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
October 29, 1969:
The First Transmission

http://www.picsearch.com/info.cgi?q=1969%20Internet&id=PVUGViNVCGnNyPh-pX1_sm_AoVagXS4c9lomC0G41zY
Timeline of Digital Dependence

1969: ARPANet Transmission

1970: Intel introduces first 1k DRAM chip.

1971—Creeper Worm demonstrates mobility and self-replicating programs on ARPANet

1973: File Transfer and TCP (packet switch)

1974—Development of the Graphical User Interface (GUI) at the Xerox Palo Alto Research Center (PARC)

1977: ARPANet Virtual Communication with Europe

1978: TCP-IP becomes universally-accepted global standard to supply network layer and transport layer functionality

1979—Intel introduces 8088 CPU and ushers in the new era of the microprocessor.

1979: First commercially automated cellular network (the 1G generation) was launched in Japan by Nippon Telegraph Telephone

1981: IBM personal computer

1982: AT&T divestiture in return for opportunity to go into computer business

© 2010, Hathaway Global Strategies, LLC
Foreshadow the Future: 1981?

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 ARPA—Net—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 ARPA Net 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 ARPA net community, "Maybe we could just settle it all with a giant computer space-war game."

—John Markoff
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

1983: **DNS Registry lays foundation for expansion of Internet** (ensure interoperability)

1983: DoD Begins using MilNet—mandates TCP-IP for all unclassified systems (ARPANet Continues for Academic Community under NSF leadership)

1983: **First Virus Emerges** (Risk/Vulnerabilities)

1983: Ameritech launches first 1G Cellular Network in Chicago

1985: **Microsoft Windows; Utility of Computer Easier for Consumer**

1985: **Generic top-level domains were officially implemented (.com, .gov, .mil, .edu)**

1988: **Digital Equipment Corp. White Paper on Firewalls**

1988: Digital Equipment Corp.

1988: **Internet Worm** (Morris) Infection affects 10% of the Internet’s computers (Disrupts Internet for Days)

1988: DoD Funds Carnegie Mellon CERT-CC

1990: **CERN develops HTML code and software** (world wide web is possible)

1989: DoD Corporate Information Management (CIM) Initiative to **identify and implement management efficiencies in DoD information systems** (Foreshadow of COTs)

© 2010, Hathaway Global Strategies, LLC
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


1991: First GSM network launches in Finland giving way to 2G cellular Networks

1992: OSD Issues Policy 3600.2 Information Warfare

1992: Sneakers

1993: WWW with Mosaic Browser – Internet adoption advances

1993: MILNET becomes NIPRNET

1994: VCJCS Directs IW Joint Warfare Capability Assessment

1994: $10M Stolen from Citibank

1994: Nokia proof – send data over cell phone (Wi-Fi possible)

1995: AOL Phishing Attacks for passwords and Credit Card Information

1995: Evident Surprise Wargame DEPSECDEF and IC Agree to Coordinate IW Policy

Timeline of Digital Dependence

1996: ITU works on Standard (H-323) for **Voice over Internet Protocol** (voice and data over single network reduces infrastructure costs)


1996: OSD Issues 3600.1 Information Operations Broadening the Definition to **Engage during Peace**

1996: **US relases export controls on encryption** products to foster global electronic commerce

1996: **Google Search Engine** invented

1997: **802.11 International Standard** agreed to (Wi-Fi global)

1997: **Eligible Receiver Exercise** Focus DOD and IC on Vulnerabilities of US Infrastructure & Foreign IO Programs

1998: **PDD-63 Critical Infrastructure Protection Policy**

1998: **DoD creates JTF-CND to address Threats to DoD networks**

1998: **Solar Sunrise**: DoD penetrations realized

1999: **Melissa Virus** Sets Stage for Rapid Infections


1999: **Net Centric Warfare Concept emerges**

**Policy Shift Begins:** Trust Model breaking down

1999: **In-Q-Tel** established to help Government innovate

1999: DCI agrees to use same definitions Signing out DCID 7-3

© 2010, Hathaway Global Strategies, LLC
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 haven 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**

2000: HTML accepted as international Standard ISO: 15445

Y2K


2000: DDOS Attacks against e-commerce

2001: Launch of first pre-commercial trial 3G network (packet-switch) by Nippon Telegraph Telephone

2001: DoD Quadrennial Defense Review Renews Focus On Information Operations

2001: Wikipedia created

2001: Council of Europe, Cybercrime Convention (Treaty)

2001: Nuclear Posture Review calls for replacement of Nuclear Weapons with Non-kinetic Weapons


2002: Social Networking Technology takes off with Friendster


2002: DOD 3600.1 policy is re-issued with new definition for Information Operations

2002: Beta version of Skype released (voice over Internet revolution)

2003: CA State Data Breach Law businesses must report breach of PII

2003: Linked-In business application of social networking

2003: Linked-In business application of social networking

2003: Beta version of Skype released (voice over Internet revolution)
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

2004: DoD IO Roadmap programs more than $1B in new funds to normalize IO

2005: Choice Point First Breach of Personal Identifiable Information (PII)

2005: NERC announces standards for cybersecurity for reliability of bulk-power systems

2006: Hengchun Earthquake (Taiwan) affects undersea cables and Internet for 49 days

2006: DoD IO Roadmap to focus DOD’s efforts to provide electronic attack options

2006: EW Roadmap to focus DOD’s efforts to provide electronic attack options

2006: Congression Testimony NSA outlines closer coordination with DHS

2007: USAF Establishes a Cyber Command

2007: Comprehensive National Cybersecurity Initiative (CNCI)

2007: Estonia DDOS highlights use of force (wartime applications with conscripted computers)

2007: TJ Maxx Breach (exploit Wi-Fi)

2007: Joint Staff, National Military Strategy for Cyberspace Operations

2008: Conficker Worm requires unprecedented International Cooperation & Operational Response

2008: Cable cut(s) in Mediterranean: dramatically slow down Internet and Egypt affected badly (need for resilience)

2008: Georgia-Russia Conflict demonstrate cyber in warfare

2008: President announces modernization program (Smart Grid, Next Gen FAA, Health-IT, Broadband to America)

2008: RBS World Pay $9M stolen in 30 minutes, 49 cities

2007: Live Free or Die Hard

Identity Theft Regularly Occurring

2005: NERC announces standards for cybersecurity for reliability of bulk-power systems

2007: Comprehensive National Cybersecurity Initiative (CNCI)

2007: Joint Staff, National Military Strategy for Cyberspace Operations

2008: Georgia-Russia Conflict demonstrate cyber in warfare

2008: President announces modernization program (Smart Grid, Next Gen FAA, Health-IT, Broadband to America)
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

2009: Heartland Payments Breach (Payment Card Industry)

2009: Cyberspace Policy Review: Cyber is Economic and National Security Priority

2009: 4G offered via WiMAX standard (Sprint); speed improvement of 10 fold

2009: Advanced Persistent Threat


2009: Operation Aurora coordinated attack on many high profile companies targeting their intellectual property

Move to Cloud Computing: Efficiency and Cost Savings

2010: Intel Corporation SEC Filing (Risk Factor)

April 2010: UK Data Protection Law: 500K Sterling Fine for lost protected data

April 2010: Court Rules in Favor of Comcast; Net Neutrality debate heats up on Internet regulation

2010: Smokescreen on-line virtual reality game guides teenagers through dangers of social networking

April 2010: TX Bank sues Customer over Cyber-Theft

May 2010: NATO Strategic Concept Review highlights Cyber

October 2010: NATO Declares Cyber Defense a Priority

May 2010: Stand-up of US Cyber Command

Proliferation of Handheld wireless devices (Mobility)

© 2010, Hathaway Global Strategies, LLC
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
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 Chuchill
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

© 2010, Hathaway Global Strategies, LLC