The Internet Kill Switch
Fact or Fiction?

• Robert L. Foster
• October 2014
ALL MATERIALS ARE DECLASSIFIED
AND IN THE PUBLIC DOMAIN

Whitehouse.gov, NSA, DHS, TSA, FBI Sites.
Guardian, NY Times, Wall Street Journal
HOW IT BEGAN...

• 1920’s – Army Gets “Black Chamber” & Western Union
• SHAMROCK Formed 1945 NSA Formed 1952 – Took Over SHAMROCK
• 1946 – JE Hoover Launched Propoganda against Domestic “enemies”
• 1956 FBI Launched COINTEL PRO – to disrupt “Commies”
• Law Changes in 1959 Unfettered NSA’s Powers
  – Established Centers in New York, San Francisco and San Antonio
• By 1960’s COINTEL PRO was Lawless Dragnet (Nixon, JE Hoover)
• 1969 – MINARET REPLACES SHAMROCK
• 1970 – 100’S Co’s Partner w/ NSA; FBI/CIA Feed Domestics
• Church Commission Exposed Violations of 4th Amendment: 1975
• 1978 – MINARET’S WRONGDOINGS LED TO FISA
• 2001 -- 9-1-1, PATRIOT ACT PASSED
• 2006 – ROOM 641A in San Francisco Exposed
• 2007 – Protect America Act – PRISM TAKES ITS FIRST RASPY BREATH
• 2008 – Requirement for Warrants Removed
• 2012 – AG, DNI, D-NCTC Update Domestic Spy Rules
• 2012 – President Extends FAA for Five Years, Modifies COGCON 5
Internet Kill Switch Legislation

- 2010 - Senate bill PCNAA –
  - Protecting Cyberspace as a National Asset Act
- Sponsored by Senator Joseph Lieberman
- Proposes Presidential Authority
  - “To seize control of or shut down portions of the Internet.” (CNET)
  - Creates new agency within the Department of Homeland Security,
    - The National Center for Cybersecurity and Communications (NCCC).
- Any private company reliant on "the Internet, the telephone system, or any other component of the U.S. 'information infrastructure'"
  - would be “subject to command" by the NCCC, and
  - some would be required to engage in "information sharing" with the agency, says CBS4.
- Bill requires that private companies--such as "broadband providers, search engines, or software firms," CNET explains
  - "immediately comply with any emergency measure or action" put in place by the
  - department of Homeland Security, or else face fines.
Federal executive branch government employees at their normal work locations. Maintain alternate facility and conduct periodic continuity readiness exercises.

Federal agencies and departments Advance Relocation Teams “warm up” their alternate sites and capabilities, which include testing communications and IT systems. Ensure that alternate facilities are prepared to receive continuity staff. Track agency leaders and successors daily.

Deployment of 50-75% of Emergency Relocation Group continuity staff to alternate locations. Establish their ability to conduct operations and prepare to perform their organization’s essential functions in the event of a catastrophic emergency.

Full deployment of designated leadership and continuity staffs to perform the organization’s essential functions from alternate facilities either as a result of, or in preparation for, a catastrophic emergency.

Activate classified CONPLAN 3600 evacuating the President and those in the line of presidential succession. Activate classified CONPLAN 3502 deploying the military to enforce law and order within the Civilian Control Districts. Seize all private communication facilities and assume control over all civilian voice and data communications. Activate internet kill switch. Commandeer all U.S. domestic resources including food and water. Seize all domestic energy and transportation infrastructure. Deploy the national citizen conscription plan to fulfill any labor required for the purpose of national defense and reconstitution.

Source: Whitehouse.gov
How Can The Internet Be Shut Down?

• Soft Spots
  – Power
  – Landlocked “Pipes”
  – Undersea “Pipes”
  – Network Components (Servers, Switches, F/W, etc).
  – Wireless Towers/Cellular
  – Capacity
  – Crossroads: e.g., ISP’s, USA Ingress/Egress Points
  – Human Element
  – DoS Attacks and Similar
  – Interdiction
“I don't see a huge technical hurdle here, other than maybe a script to disable all peering interfaces for every ISP in the US. This could be done by hand just as easily should Uncle Sam come knocking.”
FINITE LIST OF MAJOR PLAYERS
WHAT WE DIDN'T HEAR ABOUT - GOVERNMENT SECURITY AGREEMENTS

- Verizon Wireless is a JV Between Verizon Communications & Vodafone Group 2000
- Deutsche Telekom AG Owns T-Mobile, Acquired VoiceStream Wireless Corp 2001
- Singapore Technologies Telemedia Acquired Global Crossing Ltd. 2003
- Alcatel-Lucent SA is a Merger of France-based Alcatel & US-based Lucent Technologies 2006
- Ericsson Purchased Nortel Networks 2009
- Nokia Solutions & Networks Acquired Motorola Solutions Inc.’s N/W Assets 2011
- Level 3 Communications Bought Global Crossing in 2011
- Japan’s SoftBank Acquired Sprint July 2013
- German-Owned T-Mobile USA Merged with MetroPCS Communications Last Spring
Requirements in Security Agreements with the United States Government

- FED Can Appoint a Director to the Board
- Three of Top Four Telecomm Compelled to Sign
- Compel Companies to Honor Requests for Access
- Must Give a Comprehensive Description of their Networks
- Must Give Access to All Domestic Traffic
- Must Set up a Facility for Surveillance
- List All Equipment Used: Model #’s, Full Specs, Routers, etc.
- Must be Able to Interrupt Traffic To/From USA
- Can Require Firms to Remove Certain Equipment
- Can Approve Equipment & Vendors
- Fed Can Interview Employees & Conduct Inspections
Our Undersea Cable Tapping Strategy
By tapping into the worldwide network of undersea cables, our OAKSTAR, STORMBREW, BLARNEY and FAIRVIEW systems can process data as it flows across the internet. Each system is responsible for different types of intercepted data. For example, the BLARNEY system gathers metadata describing who is speaking to whom and through which networks and devices.
Two methods are employed for tapping into the undersea cable network

A modified nuclear submarine houses technicians and gear needed to place the physical taps on the undersea cables along strategic points in the network.

Second method uses intercept probes at the point where cables connect to the landing stations in various countries. These probes capture and copy the data as it flows onward. “Jimmy Carter” Sub $3.2 Billion
UUNET Global Network
United States transmission grid
Source: FEMA
http://www.brgwireless.com/recordings/HAZMA_2-male-es.mp3
Your Mission

• The USA has been attacked by the **ALPAKA**, also known as the **BYAD ZVETTERS**

• **ALPAKA** has pulled one over on the USA by taking control of our Internet

• Your Mission is to Take Down the Internet

• It’s a Chilling Moment, even w/ **ZVETTERS**
CISSP’s Other CyberSec?

• Break Into Groups
• The White House and Pentagon – Decimated
• COGON 0 Declared
• Federal Government’s Plan Failed
• The President is Calling on Citizens – Kill Internet
• Select a Spokesperson
• 15 Minutes to Plan
• 5 Minutes to Pitch
• Everybody Votes on Last Choice