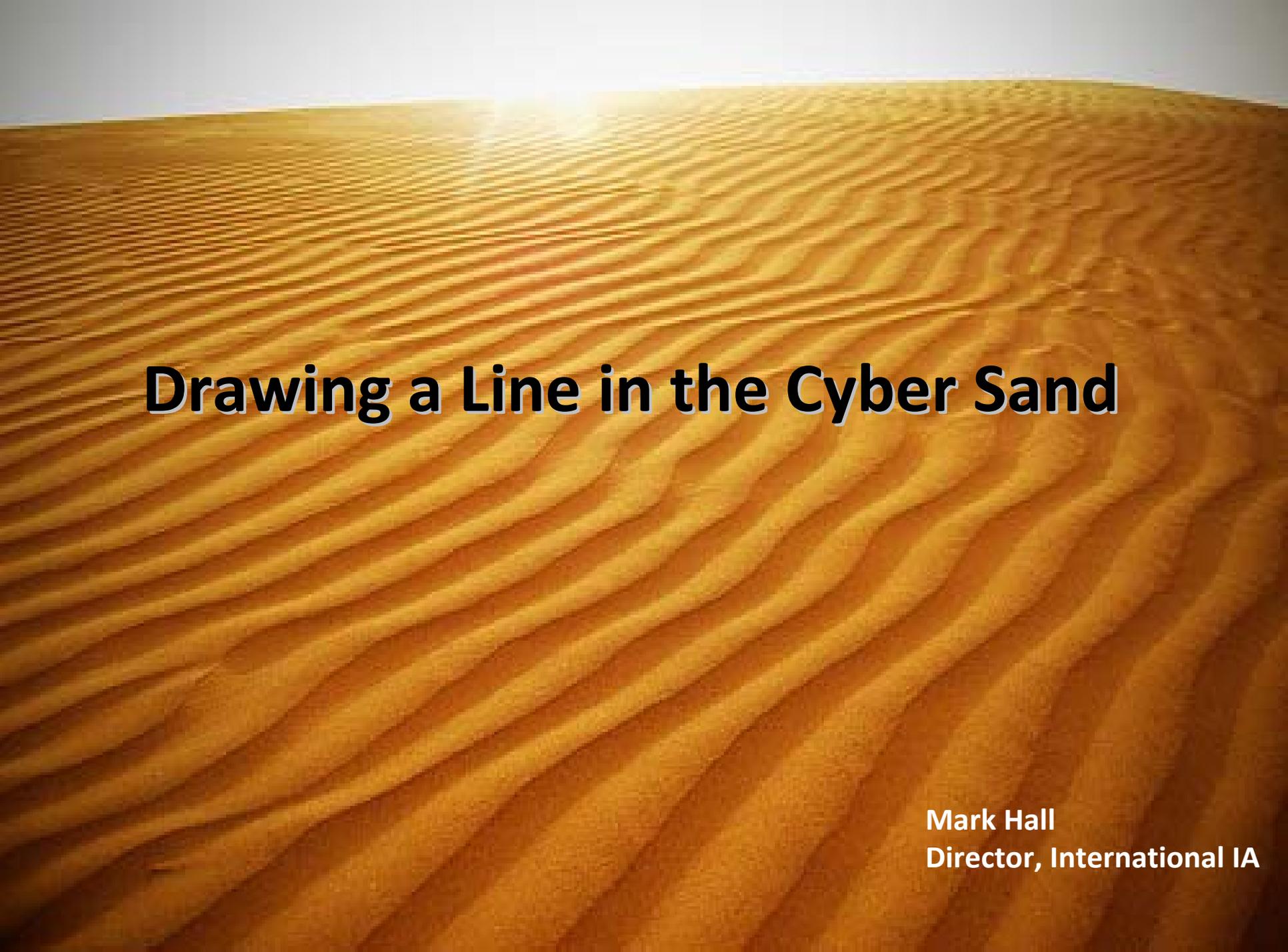


- **Delineating NATO and National responsibilities**
- **Building sufficient maturity in Member Nations' Emergency Response Teams**
- **Resolving International Law issues**
- **Countering a sustained attack**
- **Integrating / harmonizing Civil and military responsibilities and capabilities to this Hybrid threat**
- **Operationalizing a Global Perspective**



NATO's View of Cyber Defence

Questions?

A vast desert landscape with rolling sand dunes under a bright sun, serving as a metaphor for the digital world. The dunes are golden-brown and have a rhythmic, wavy pattern. The sun is low on the horizon, creating a strong glow and long shadows.

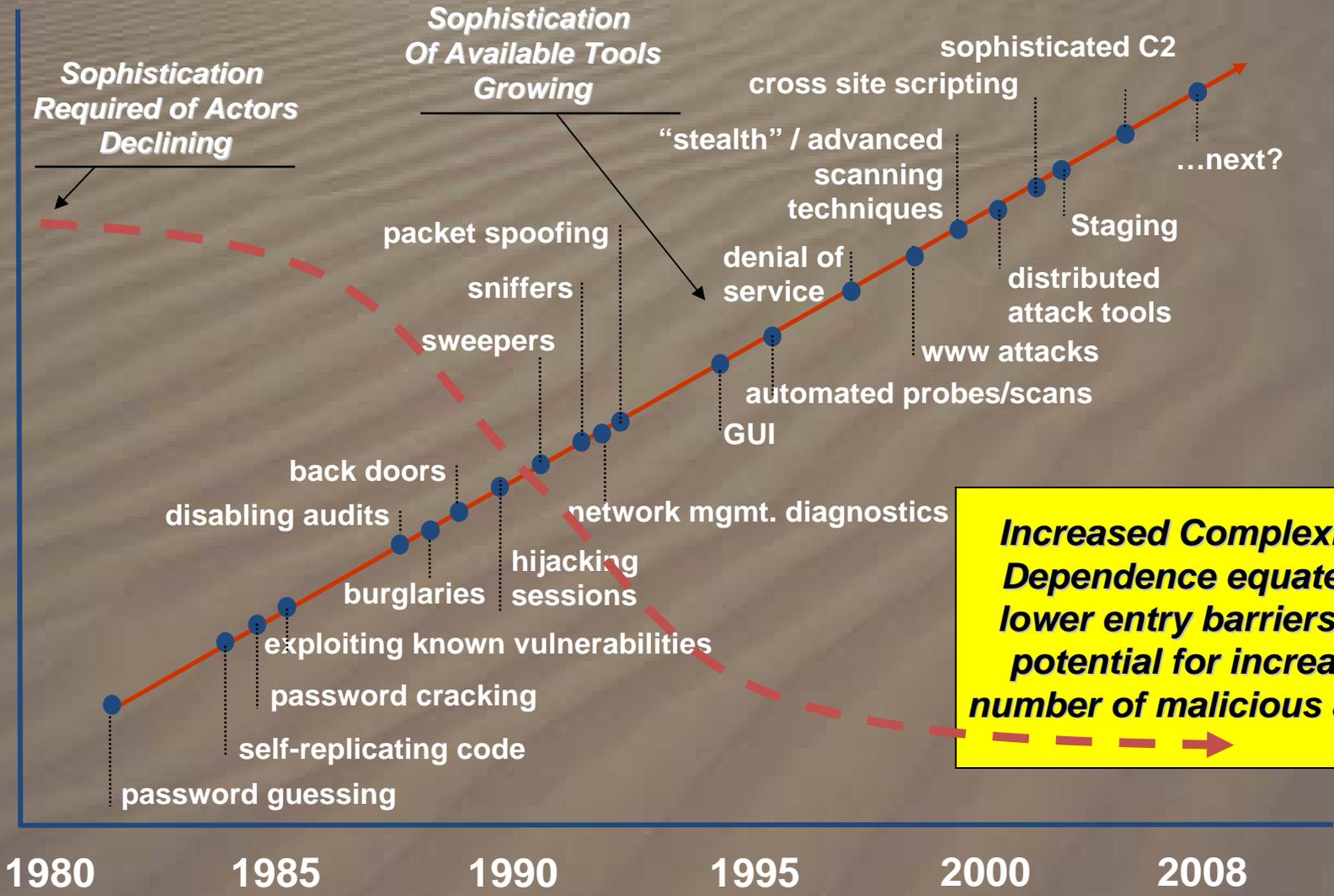
Drawing a Line in the Cyber Sand

Mark Hall
Director, International IA

High

Sophistication

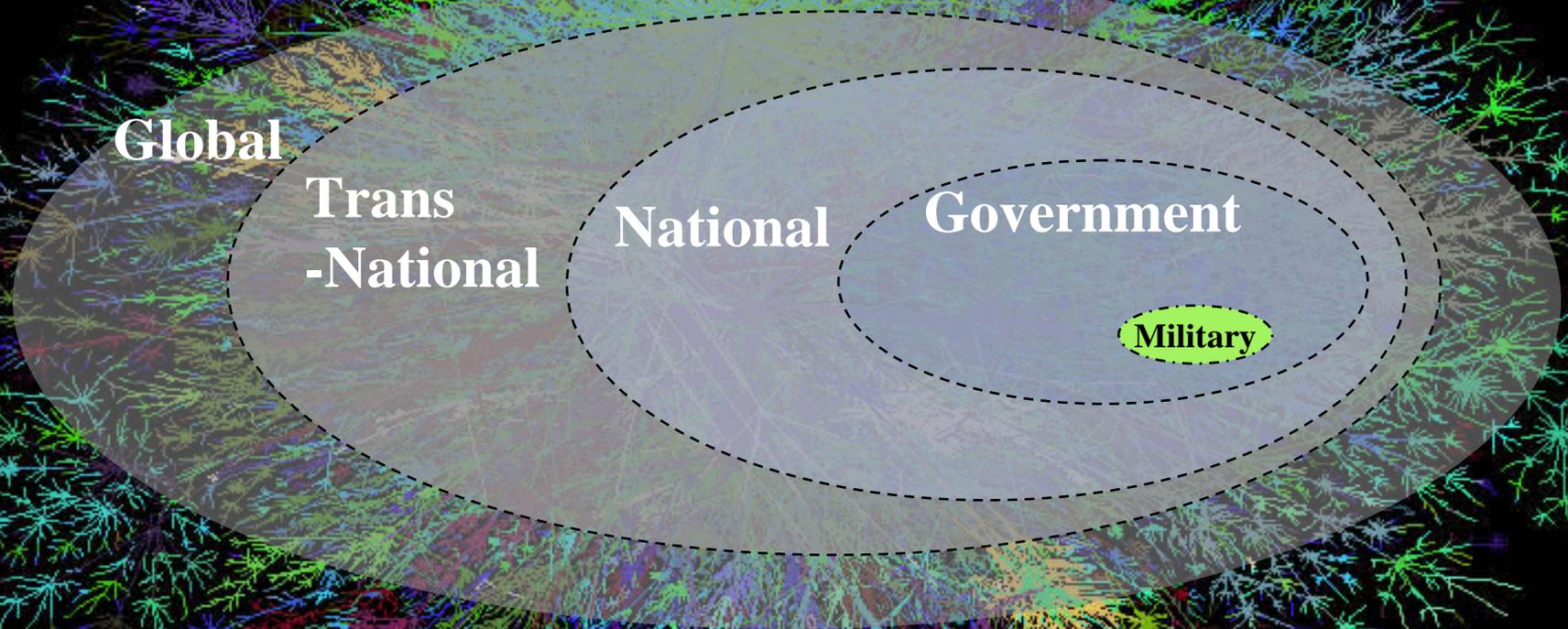
Low



Increased Complexity & Dependence equates to lower entry barriers and potential for increased number of malicious actors

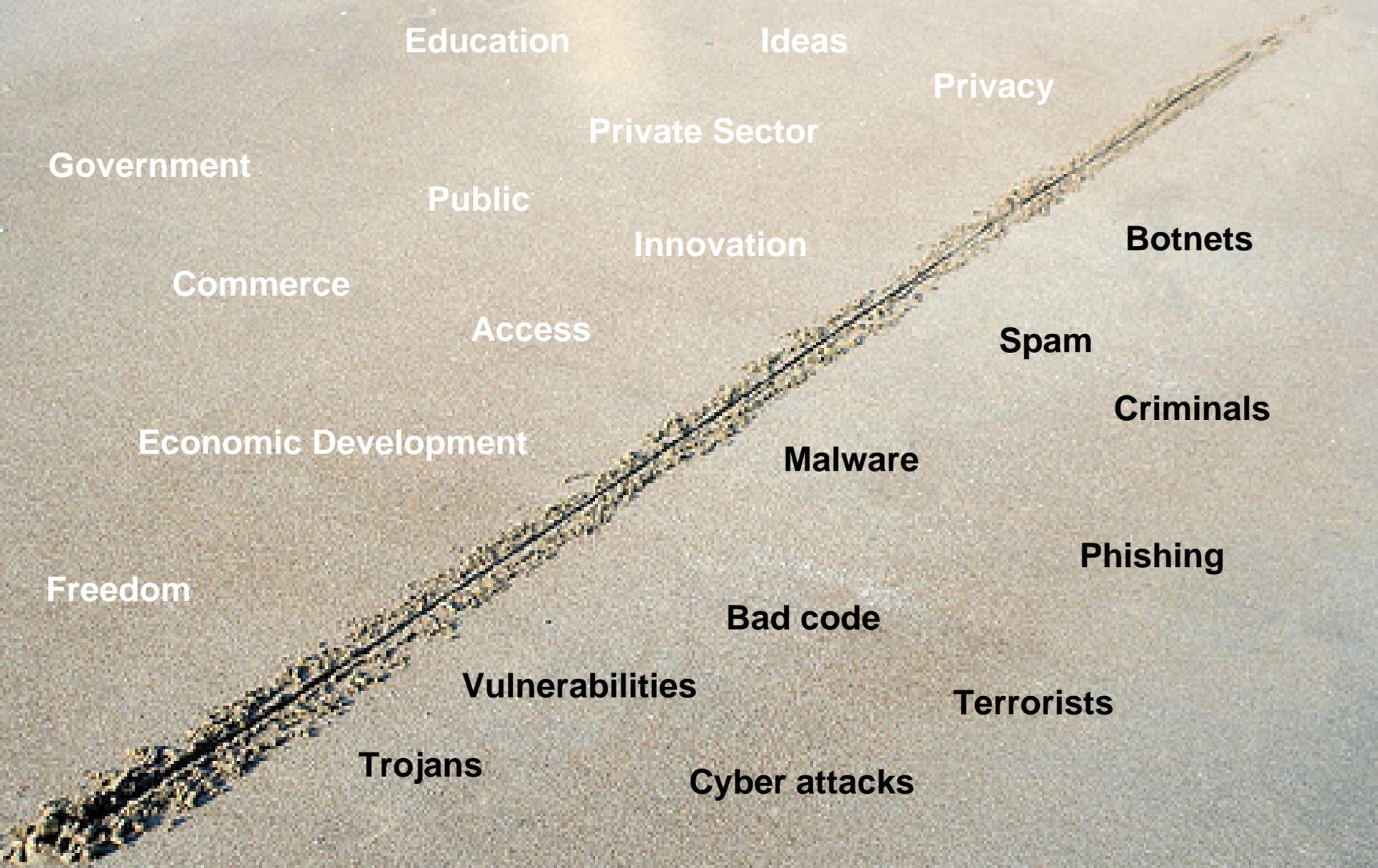
Global Information Infrastructure

We are part of a Global Information Infrastructure



Threats & vulnerabilities are common across national and international boundaries, and between the public and private sector

There are no recognized lines in cyber sand



Education

Ideas

Privacy

Government

Private Sector

Public

Innovation

Botnets

Commerce

Access

Spam

Economic Development

Malware

Criminals

Freedom

Phishing

Bad code

Vulnerabilities

Terrorists

Trojans

Cyber attacks

How do we draw The Lines?

- **Lines should be widely accepted by both the victim and the international community**
 - Shared perception and standards for hostile or malicious activity
- **Do multiple lines exist (international, commercial and sovereign)?**
- **Who is responsible for monitoring the lines?**
 - Do we need/want broad multinational surveillance of cyberspace?
- **Who enforces breaches?**
 - National gov't, LE, Mil, Int'l body, private sector
 - Do we need a World Cyber Court?
- **Recommendation: Implement a phased approach**
 - Phase 1: Secure the Global Commons
 - Phase 2: Address nation-state cyber actions as part of the larger deterrence dialogue

Phase 1: Secure the Global Commons

Recognize that it is in the interest of all peaceful nations to have an accessible, reliable, and secure means to conduct business, exchange ideas, and prosper in cyberspace

- 1. Develop internationally accepted norms of behavior; focus on low- to medium-level threats in order to reduce the noise level**
 - Phishing, botnets, viruses, key-stroke loggers, spam, and other malware**
 - Bi-lateral, multi-lateral, international standards**
- 2. Develop common international laws and robust national laws-- each nation must be responsible for managing their corner of cyberspace**
- 3. Create national processes and capabilities to enforce these laws and standards of behavior**
 - Consider building capacity for some nations and utilizing agreements with international carriers**

Phase 1: Secure the Global Commons (con't)

4. **Partner closely with the Telecom's and ISP's as they are integral to achieving success**
 - Requires worldwide coordination

5. **Increase partnerships with product and software providers to increase the security of new offerings**
 - Share best practices and provide ways for smaller firms to enter the market

6. **Address anonymity on a global scale**
 - Escalating authentication as privileges or activity across the net changes
 - Work with civil liberties and privacy community to find acceptable solutions that allow both private and public internet behavior

7. **Address these norms through all educational levels**
 - Integrate individual responsibility when teaching technology
 - Specialized training for H/W and S/W developers (licenses?)

Phase 2: Address nation-state actions as part of the larger deterrence dialogue

- **If we have agreed to clean up cyberspace as described in Phase 1, should cyberspace have different rules for offensive actions taken by nations?**
 - **What are the pros and cons**
- **Discussion**

A wide-angle photograph of a desert landscape featuring rolling sand dunes. The dunes are covered in fine, rhythmic ripples that create a textured, undulating surface. The sun is positioned high in the sky, slightly to the left of the center, casting a bright, warm glow over the scene and creating a lens flare effect. The overall color palette is dominated by warm, golden-yellow and orange tones, with a clear, pale blue sky at the top.

Questions for the panel?



CHALLENGES IN INTERNATIONAL CYBER SECURITY

Center for Technology and National Security Policy
National Defense University

Harry D. Raduege, Jr.

Lieutenant General, USAF (Ret)

Chairman, Center for Network Innovation

Deloitte & Touche LLP

April 30, 2009

Coalescing International Cyberspace Governance

- Words Are Important
- Building National Governance
 - DoD & Others
 - Authoritative vs. Distributed Structures
 - CSIS Cybersecurity Commission
 - 60 Day Assessment
- International Coalescence
 - “Age of Interdependence”
 - Back to Basics
 - Who
 - Why
 - What
 - When
 - How

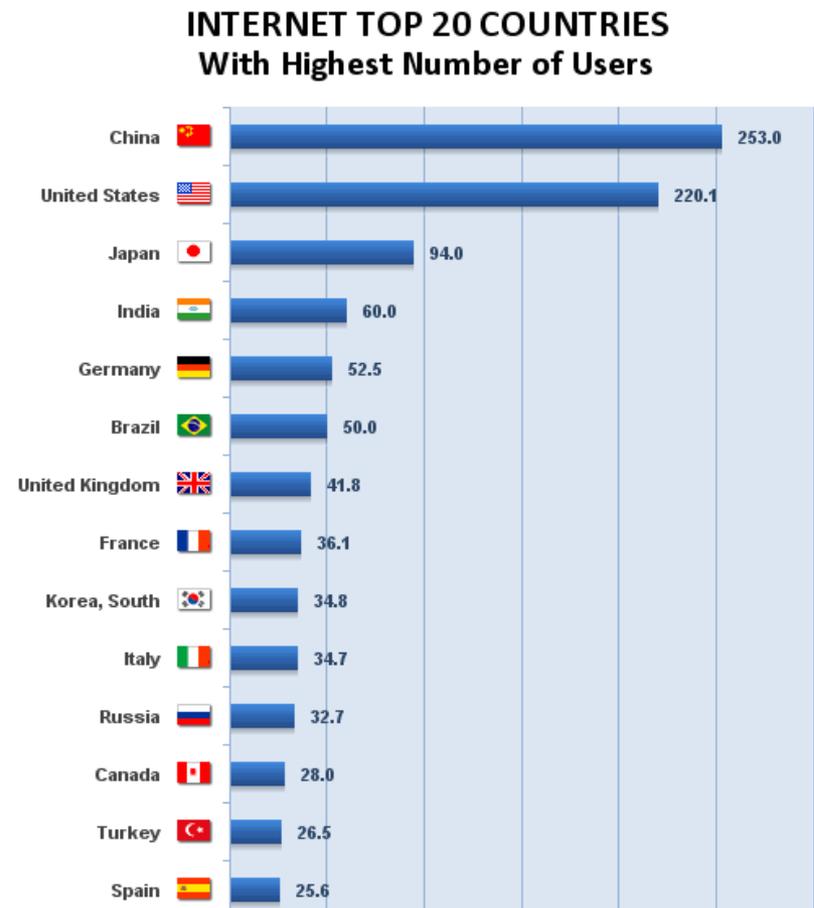
India: Country Perspective on Cyber Security

Nandkumar Saravade, Indian Police Service
(Ret'd)

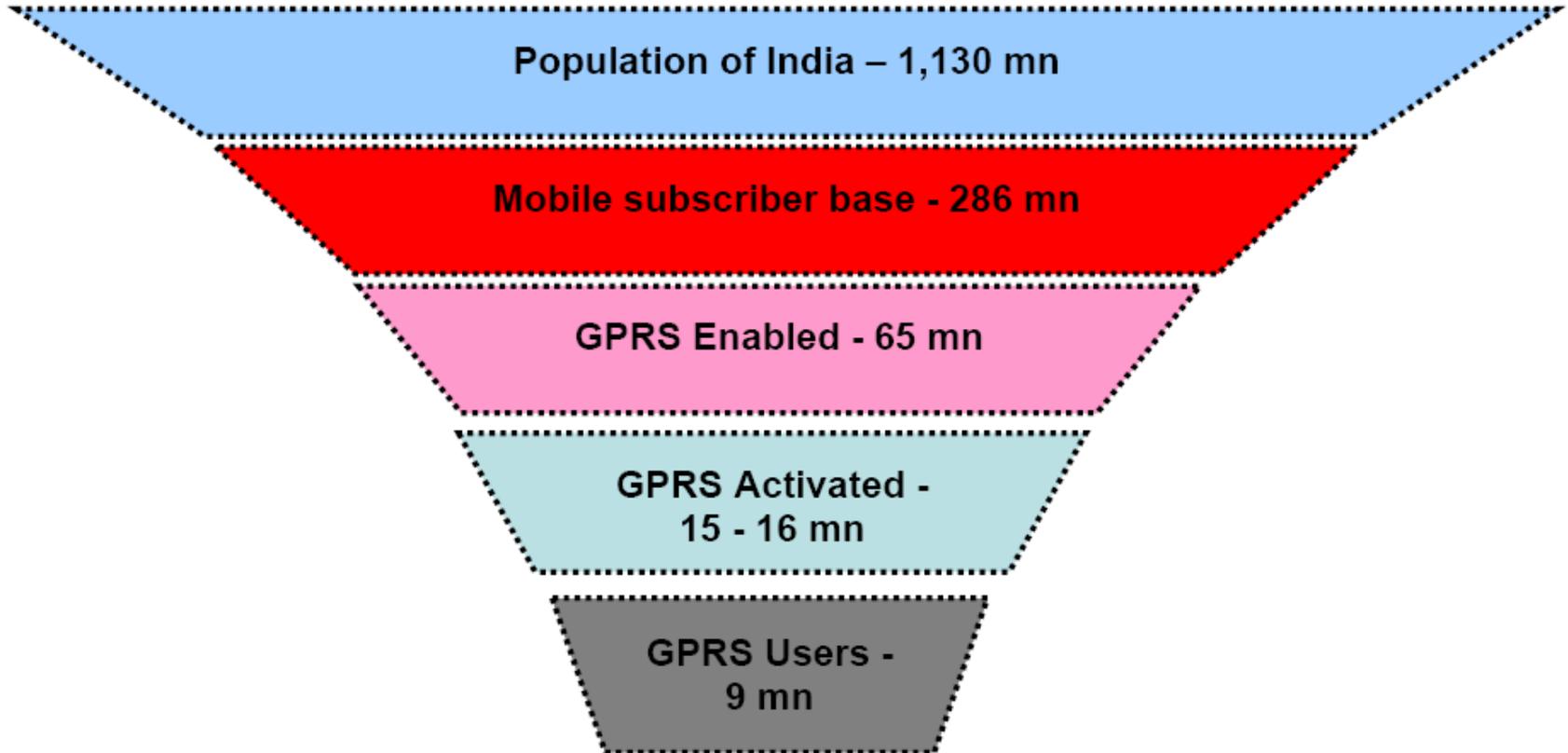
Internet penetration in India

- Internet growth in India
 - Penetration: 5.2% compared to 73% in US/Japan and 19% in China
 - Growth rate: 1100%
- Mobile phones (March, 2009)
 - User base: 392 million
 - Added during the month: 15.6 million
- Broadband: 6.2 million

(Source: Internet World Stats & TRAI)

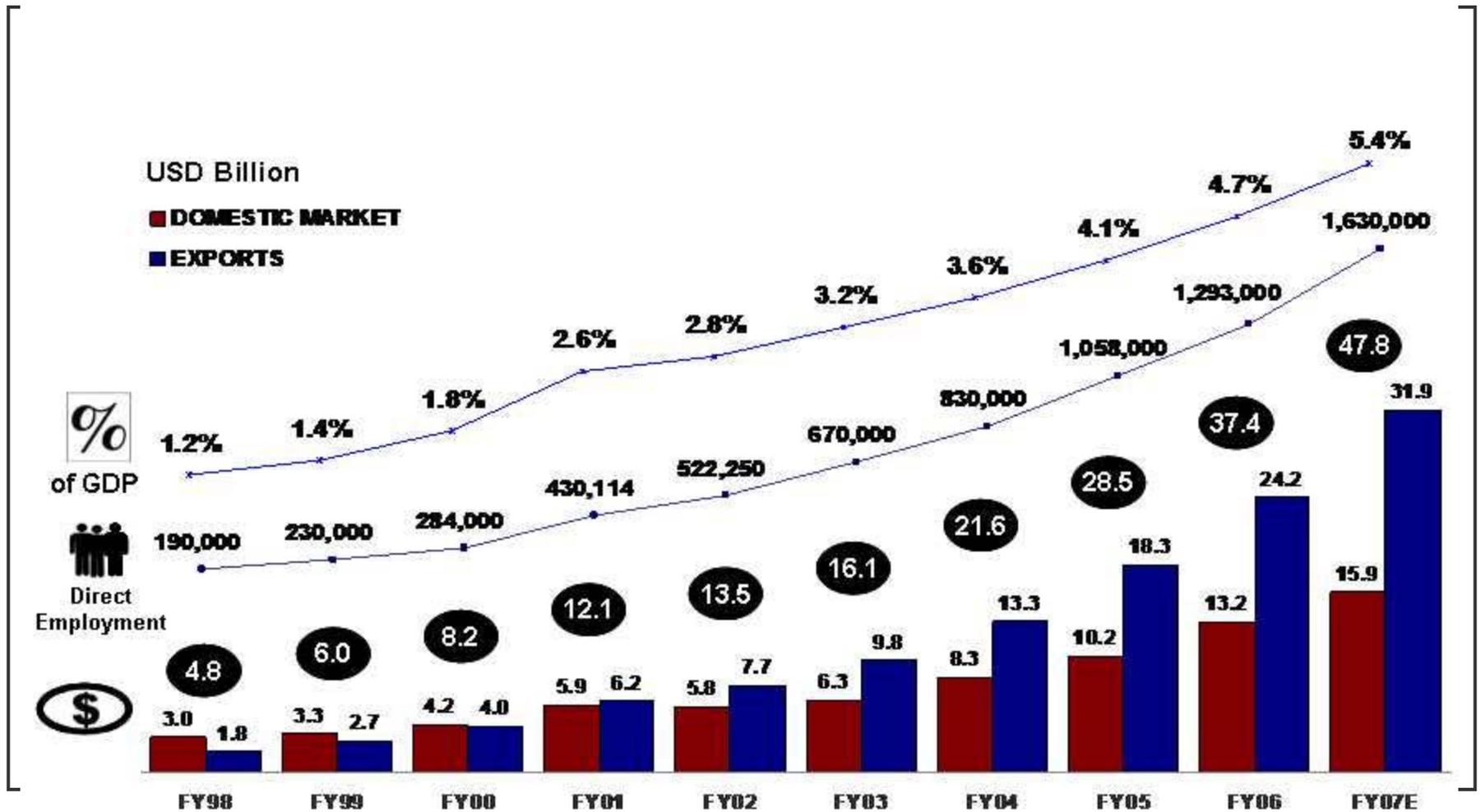


Mobile Telephony and Internet Growth



Source: *TRAI Report, eTechnologyGroup@IMRB*

Growth of the Indian IT industry



Tenfold growth over a decade (Source: NASSCOM)



Cyber Security Awareness

- High profile incidents
 - Detection of spyware in government mail servers
 - Tor interception
 - Theft of hard disks
 - Navy war room leak
- Rising awareness
 - Driven by outsourcing concerns
- Election manifesto!
 - Digital Security Agency

Legal Framework

- Information Technology Act, 2000
- ITA 2.0, passed in December 2008
- Still a work in progress
- Features
 - Corporate liability for data protection
 - Reasonable Security Practices
 - Data retention by intermediaries
 - Recognition of cyber terrorism
 - Sub-section 66F: punishment for cyber terrorism – up to life imprisonment.
 - Cyber terrorism: denial of service, illegal access, introducing a virus in any of the critical information infrastructure of the country defined with the intent to threaten the unity, integrity, security or sovereignty of India or strike terror in the people or any section of the people; or gaining illegal access to data or database that is restricted for reasons of the security of state or friendly relations with foreign states.

Structures

- Government
 - CERT-In
 - Standardization, Testing and Quality Certification (STQC) organization
- Private Sector
 - Data Security Council of India
 - Banking industry CERT
- Law enforcement
 - Leadership by Central Bureau of Investigation
 - Cyber Crime Investigation Cells

Initiatives

- National E-governance Action Plan
 - \$2.5 billion project
- CERT-In participation in the global efforts
- Information Security Education and Awareness Program
- Public Private Partnerships
 - India Cyber Lab
 - Cyber Safety Week

Further Queries?

National Perspectives on: Infrastructure Protection, Cyber Crime and the Potential for War in Cyber Space

A View from Russia

Alexey A. SALNIKOV

Vice-director

Information Security Institute

Lomonosov University, Moscow



INFORMATION
SECURITY
INSTITUTE

LOMONOSOV UNIVERSITY
MOSCOW



Background:

- the World Summit on the Information Society
 - Geneva (2003)
 - Tunis (2005)
- The Internet Governance Forum
 - 2006 (Athens, Greece)
 - 2007 (Rio de Janeiro, Brazil)
 - 2008 (Hyderabad, India)
- Shanghai Co-operation Organization and the Collective Security Treaty Organization
- UN General Assembly resolution 63/37 «Developments in the field of information and telecommunications in the context of international security»
- OSCE Workshop “Comprehensive OSCE Approach to Enhancing Cyber Security” (Vienna, March 2009)



Our efforts are aimed at

- preventing the next round of an arms race at a qualitatively new level in the development of ICT
- preserving resources in the interests of development
- limiting the aggressive use of these technologies to resolve inter-State conflicts by means of force



CHALLENGES IN INTERNATIONAL CYBER SECURITY

Center for Technology and National Security Policy

National Defense University

Washington, DC, 29-30 April 2009



politico-military threat

"using of ICT to achieve political aims by exerting «force» on the leadership of opposing States, essentially the «hostile» use of ICT"

is of priority importance



INFORMATION
SECURITY
INSTITUTE

LOMONOSOV UNIVERSITY
MOSCOW



REASONS:

ICT is gradually turning into new and powerful means of having a destructive effect on industrial and economic facilities, social infrastructure and governments, i.e., a means of waging armed struggle with the capacity to resolve the problems of inter-State confrontation at the tactical, operational and strategic levels



ICT is acquiring the characteristics of a weapon

“devices and arrangements that are constructively designed to defeat one's opponent in combat”



Using of ICT as a means of «force» against an opposing State may result in the emergence of *«situations that could threaten international peace and security»*



Specific features of new threat:

- possibility of its latent transboundary application;
- covert and anonymous nature of the preparation and execution of hostile activities;
- difficulties encountered in preventing such activities and responding to them in an appropriate manner.



CHALLENGES IN INTERNATIONAL CYBER SECURITY

Center for Technology and National Security Policy

National Defense University

Washington, DC, 29-30 April 2009

Proposals:

- Common terminology of international information security (some work has been done in the Shanghai Co-operation Organization and the Collective Security Treaty Organization);
- development of international security and humanitarian law for creating an effective system of preventing and suppressing possible aggressive actions involving the use of ICT.
 - whether the existing norms of international law are sufficient for countering the threat posed by the «hostile» use of ICT
 - to draw up a document, acknowledging the existence of politico-military and criminal threats, including terrorist ones, to international information security and providing for the possibility of carrying out joint measures to minimize the damage to the national interests of individual countries and to the interests, of the international community as a whole
 - creating a system for (provable) identifying the source of «hostile» activities associated with the use of ICT as a means of attacking an opposing State.
 - preventing «perfidy» in the use of ICT as a means of «force» (this kind of use of ICT is possible, first and foremost, given the presence of prepared «positions» in the general hardware and software of the information and communication systems of the opposing party)
- international co-operation with a view to making the Internet more secure
 - increasing confidence in this global information infrastructure by means of more globalize governance of the Internet
 - ensuring the investigation and criminal prosecution of cybercrime, including cybercrimes committed within the jurisdiction of one country but having consequences in another country.



INFORMATION
SECURITY
INSTITUTE

LOMONOSOV UNIVERSITY
MOSCOW



Moscow University named after M.V.Lomonosov has been appointed by the **Security Council of Russian Federation** as the **leading scientific organization** in Russia on humanity problems of information security

Proposals for common Universities' projects:

- Creating web site and virtual net of international experts for preliminary discussions on disputable issues of international cyber security
 - Starting topic: Basic concepts and terminology
- Comparative interdisciplinary analysis of National Information Security Doctrines and Strategies
 - Starting topic: US National Strategy to Secure Cyberspace vs Russian Information Security Doctrine.



CHALLENGES IN INTERNATIONAL CYBER SECURITY

Center for Technology and National Security Policy

National Defense University

Washington, DC, 29-30 April 2009

THANK YOU!

www.iisi.msu.ru



INFORMATION
SECURITY
INSTITUTE

LOMONOSOV UNIVERSITY
MOSCOW

