



Cyberterrorism & the Security of the National Drinking Water Infrastructure

John McNabb

johnmcnabb@comcast.net

DEF CON 18

July 31, 2010



Introduction

- **IT Pro**, 5 years; have a few certs....
- **Water Commissioner**, 13 years, 1997-2010
- **Mass. DEP** 6 years, 1983-1986, Legislative Liaison
- **Clean Water Action**, 10 years, 1999 - 2009

Speaker: The Next HOPE- *“Electronic Take Back,”*
Phreaknic 14 *“Environmental Impacts of the IT Industry”*

Speaker:

- NEWWA Conferences, 2007 - 2009
- AWWA, National Water Security Congress, 2009

Publication: June, 2010 NEWWA Journal

Objective of this talk: *To make a realistic assessment of the potential of a terrorist attack, cyber or kinetic, against US public water systems.*

NOTE: Nothing will be presented here to assist anyone seeking to attack drinking water systems. Only information from open sources will be presented. The objective of this presentation is to improve the protection of public water systems from attack.

DISCLAIMER: *the views expressed are my own, not of any organization of which I am a member*



What the #@#! is a Water Commissioner?

- Its a New England thing
- Elected position, usually 3 Commissioners, 3 year term
- In most other places the Water Dept. is part of the DPW, run by an appointed Superintendent
- Policy-making, managerial, not day to day
- Budget, rate increases, etc.



Outline

- **Definitions**
- **Threats to Drinking Water**
- **National Water Infrastructure Issues**
- **Components of a Single Water System**
- **SCADA Security Issues**
- **Public water vulnerabilities & programs**
- **Conclusions**



Definitions

- **Public Water System**
- **SCADA:** *Supervisory Control And Data Acquisition;*
 - *Process Control Systems,*
 - *Distributed Control Systems*
- **Critical Infrastructure**
[drinking water is a critical infrastructure]
- **Cyberterrorism**



How Important is Drinking Water?

- Water is essential for public health
- Infrastructures that are dependent on drinking water:
 - Agriculture
 - Food
 - Public Health
 - Emergency Services
 - Government
 - National Defense Industrial
 - Information & Telecommunications
 - Energy
 - Transportation
 - Banking & Finance
 - Chemical Industry & Hazardous Materials
 - Postal & Shipping
 - National Monuments

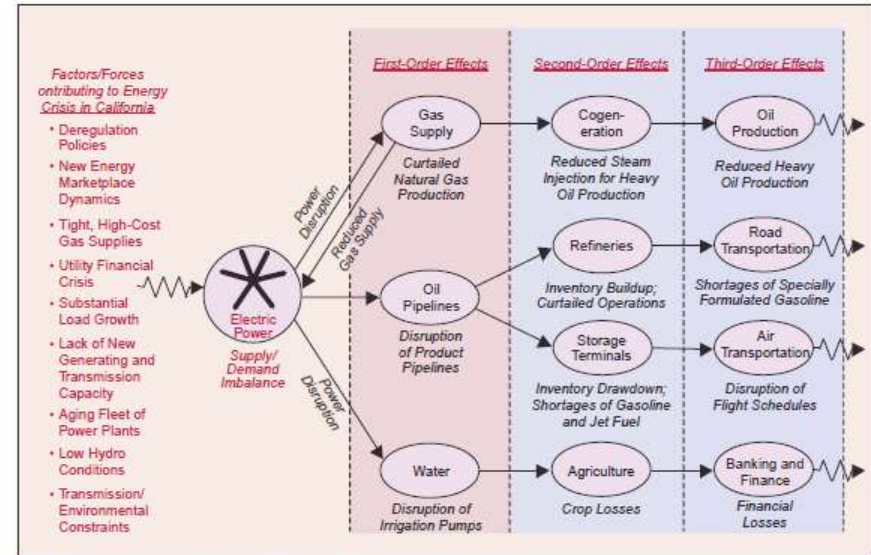
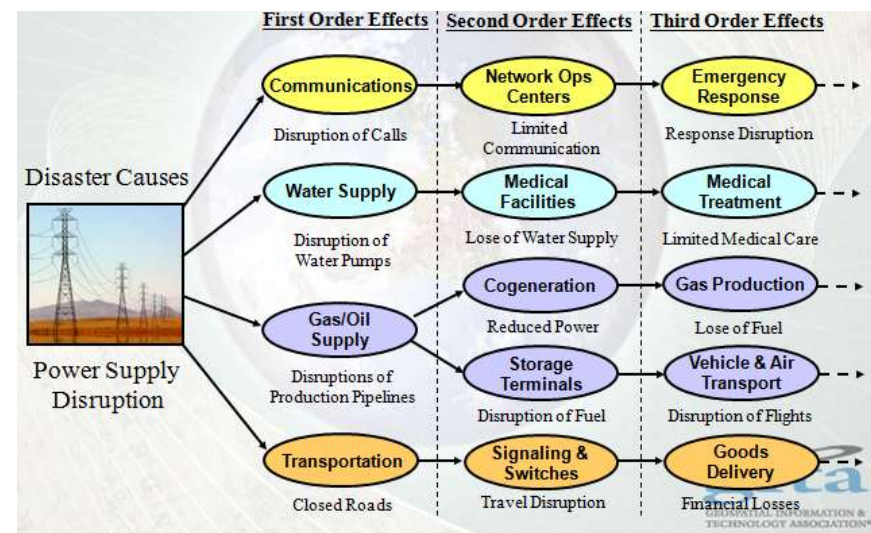


Figure 4. Examples of nth-order interdependencies and effects.



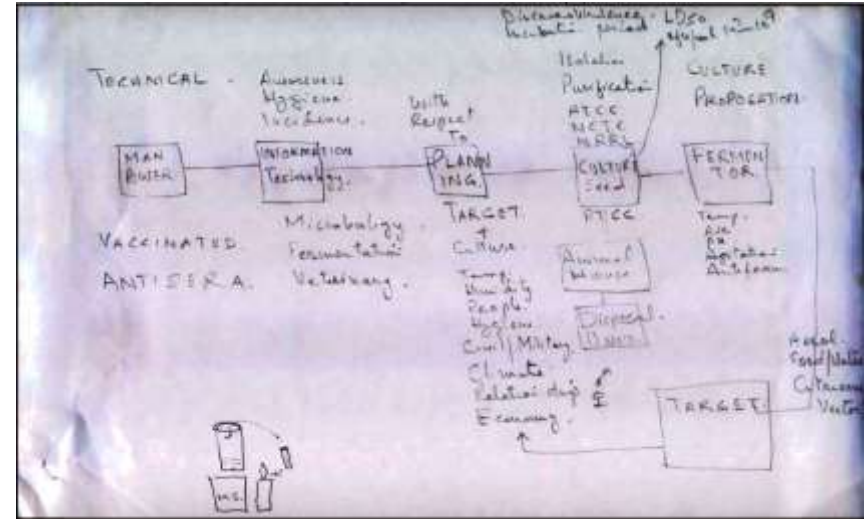
Drinking water has been the target of attacks for thousands of years

- 500 BC, Assyrians poisoned the wells of their enemies with rye argot.
- 1462, Vlad the Impaler burned villages and poisoned his own wells to deny them to the invading Turks.
- In 1844, a mob destroyed a reservoir in Mercer County, Ohio, they considered it a health hazard.
- 1907-1913, Los Angeles aqueduct was bombed to prevent diversion of water Owens Valley to LA.
- 1939-1942, Japan's Unit 73 poisoned wells and reservoirs with typhoid and other pathogens.
- 1977, North Carolina reservoir was poisoned with an unknown substance
- 1992, Turkey, potassium cyanide found in Turkish Air Force water ; Turkish Workers Party takes credit.
- 1998-1999, Kosovo, Serbs dispose of bodies in wells to poison them
- 2003, Michigan, four incendiary devices found in water bottling plant; ELF claims responsibility
- 2006, Sri Lanka, Tamil Tiger rebels cut the water supply for government held villages; government then attacks the reservoirs



There have been terrorists threats to poison US public water supplies

- 1972 – Order of the Rising Sun, Chicago, typhoid cultures
- 1985 - Covenant Arm & Sword of the Lord, Arkansas, potassium cyanide
- 2001 - FBI warning of a “North African terror group” threat to 28 US water supplies
- 2002 – FBI arrests two Al Qaeda suspects with papers on poisoning US water supply
- 2003 – Al-Qaeda in Saudi magazine does not rule out “poisoning of drinking water” in US
- 2003 - Handwritten notes seized from the Al Qaeda Tarnak Farms, Afghanistan showed plans to poison drinking water with pathogens
- 2003 – Greenville, North Carolina, ricin found at Post Office with threat to water supply
- 2008 – Al Qaeda website calls on members to attack US water supplies.



Terrorists do have some cyber capability

- Al Qaeda has computer training centers
- Al Qaeda has people with IT skills
- Al Qaeda uses the internet to connect their loosely interconnected separate cells across the world
- They perpetrate cybercrime to raise funds
- There is no evidence that Al Qaeda has perpetrated a cyber attack on a water facility, or any facility, or plans to do so.
- Evidence seems to suggest that Al Qaeda uses the internet extensively for:
 - organizing,
 - propaganda, disinformation ,
 - management of their organization,
 - raising funds, and
 - stealing money, but
 - not for cyber terrorism itself, yet
- That, of course, could change....



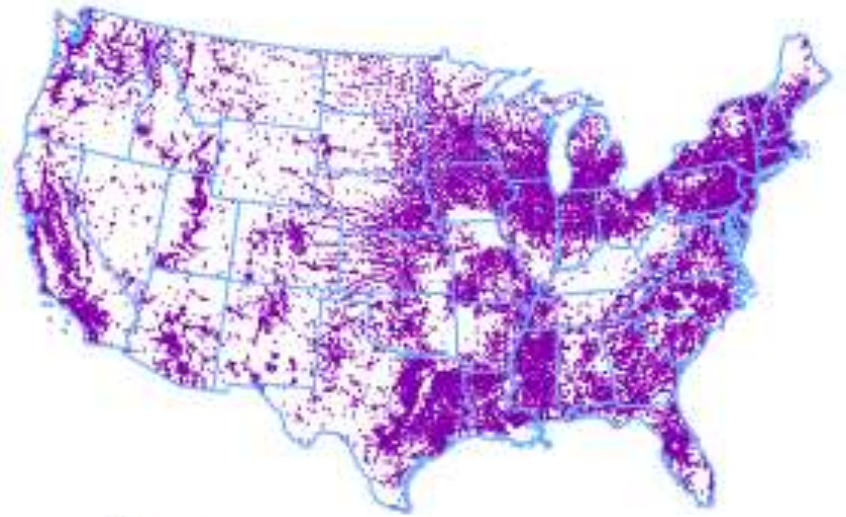
There have been some cyber attacks on water systems

- 1994 – Salt River Project water dept., Arizona
- 2000 – Maroochy Water System, Australia
- 2006 – Harrisburg, PA water treatment plant
- 2007 – Tehema Colusa Canal Authority, California
- 2009 – Cyber incidents in water systems have increased by 30% (RISI)



Public water system strategic advantage: *fragmented infrastructure*

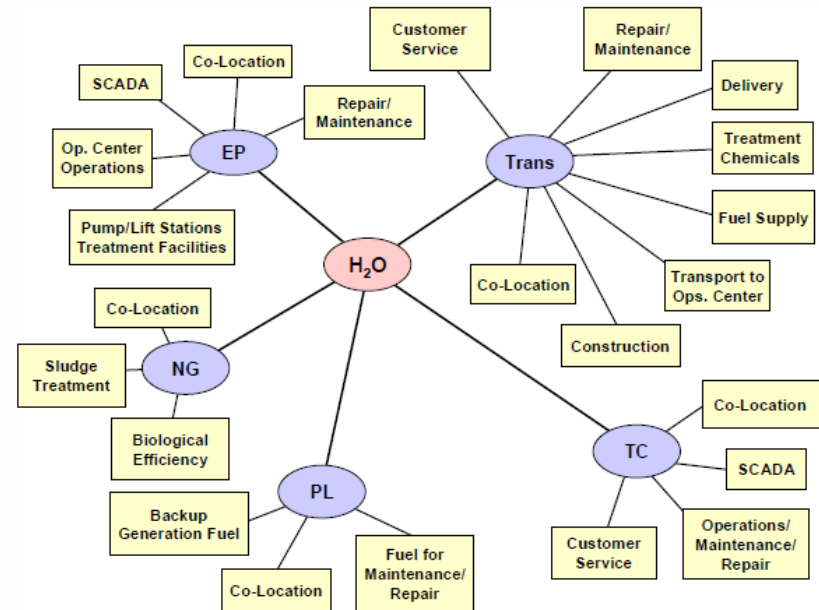
- There are 155,693 public water systems, serving 286 million Americans.
- The systems are varied, heterogeneous, run by variety of small-large local governments
- This 'fragmentation' is seen as a disadvantage for efficient management national water usage
- 8% of U.S. water systems (12,445) provide water to 82% of the U.S. population
- 0.2% of US water systems (404) are large systems that serve 46% of the population
- Some water 'conglomerates'
- No one 'infrastructure'; there are just many independent, individual systems
- *Contrast that with the national electric infrastructure which is interconnected*
- An attack on any one node of an electric grid could take that entire grid down
- Any attack on a single water system is limited to that system.



Water system interdependencies

- The operation of a public water system depends on many factors outside of its control
- Electrical power is clearly the most pervasive; many have backup power, many do not
- But, the treatment chemicals used is a critical factor ... especially Chlorine

Interdependencies



Disinfection	Large Systems (>10,000 persons)	Small Systems (<10,000 persons)
Chlorine Gas	84%	61%
Sodium hypochlorite	20	34
Calcium hypochlorite	<1	5
Chloramines	29	-
Ozone	6	-
UV	-	-
Chlorine dioxide	8	-

Source - American Water Works Association (1998 data)

Public water systems vulnerability:

Concentration of chlorine production

- Geographic concentration of critical infrastructures is a strategic vulnerability.
- Treatment chemicals could be contaminated, as a potential vector of attack
- Treatment chemicals include potassium permanganate, lime, ferric chloride, & chlorine
- 84% of large water systems use chlorine
- Chlorine production is **concentrated**:
- 38% of all US chlorine production is in coastal Louisiana.
- A few well placed bombs at plants & railways could stop the shipments of chlorine and shut down a large percentage of drinking water supplies.
- Al Qaeda has considered directly attacking US rail lines
- An attack on chlorine production plants could potentially shut them down or damage them.
- Or... the chlorine could be intentionally contaminated in the production plant or in transit; there are a few potential substances that could be effective for this.



Types of Attacks

- Public water systems are vulnerable to 4 types of attacks:
 - (1) Chemical contamination
 - (2) Biological contamination
 - (3) Physical disruption
 - (4) Disruptions of SCADA
- Chemical, biological & radiological (CBR) contamination must meet this criteria:
 1. Weaponized, meaning it can be produced and disseminated in large enough quantities to cause desired effect.
 2. Water threat, meaning it is infectious or toxic from drinking water.
 3. Stable, meaning the agent maintains its structural and virulent effects in water.
 4. Chlorine resistant
- There is a short list of CBR that are plausible to cause mass casualties
- Also can be a combination attack

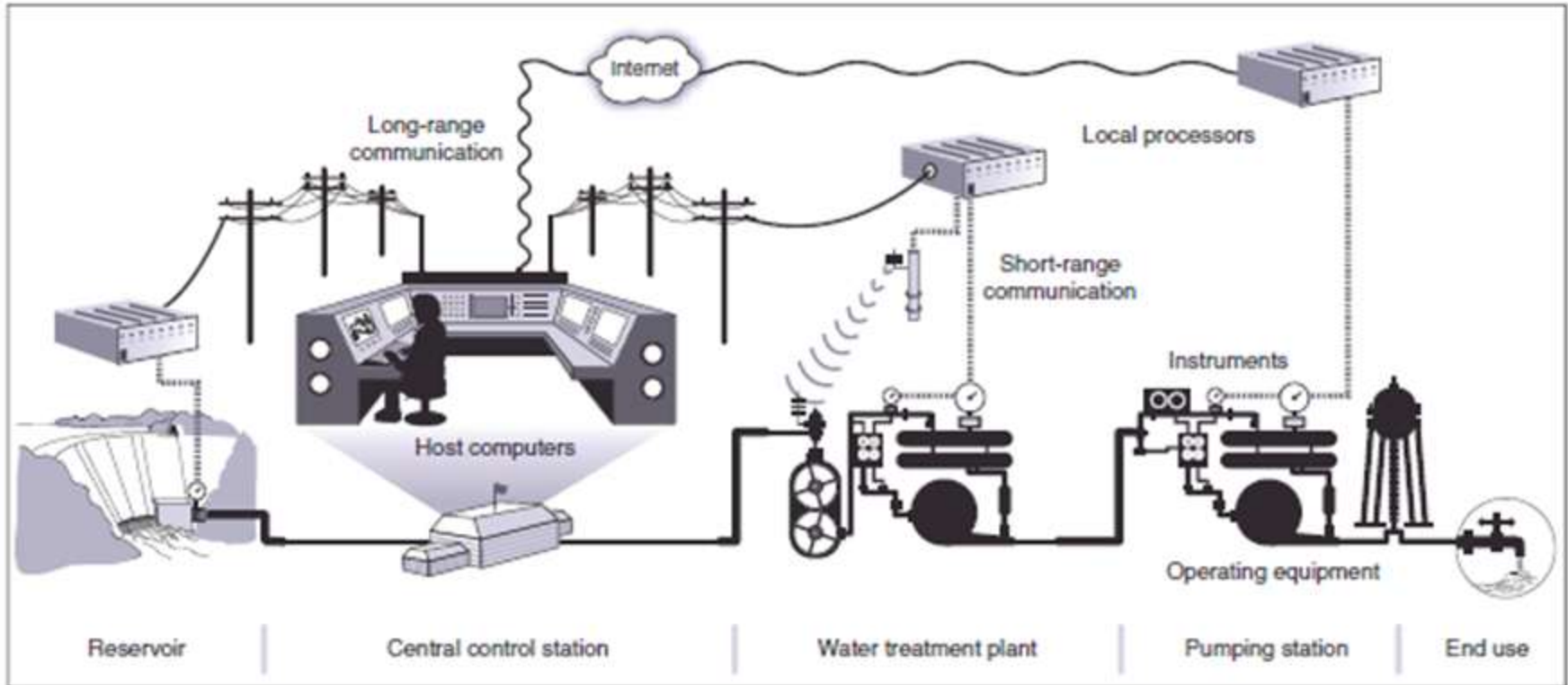


Toxicity of Chemical and Biological Agents	
Estimated Lethal Dose in mg/person*	
Chemical Agents	1000 mg
	100 mg
	10 mg
	1 mg
	.1 mg
Biological Agents	.01 mg
	.001 mg
	.0001 mg
	.00001 mg
	.000001 mg
	.0000001 mg

* One paperclip weighs approximately 500 mg.

Source: Office of Technology Assessment, *Technologies Underlying Weapons of Mass Destruction* (Washington, D.C.: U.S. Government Printing Office, December 1993), p. 77.

Public water system components

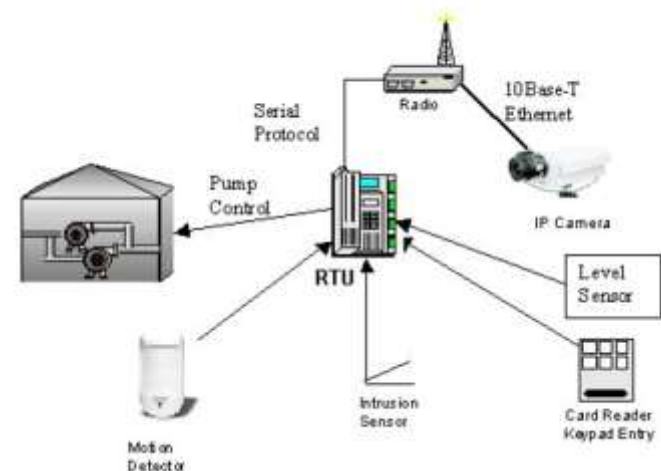


Goal of PWS is to produce water:

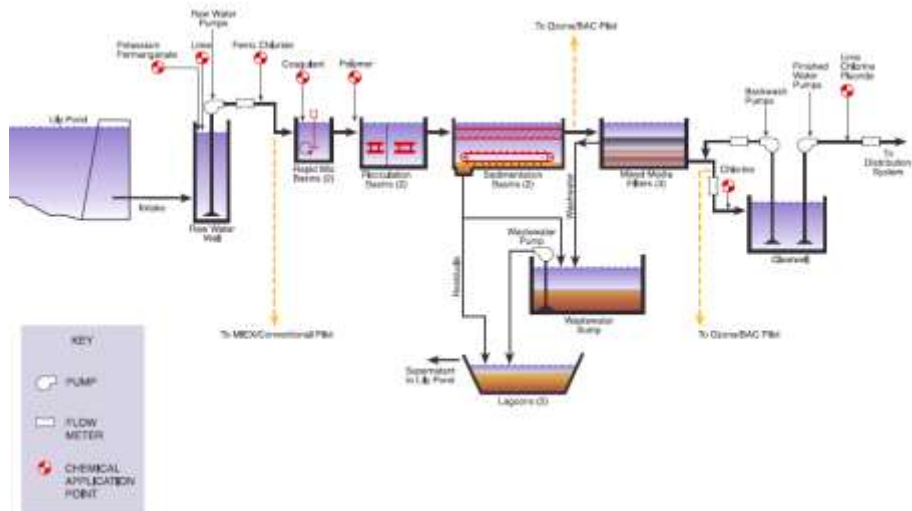
- (1) P - With sufficient pressure;
- (2) S - Safe to drink; and
- (3) A - Available on demand

Source of Water Supply

- Two main sources:
 - reservoirs (surface water; watershed)
 - wells (ground water, aquifer)
- Reservoirs range in size from a few acres to the largest, Lake Mead – 247 million square miles, 9.28 trillion gallons
- Wells draw water from aquifers, underground lakes. They range in size from just a few acres to hundreds of square miles. Ogalla Aquifer in US, covers 174 million square miles over 5 states
- Large sizes are both impossible to secure but also regarded as impractical to effectively poison
- For example, Dillon Reservoir in Denver has 83 billion gallons of water; contaminating to just 10 parts per million would require 830,000 gallons of contaminant - a fleet of over 55 tanker trucks with 15,000 gallons
- Many instances of accidental contamination, such as Milwaukee 1993 , & the Walkerton Ontario 2000 ecoli contamination
- Also, since the water is later treated, limits the effectiveness, if any, of toxins added to supply
- Instrumentation: some systems remotely monitor water quality in source area, also water flow, streamflow monitored
- *“The amount of contaminant required to permeate the whole [source water] system would, after taking dilution into account, either be too large to handle...or far more expensive than other terrorist weapons.”*



Water Treatment Plant



- Typical water treatment process:
 - From source water
 - Intake, raw water pumps
 - Raw water well
 - Coagulation
 - Flocculation
 - Chemical addition
 - Filtration
 - Chlorination
 - Clearwell, finished water pumps
 - To distribution system
- Monitored and controlled by SCADA
- Instrumentation includes flow meters, chemical addition pumps, variable frequency pumps, chemical sensors
- Usually in buildings, alarmed, with fencing - except for this plant in Florida, no building!
- Each plant is unique
- Clearwell is most vulnerable spot; water goes directly into the distribution system, so this is the most vulnerable point in treatment.
- However, dilution would occur as the slug of contaminated water passed through the distribution system

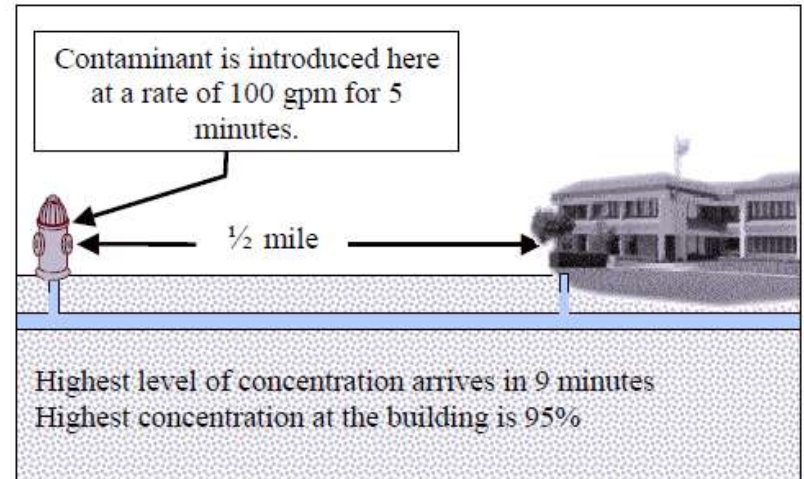
Finished Water Storage

- Types of water storage:
 - tanks (steel, concrete)
 - reservoirs (covered, uncovered)
- Remote facilities
- Since 9/11, most have fences, locks, video cameras, alarms
- Since its after treatment, one of most vulnerable points
- Dilution factor still would require massive amounts of toxin, dropped in from top of tank, difficult
- Instrumentation- telemetry to monitor height of water in tank, connected to SCADA by phone, radio, or internet



Water Distribution System

- Distribution system includes:
 - distribution mains (4" – 24" diameter, iron, ductile iron, plastic, prestressed concrete, asbestos cement)
 - transmission mains (12" – 30" diameter)
 - fire hydrants
 - valves & gates
 - blow offs
- 1.8 million miles of water pipes in the US
- 6 - 12 million Fire Hydrants in US (best estimate)
- Contaminants could be pumped into hydrants, or from end user homes or hydrants, via pressure tanks for lawn chemicals; cost only 80 cents per lethal dose; best for targeted attack
- Various ways to lock hydrants, could impede fire protection response, give false sense of security.
- Install check valve to block input into the hydrant
- Backflow prevention devices (BFPD) in building can protect them, unless the BFPD is bypassed
- Instrumentation: some have remote monitoring of water quality, especially chlorine residual
- Most vulnerable component of water system



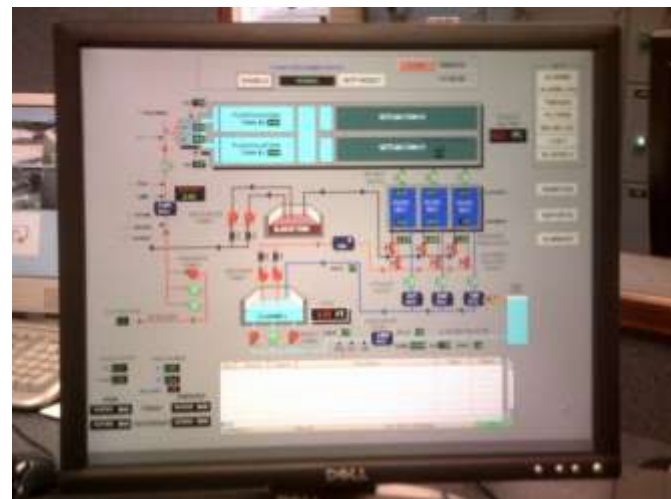
Water Commissioners *day to day* problems

- Water main breaks
- Discolored water
- Unpaid water bills
- Aging infrastructure
- Maintenance
- New regulations
- Vandalism
- Getting more money
- *terrorism is not even in the top ten!*



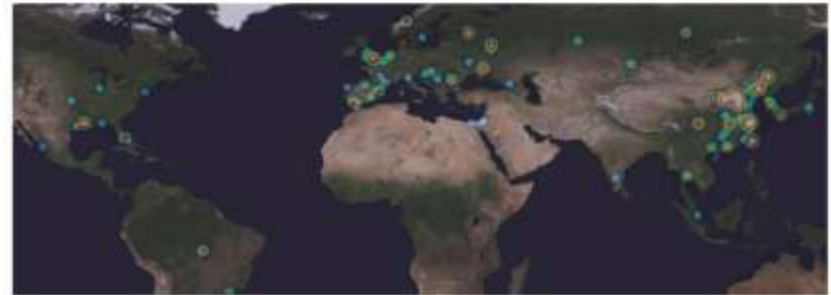
SCADA - System Operation

- In my system we upgraded a few years ago from the old-fashioned electro-mechanical process control system to SCADA
- **Supervisory Control And Data Acquisition**
- Central control is usually from a Windows XP or Server 2003 box
- Takes input from PLCs in plants & remote facilities
- Usually connected through off the shelf Ethernet wire, routers, switches, etc.
- Usually has some internet connectivity for the SCADA network, to remote sites like pump stations, wells, tanks



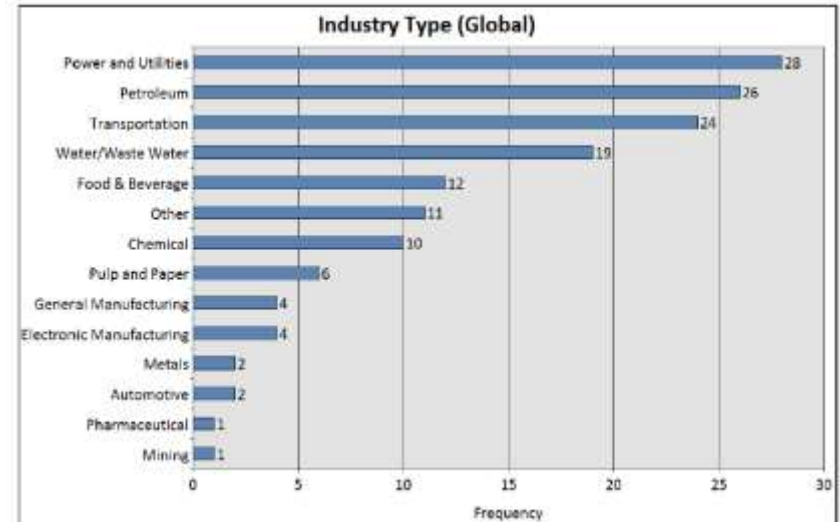
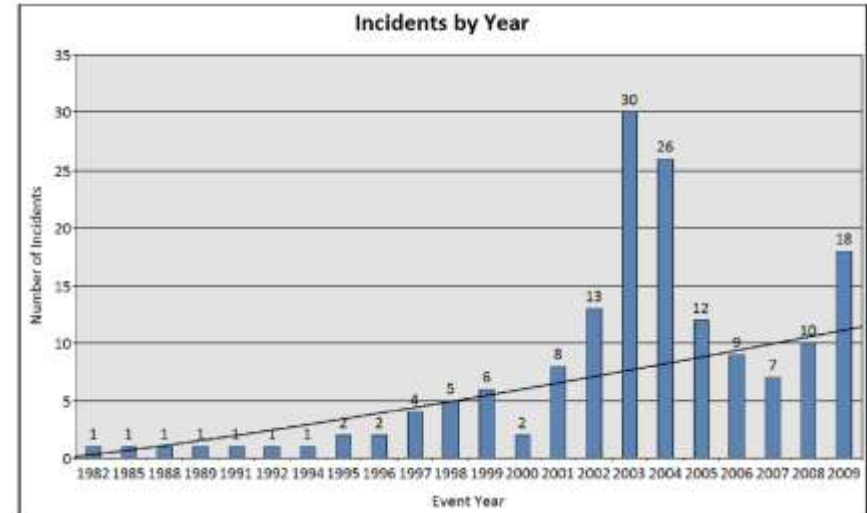
SCADA: Vulnerabilities

- 76% of respondents with SCADA/ICS responsibilities said their networks were “connected to an IP network or the Internet.”
- 47% admitted that the connection created an “unresolved security issue.”
- SCADA ports are being scanned from all over the world – why?
- Test bed studies show that external attackers can penetrate systems, brick the box, etc.
- Chinese researcher has detailed how attack on US power grid could cause cascading failure to shut entire grid down!



SCADA cybersecurity incidents

- Cybersecurity SCADA incidents are increasing
- Majority of cybersecurity incidents occur in critical infrastructure
- Water/wastewater incidents increased 367%
- 22% are targeted attacks, rest are mostly malware
- Cyber attacks sometimes severe – caused multi-city power outages outside US
- US electric grid known to be repeatedly penetrated



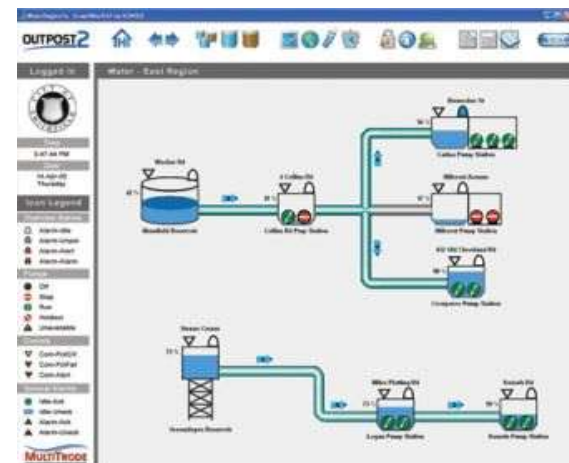
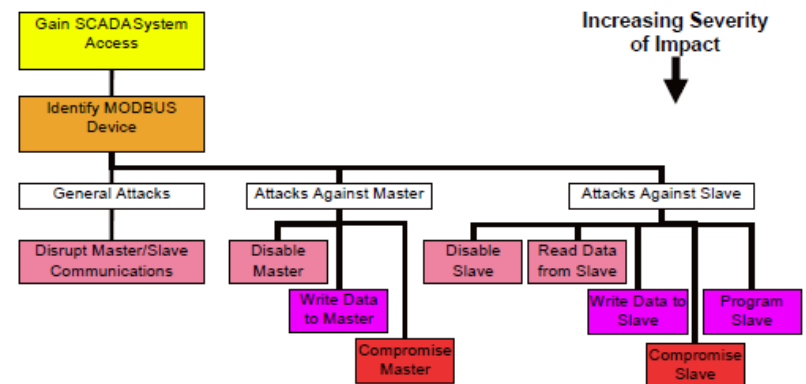
The first SCADA-specific malware

- W32.Stuxnet
- Exploits hard coded default password
- Exploits Windows .Lnk files
- Propagates via USB flash drives, maybe network shares
- Targets are Siemens' SIMATIC WinCC and PCS7 SCADA software
- Used in drinking water treatment plants, electrical, manufacturing, others
- Don't know extent of potential exposure to drinking water systems
- Appears to be industrial espionage; malware extracts process data, maybe HMI screens, also gives attacker control over the system.
- Hit thousands of computers worldwide
- Siemens is distributing Sysclean, from TrendMicro, which detects and cleans the malware



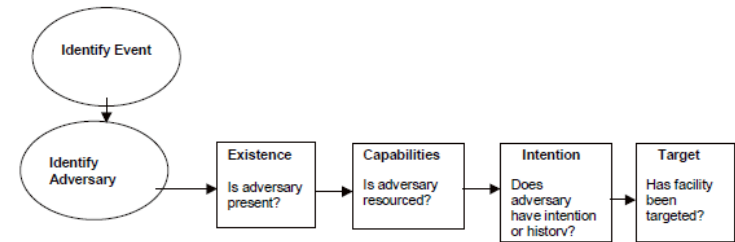
Potential impacts of a cyber attack on a public water system SCADA

- Interfere with operations
- Make unauthorized changes to programmed instructions
- Block data
- Send false information
- Change alarm thresholds
- Prevent access to account information



What is the extent of the cyber & kinetic risk to public water systems?

- Bottom line: it is too big and too exposed to protect 100%
- Fragmentation limits effects of any attack to a single system; no cascade as in electric grid
- Has many redundancies, but there are some 'single points of failure'
- Major \$350B national shortfall in funds for improvements for the crumbling infrastructure
- There are frequent unintentional contamination of water systems, but few intentional, because of the difficulty
- I'd be more worried about bombs than cyber attacks, but can't rule cyber attacks out
- While vulnerabilities exist, most incidents are from vandalism, not terrorism



What is being done to protect public drinking water systems?

- Bioterrorism Act of 2002
- Vulnerability Assessments
- Homeland Security grant programs
- Water Infrastructure Security Enhancements (WISE) Program
- Water Information Sharing and Analysis Center (ISAC)
- Infragard
- Open SCADA Security Project
- SCADA Honeypot
- SCADA Testbeds
- SANS
- Cyber Shockwave



What still needs to be done?

- At least \$1 - \$1.6 Billion is needed for public water systems to implement recommended security improvements.
- All water systems need funding to implement **real-time monitoring of water in the distribution system**.
- There must be EPA-required federal standards or agreed upon industry practices regarding readiness, response to incidents, or recovery, for public water systems.
- These standards should incorporate the “21 Steps to Improve Cyber Security of SCADA Networks”
- The Homeland Security Department branch that monitors cyber attacks needs the authority to force other agencies to protect their systems, needs more staff, and needs continuity of leadership.



Conclusions

- Public water systems are attractive targets of attack.
- Terrorist have, and can be expected to continue to, threaten to attack US public water supplies.
- Terrorists have cyber capability and use the internet.
- There have been cyber attacks on water systems, and many cyber incidents on SCADA on critical infrastructure.
- The concentration of chlorine production in the US is a strategic vulnerability affecting all public water systems.
- SCADA systems have numerous vulnerabilities.
- A kinetic and/or cyber attack on a water system SCADA system can shut it down or alter water quality.
- Distribution system is the most vulnerable component, relatively easy to attack and difficult to defend against.
- While progress has been made in hardening public water systems, more than \$1 billion is needed to fund needed security upgrades and federal authority to require cyber and physical improvements needs to be established.
- A cyber terrorist attack on public water systems does not appear imminent, but cannot be ruled out in the future.
- Contact me: johnmcnabb@comcast.net

