

Digital Dependence: Cybersecurity in the 21st Century

Melissa E. Hathaway

Senior Advisor, Belfer Center for Science and International Affairs

Harvard University

Presented as part of Project Minerva

14 October 2010



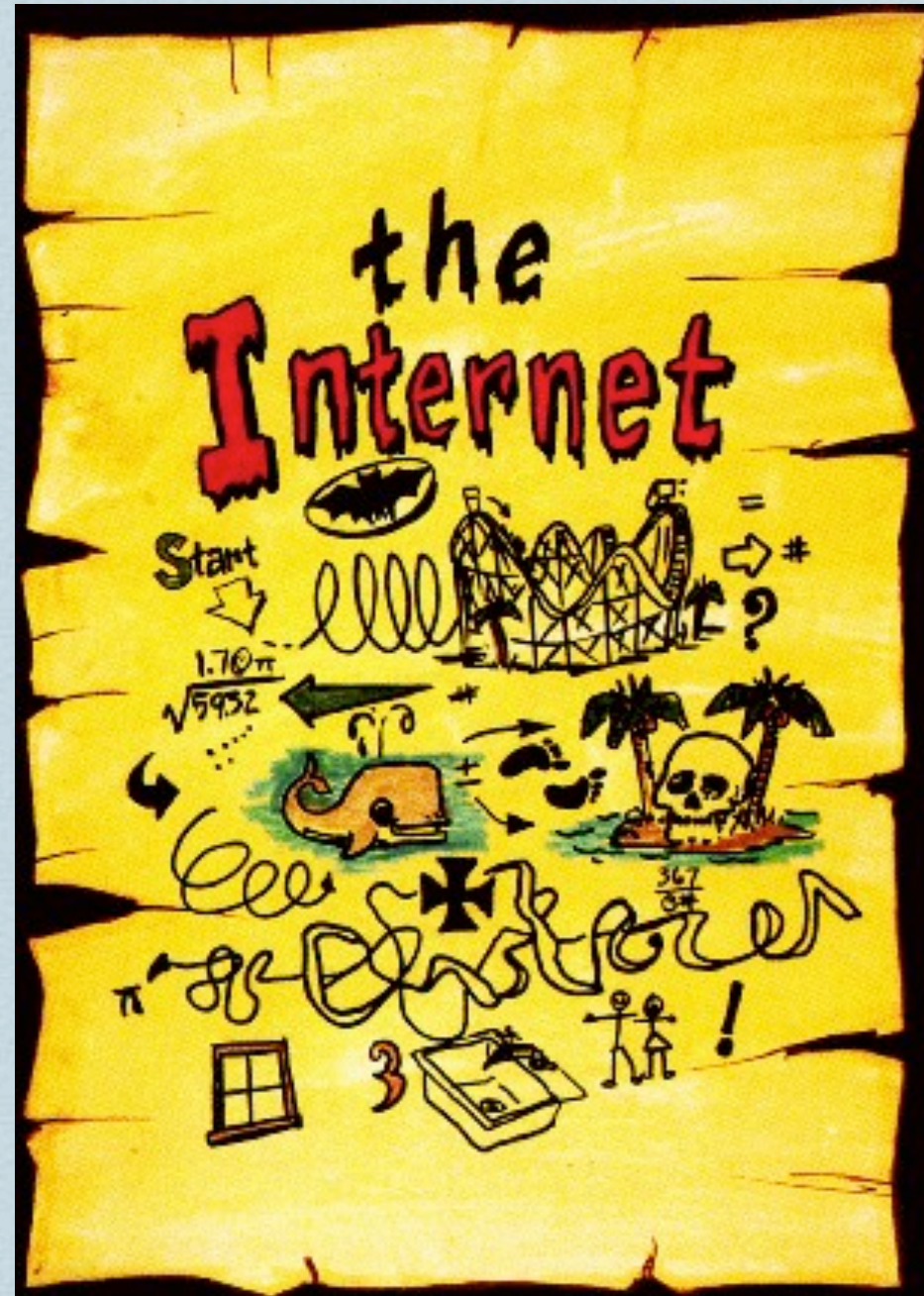
HARVARD Kennedy School

BELFER CENTER for Science and International Affairs

© 2010, Hathaway Global Strategies, LLC

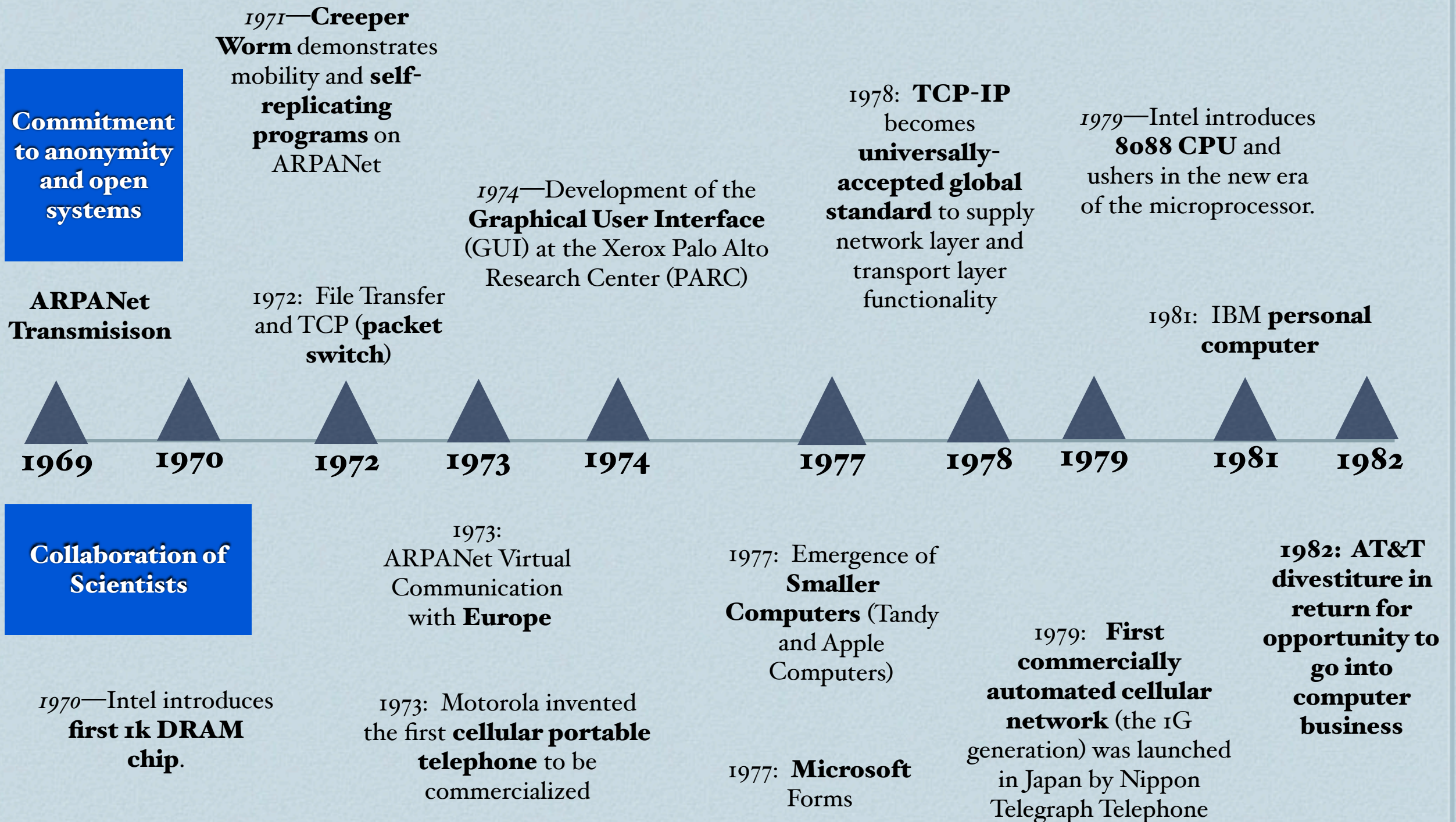
Sunday, November 28, 2010

October 29, 1969: The First Transmission



❖ http://www.picsearch.com/info.cgi?q=1969%20Internet&id=PVUGViNVCgNvPh-pX1_sm_AoVagXS4c9lomC0G41zY

Timeline of Digital Dependence



Foreshadow the Future: 1981?

MOTHER JONES

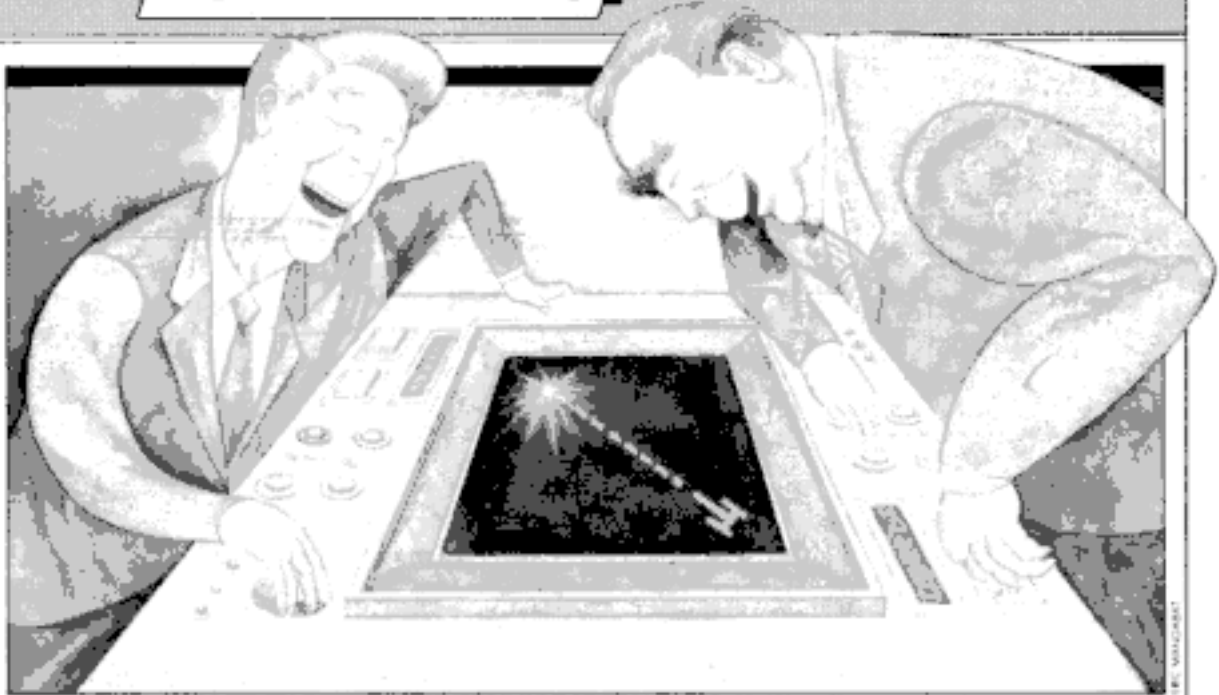
FRONTLINES

Computerized Detente

As the chill between the Soviet Union and the United States intensifies, the Reagan administration has been busily closing down all the channels of communication that marked the era of detente. Technology trade has been limited; cultural and scientific exchanges have been curtailed, and space cooperation is nonexistent.

There is, however, still one unofficial link between the two superpowers. Sources have told *Mother Jones* that for several years there has been an electronic pathway from the ARPAnet—the experimental Pentagon computer network, which ties together major academic, corporate and military computer research centers in the U.S.—directly to Moscow.

The pathway, according to a Silicon Valley computer scientist and corporate president,



“runs from an ARPAnet computer, the MIT Artificial Intelligence computer, via Telenet, a private commercial computer network, to a multinational research center, the International Institute for Applied Systems Analysis (IIASA), which is located outside of Vienna. IIASA, in turn, has a direct high-speed data link to

Moscow.”

The unofficial link makes it possible, hypothetically at least, for computer scientists and defense researchers on both sides to send each other messages despite the hostile international climate.

As might be expected, Department of Defense officials refused to comment on the existence of the East-West computer tunnel.

Some observers feel, however, that it just might offer a solution to the arms race. Suggests one member of the ARPAnet community, “Maybe we could just settle it all with a giant computer space-war game.”

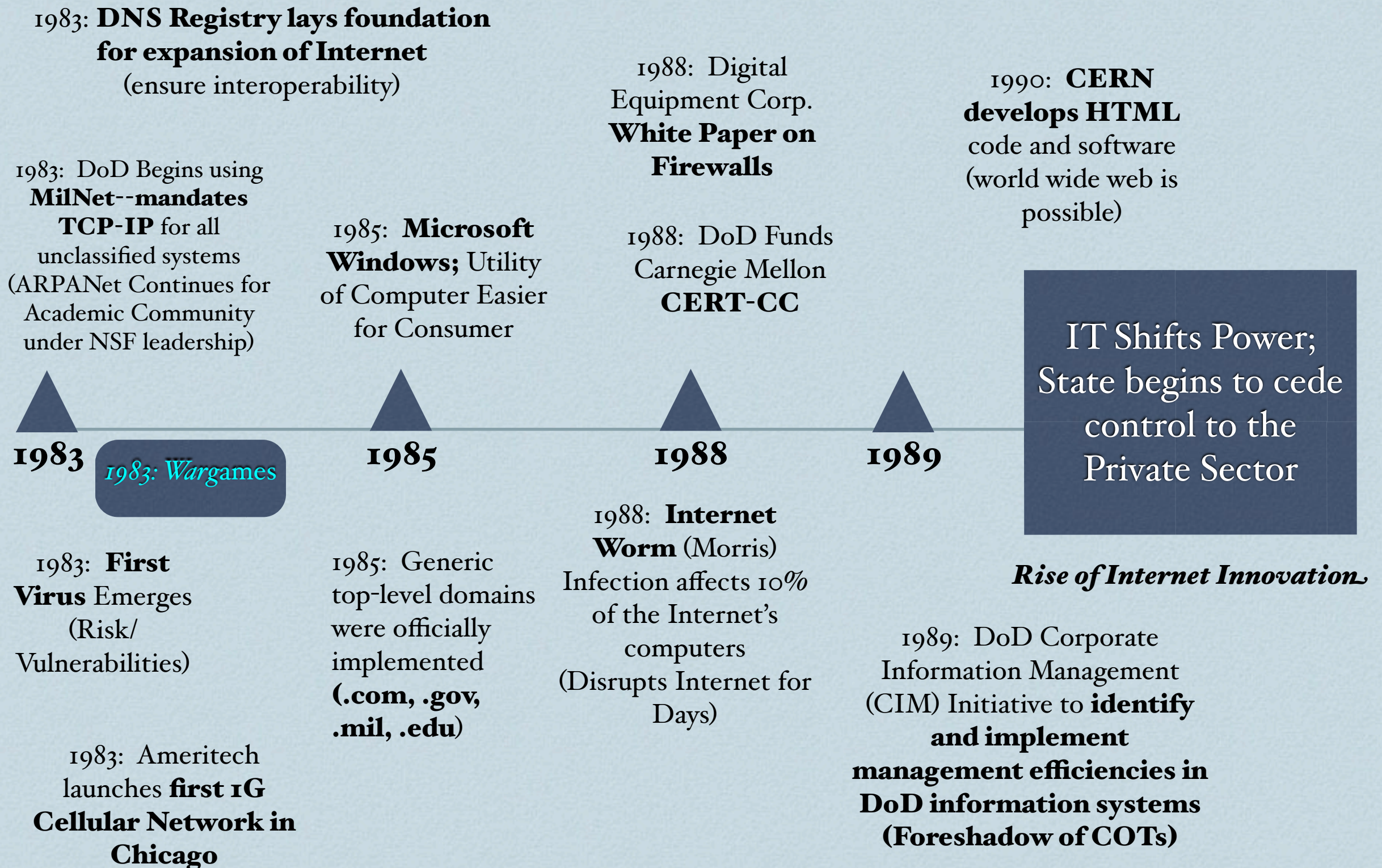
—John Markoff

❖ http://books.google.com/books?id=a-YDAAAAMBAJ&pg=PA11&lpg=PA11&dq=computerized+detente+john+markoff&source=bl&ots=w2IZQuT6ro&sig=3M268mjlqFSq-HXLTFffD-NmYdk&hl=en&ei=AHq8S5iAA4aM8gTwrOn5Bw&sa=X&oi=book_result&ct=result&resnum=3&ved=0CAsQ6AEwAg#v=onepage&q=computerized%20detente%20john%20markoff&f=false

Reflection on the First 13 Years

- ❖ Mobile platforms emerge with the birth of personal computer and cellular voice communications
- ❖ ARPANet enabled global data communications
- ❖ AT&T divestiture signaled first market force tensions -- innovation at the expense of national security and the beginning of loss of interest in State influence of core infrastructure (control)

Timeline of Digital Dependence



Dawn of Information Sharing

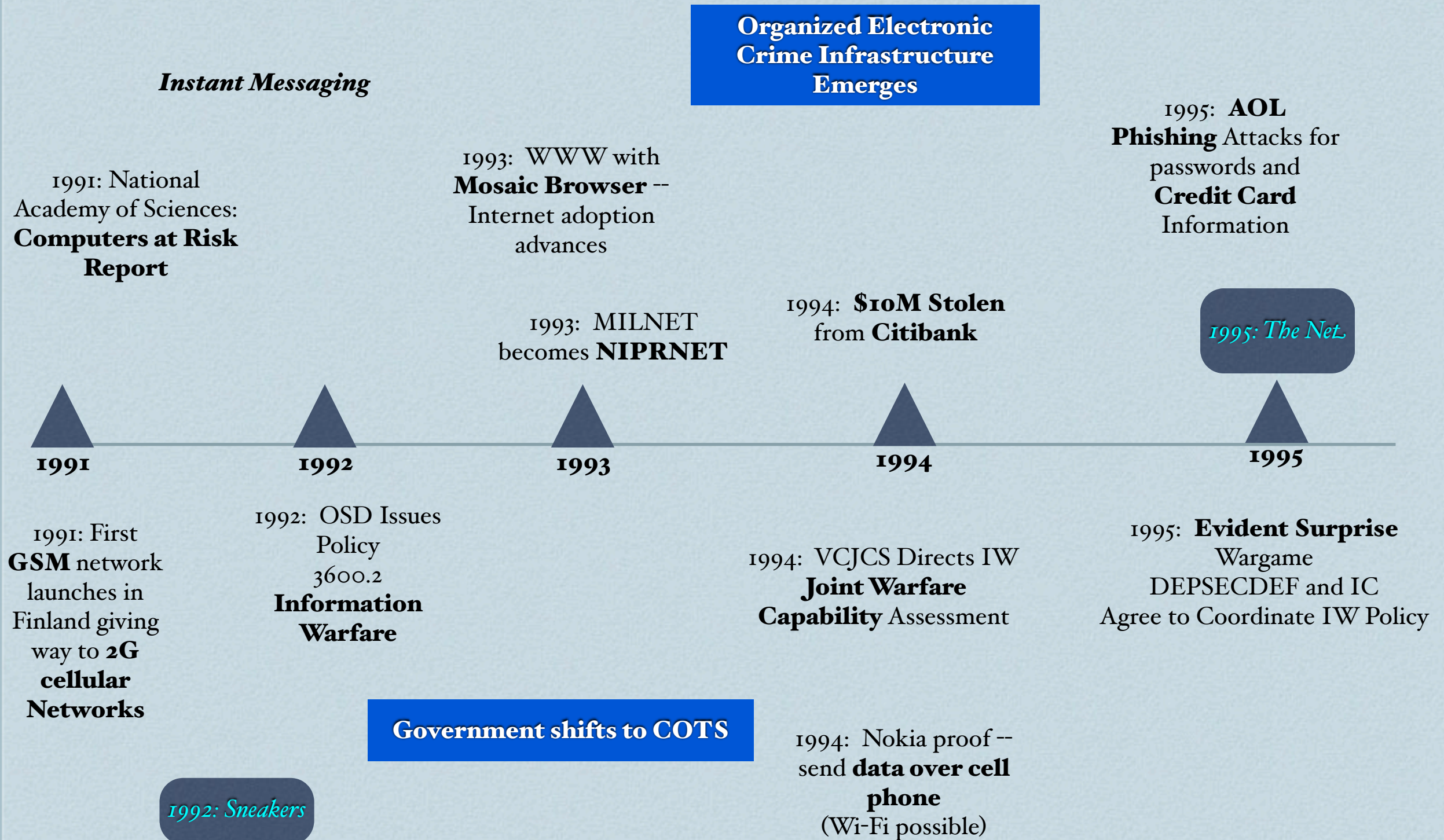


- ❖ World Wide Web enables expanded and user-friendly information sharing on the Internet

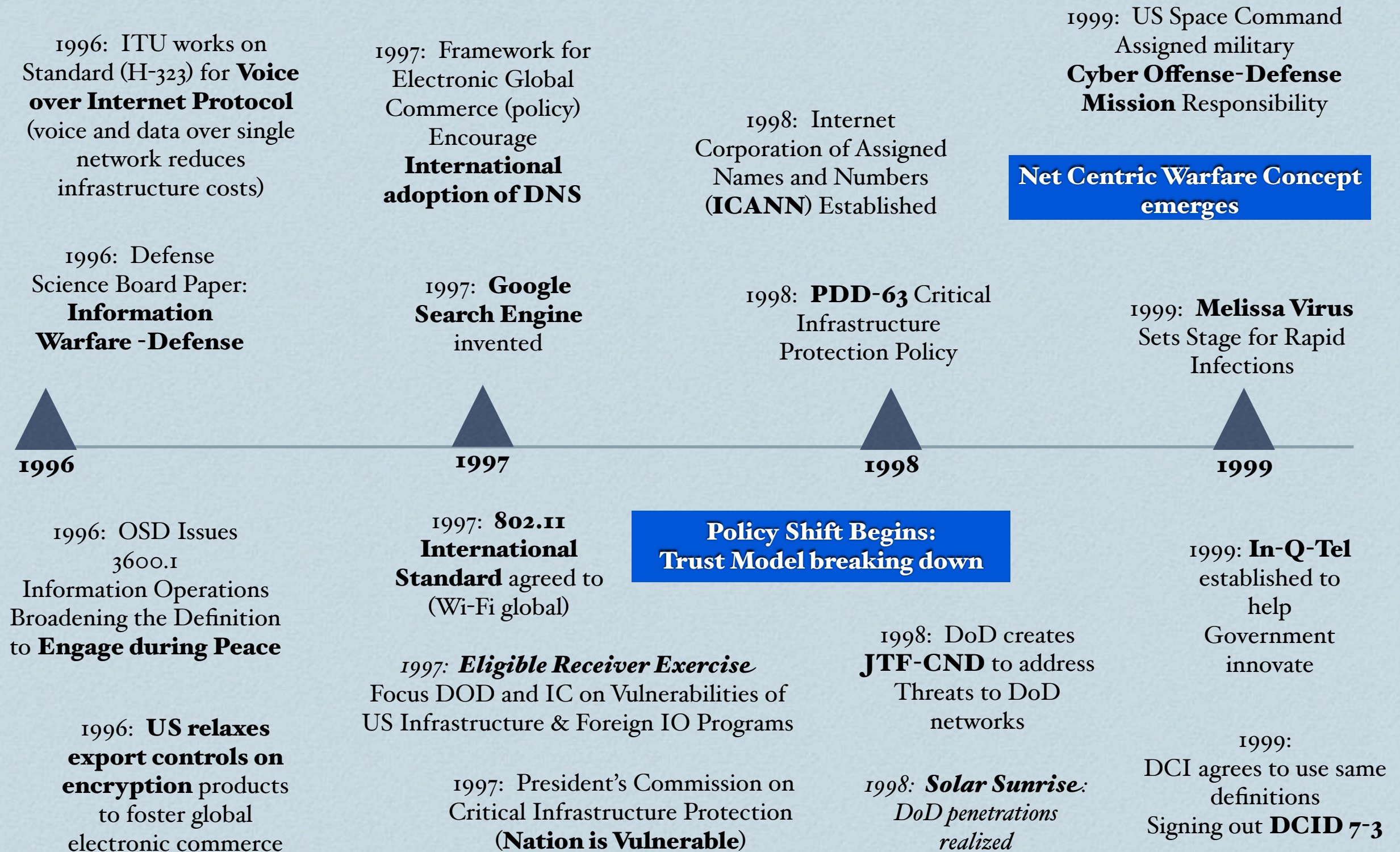
Reflection at Year 20

- ❖ DoD becomes the early adopter of the technology
- ❖ Private sector driving innovation and adoption with value proposition of productivity and efficiency and consumer usability of technology
- ❖ Foreshadow the potential for e-commerce with .com domain and emergence of world wide web
- ❖ First demonstration of vulnerability and exploitation possibilities and subsequent emergence of a new market (e.g., Firewall, anti-virus software, IDS and IPS)

Timeline of Digital Dependence



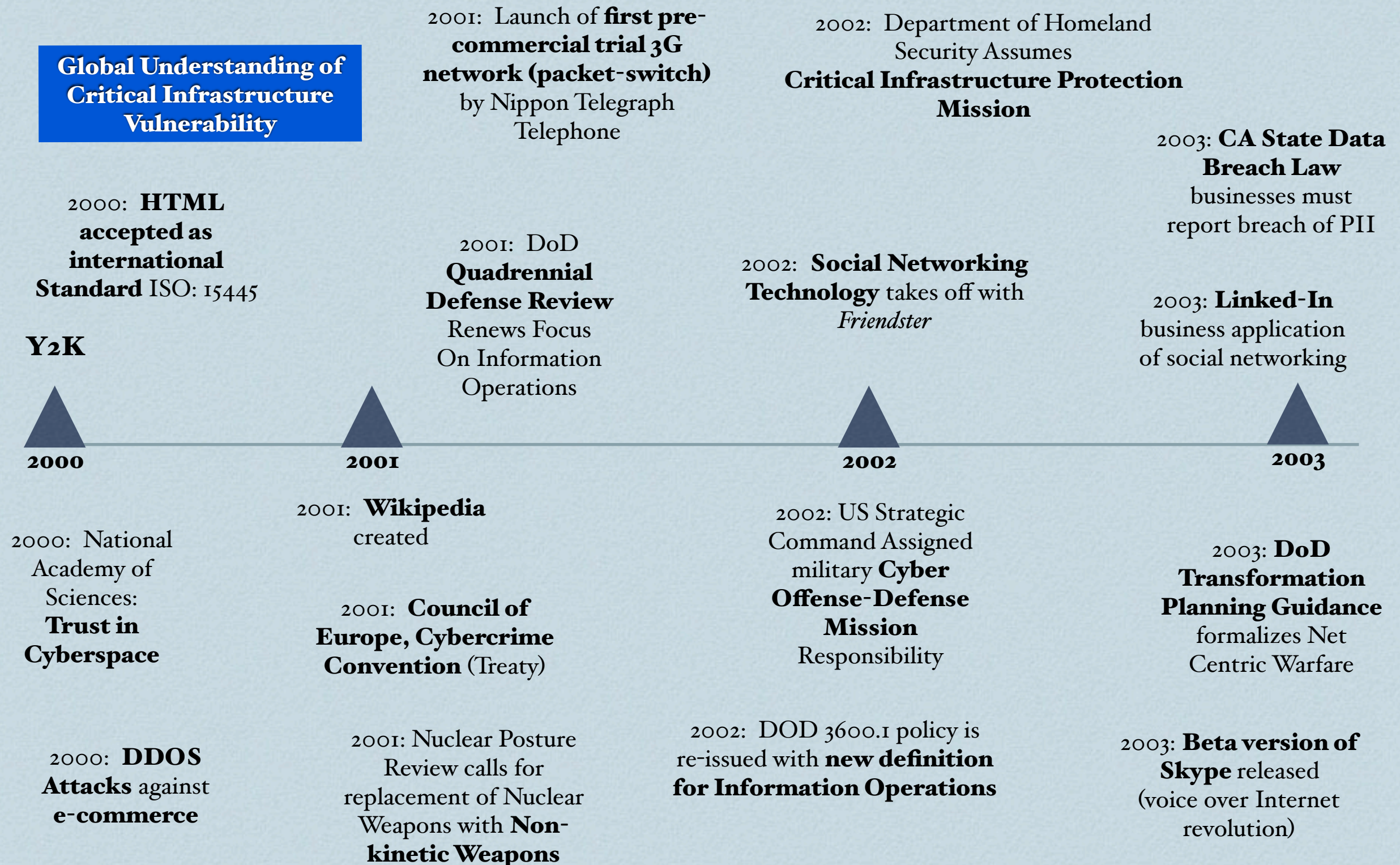
Timeline of Digital Dependence



Reflection at Year 30

- ❖ Rapid infections on Internet realized; policymakers begin to discuss and write about problem
- ❖ Organized electronic crime infrastructure emerges--anonymity provides safe have for criminals-- e-commerce trust model begins to break down
- ❖ Data over wireless emerges as next market wave and voice over Internet presents a second market disruption to “traditional voice carriers”
- ❖ Relaxation of export controls (crypto) along with promotion of international adoption of DNS encourages the world to depend upon the Internet
- ❖ Need for “controls” on interoperability and stability of the Internet is recognized with establishment of ICANN

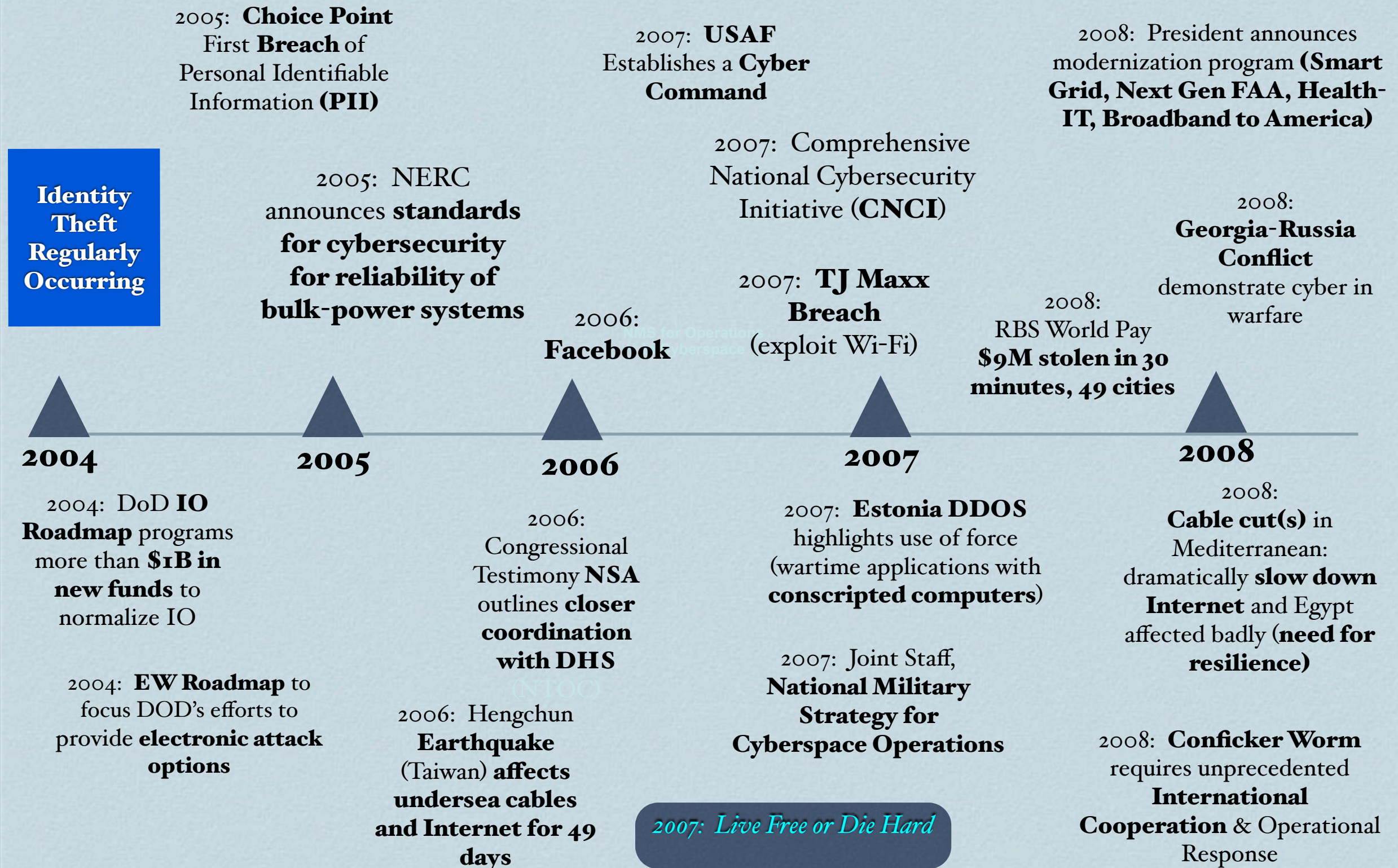
Timeline of Digital Dependence



Reflection at Year 35

- ❖ World wide recognition of convergence of Internet with critical infrastructures because of Y2K computer programming error and that problem cannot be solved without a private-public partnership
- ❖ International awareness on threat of cybercrime -- but not fully embraced
- ❖ 9/11/01 refocused mission toward physical security vice electronic security and blurred mission responsibility with stand-up of Department of Homeland Security
- ❖ Recognition that the government must embrace innovation wave
- ❖ Social Networking technology emerges with fast consumer adoption rates, foreshadows next “rich” target for exploitation

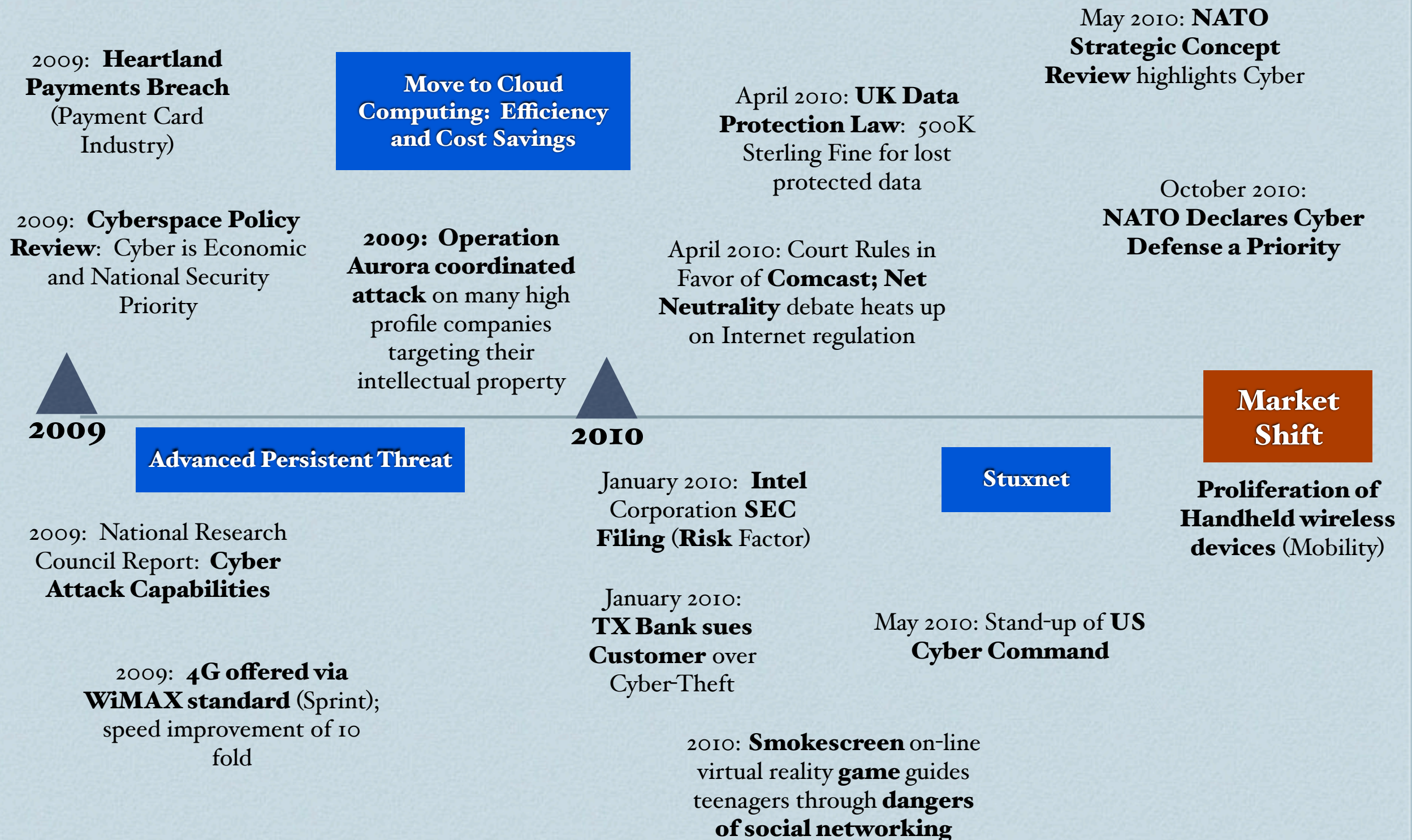
Timeline of Digital Dependence



Reflection at Year ~40

- ❖ Doctrine and rhetoric publicly address use of Internet for offensive means; Estonia and Georgia events demonstrate first use of Internet as a means for warfare
- ❖ Recognition that other key infrastructures (power) are now more vulnerable due to dependence on Internet infrastructure
- ❖ Conficker Worm highlights need for international cooperation and necessity of private sector information sharing
- ❖ CNCI policy illuminates need for stronger defensive posture and cooperation, cross-cueing, and leverage of mission authorities (Title: 6, 10, 18, 32, 44, 50)
- ❖ Cybercrime and cyber espionage can no longer be ignored
- ❖ Cable cut(s) in the Mediterranean demonstrates importance of undersea cables and resilience

Timeline of Digital Dependence



Reflection at Year 41

- ❖ Google incident -- tipping point in US policy and serves as catalyst for corporate awareness
- ❖ Cybercrime and cyber espionage are affecting bottom line and risk factors of major corporations
- ❖ Legislation and regulation are emerging as mechanisms to assert “control”, manage risk and build security back into the infrastructure
- ❖ Nations realize lack of resilience is national and economic security risk
- ❖ Stuxnet targets control system (product) functionality, putting critical infrastructures at risk around the world
- ❖ Government intervention has become more pronounced and pervasive – and censorship and surveillance practices are on the rise

❖ *It happened so fast that we have not had time to be astonished...* Vaclav Havel

Source: http://www.nixoncenter.org/publications/Perspectives/Cohenvol.3_8.htm

Economic and National Security Cannot be *Shoved* to the Back Burner for Economic Efficiency

❖ *...That the further one looks back -- the further forward one can see...* Winston Churchill

What is Needed?

- ❖ Begin an honest conversation about what is happening in the United States to our long-term strategic posture (denial will not lead to recovery)
- ❖ Reconcile the tension between economic recovery and national security needs
- ❖ Retard the quick-to-adopt movement of all critical infrastructures to rely on Internet based protocols and technology
- ❖ Enlist and incentivize the private sector to understand and address the vulnerabilities and innovate our way through a solution
- ❖ Engage Congress to clarify and legislate new authorities
- ❖ Review regulatory authorities (FCC, FTC, SEC, FERC) and demand coordination across Internet jurisdictional overlap; Legislation has not kept pace with technology, making regulation difficult
- ❖ State US policy of what is tolerable (crime, espionage, and armed aggression) and impose costs if threshold is crossed