Planning for Certain High Risk Security Incidents

Internet2 Member Meeting, San Diego
San Diego Room, 8:45 AM, October 11th, 2007

Joe St Sauver, Ph.D.
Internet2 Security Programs Manager
Internet2 and the University of Oregon
(joe@uoregon.edu or joe@internet2.edu)

http://www.uoregon.edu/~joe/highrisk/

Notes: All opinions expressed in this talk are strictly those of the author. These slides are provided in detailed format for ease of indexing, for the convenience of those who can't attend today's session in person, and to insure accessibility for both the hearing impaired and for those for whom English is a secondary language.

I. Introduction

Today's Talk

- Today we're going to talk about two unusual threats: **high altitude electromagnetic pulse (EMP) effects and pandemic flu**.
- Those may seem like a couple of odd topics. After all, aren't system and network security guys supposed to worry about stuff like network firewalls, hacked systems, denial of service attacks, computer viruses, patching, and when you last changed your password? Sure. No question about it, those are all important system- and network-related security topics, and those are all topics which have been covered repeatedly in a variety of fora.
- Given all those sort of mundane threats, it can be hard to think about **"throw it long"/less-talked-about threats** -- after all, there are just too many high profile day-to-day operational IT security threats which we have to worry about instead, right? No – emphatically no! You need to worry about **both** the day-to-day stuff, and the really bad (but thankfully less common) stuff, too.

What Do EMP and Pandemic Flu Have In Common? Both Are National Scale Threats

- "We need to plan for a class of national scale disasters that pose a significantly greater challenge than local or even regional disasters such as Hurricane Katrina. **Examples include nuclear EMP and national scale epidemics.** Such national scale disasters deserve particular attention to preparedness and recovery since assistance from non-affected regions of the nation could be scarce or non-existent. **A major problem with such disasters is maintaining communication and transportation line connectivity.** Communities and regions become isolated making it difficult to maintain their survival."

Proceedings of the 2006 Spring Research Symposium, Homeland Security: Engaging the Frontlines, Institute for Infrastructure and Information Assurance, James Madison University, in cooperation with the National Academic of Sciences Federal Facilities Council, IIIA Publication 07-02, "Emergent Themes" section, section 1, page 5 [emphasis added]

Why Talk About Those Threats Here?

- It is perfectly valid to ask why we should talk about these sort of threats here. I think there are many good reasons, including:
  -- One explicit activity of the Internet2 Middleware and Security Group is **Salsa-DR**, Internet2's disaster recovery and business continuity working group. Obviously, today's topics align very well with that defined focus area.
  -- This community controls **critical Internet infrastructure**, and has 24x7 **operational responsibilities** which go along with that. Because of that, operational threats which can jeopardize critical shared facilities demand our attention as a community.
  -- The high performance R&E networking community works closely with government, the international community, vendors and commercial networks, and part of that work includes **providing leadership** on emerging network centric issues such as the security topics we'll be talking about today.

Why Talk About These Issues Now?

- We've been **preoccupied** over the last few years. As a nation, we needed to take care of the vulnerabilities which were exploited on **9/11**, and we've also needed to devote a tremendous number of resources to fighting wars in **Iraq** and **Afghanistan**. Now that we've done most of what we can to fix the vulnerabilities of 9/11, and we're making progress toward transitioning our responsibilities abroad, it is time for the nation to revisit other critical national security priorities.
- As you'll see later in this talk, **conditions relating to these issues have evolved over time, and are now becoming ripe**. We'll talk more about that later in this talk.
- Time continues to go by, time that we **could** be using to mitigate these threats and to prepare our networks, our campuses and our families. **We can't afford to waste any more time**.

"What Is It That You Want Us to Do?"

- Let me keep it simple. There are **three things** I'd like you to do once we're done here today:

  -- Take appropriate steps to harden your own networks against electromagnetic pulse effects (I'll tell you how to do this later in this talk)

  -- Begin planning for how you'll cope with pandemic flu, if it affects the United States

  -- As opinion leaders, talk with others folks about these issues

- Let's start by talking about electromagnetic pulse effects.

II. Electromagnetic Pulse:
A Non-Technical Introduction

How Can We Understand and Appreciate a Threat We've Never Directly Experienced?

- It is hard to "wrap your head" around a risk that none of us have ever directly "been through."
- I finally decided that the best way -- really the **only** way -- to tell the EMP story, a story with some very hard and very factual material, would be to start with a short fictional tale, a "historical narrative from a future not yet seen," explaining how one individual might personally experience an electromagnetic pulse attack.
- So, all you technical folks, we'll get to the nuts and bolts in just a minute, but before we do, let me just begin by pulling out my crystal ball to "remember a story from the future." Maybe, if we're lucky, this story can help us to sort of "vicariously experience" what an electromagnetic pulse event might be like.
- I hope you'll forgive this approach, and please remember that at root, "all transmission of knowledge is about story telling."

A Hypothetical Future Narrative

"It was December 7th, 2008, a beautiful crisp and cold late Sunday afternoon, when the EMP attack happened. I was outside, admiring the Christmas lights I'd just finished putting up twinkle, when the high altitude nuke exploded hundreds of miles away.

"It didn't feel like a nuke. There **was** a blindingly bright flash, but no sound, no hurricane winds, no waves of heat, and no stereotypical mushroom cloud. It was just as if some immensely powerful photographer's strobe had gone off somewhere very high above the middle of the country.

"Even though I happened to be looking away from the nuke when it went off, the light still seemed to reflect off of everything, and it took a minute for my vision to come back. When I got done rubbing my eyes, the sun was still shining, the sky was still blue and we were all still alive, but all my Christmas lights were out.

"As we tried to figure out what had happened, we found out that more than just our Christmas lights were out. All the lights in our house were out, too, and the TV and our radios smelled funny and wouldn't come on, either. As our neighbors came out from their houses, we learned that their power was out, too. We tried to call the power company to report the problem, but there was no dial tone, and our cell phones also didn't work.

"That night my wife and I found some candles and we had a fire in the fireplace, and cooked dinner out over the gas BBQ. At bed time we dug out more blankets before calling it an early night, confident that on Monday things would be back to normal.

"Unfortunately, when we woke up on Monday, the electricity was still out. We wondered what was happening at work, and tried calling in, but the phones were still dead. We finally decided to get in the car and get some groceries and some more propane for the grill, but we didn't get far because neither of our cars would start.

"As time went by, we learned that all of our problem with electrical and electronic things wasn't something unique to just us, or just to our neighborhood or city or state, but something which had happened to the entire country all at once, apparently part of some intentional attack on America, we still don't know for sure.

"Over time some things got better, and some things got worse -- the famines and food riots of 2009 were probably the worst of it for us. On the other hand, when the power did finally came back on in some places, we learned that some electrical stuff was actually okay, and other electrical stuff just needed new fuses or needed to have tripped circuit breakers reset.

"But the most sophisticated stuff, the stuff with embedded microprocessors or integrated circuits, well, virtually all of that stuff was dead. All the modern electrical gadgets were toast, as if there'd been a single nationwide lightning strike, and no one had bothered to protect their systems with surge suppressors.

"We quickly came to appreciate that computers were hidden everywhere. Even though it was a cold winter, gas and heating oil was in short supply because the computers which controlled the pipelines had all been knocked out. Food, particularly the sorts of things that most of us would pick up every few days, things like milk, eggs, bread and fresh fruits and vegetables, those things disappeared like smoke in the wind. We also came to understand that most pharmacies carried only a few days worth of drugs on hand, relying on daily deliveries for any exotic medications, and even for daily resupply of the common stuff as it was sold.

"Heck, we also learned that without computers you didn't really have any money except for the cash in your pocket. Without computers you couldn't buy things with credit cards, and checks were equally meaningless. The stores that did still have supplies were all "cash only," but most of us only had maybe a couple hundred bucks in cash, even if we'd had plenty of "electronic money" before the attack took place. Barter became the norm.

"Travel was hard, too. Even if you were one of the lucky ones who had a car which made it through the attack okay, and you had gas, the roads were clogged with all the other cars which had been shorted out, or which had simply been abandoned. Then, when a fluke heavy winter snow storm hit from out of nowhere, that was it -- all the roads were locked down till spring. The lucky ones had cross country skis, or snow machines, or just good winter boots.

"**The toughest thing about all this was that we just weren't ready, we just weren't expecting it. No one had explained to us that there was a threat which could wipe out most of our electrical and electronic items in the blink of an eye -- and not just the electronics in one city, but electrical and electronic items all across the country, and all from just one nuke.**

"We always worried about Bin Laden and the other terrorists hitting some big city with a nuke, but we never worried about an EMP strike. Of course, if someone had told us about EMP, we probably wouldn't have believed them anyway…"

That's The End of the "Fictional Narrative" Part of This Talk

- We'll leave our fictional account here, even though it wouldn't be hard to continue to tell this story at the length of a novel. How we'd experience life without electronics or electricity is something provocative to ponder, but we don't need to explicitly follow that path any further here – I think we can all imagine the tremendous challenges we'd all be facing in that sort of world.
- A couple of quick additional points:

  -- Everything from here on out is strictly factual, and I've tried hard to provide sources for further study throughout.

  -- To the best of my knowledge, all the information in today's talk has come from publicly available sources, and this talk should not in any way exacerbate any pre-existing risks our country and its citizens already face.

When It Comes to EMP, Authorities Have Been Trying To Warn Us Since at Least 1997

- "EMP does not distinguish between military and civilian systems. Unhardended systems, such as commercial power grids, **telecommunications networks, and computing systems**, remain vulnerable to widespread outages and upsets due to HEMP. While DoD hardens assets it deems vital, no comparable civil program exists. **Thus, the detonation of one or a few high-altitude nuclear weapons could result in devastating problems for the entire U.S. commercial infrastructure."**

Statement of Dr. George W. Ullrich, Deputy Director, Defense Special Weapons Agency, Threats Posed by Electromagnetic Pulse to U.S. Military Systems and Civilian Infrastructure, July 16, 1997, House Military Research & Development Subcommittee [emphasis added]
http://www.fas.org/spp/starwars/congress/1997_h/h970716u.htm

And Those Efforts Have Continued Over Time... Congressman Roscoe Bartlett, 2004:

"On the same day [that] the 9/11 Commission Report asked our country to look in the rear view mirror to find out why America failed to prevent that terrorist attack, **Congress was warned that we are vulnerable and virtually unprotected against an EMP attack that could damage or destroy civilian and military critical electronic infrastructures, triggering catastrophic consequences that could cause the permanent collapse of our society.**

"The Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack reported on July 22, 2004 that "the current vulnerability of our critical infrastructures can both invite and reward an [EMP] attack if not corrected.

"**A single unsophisticated nuclear missile detonated at high altitude could produce an EMP attack that damages or destroys electronic systems across the entire continental United States**. Satellites in low earth orbit would also be damaged. Millions of Americans could die from starvation and disease as an indirect consequence of an EMP attack that disrupts the infrastructures for transportation, medical services, food and water. However, the most important finding of the EMP Commission is that this threat can be greatly mitigated at modest cost and in 3-5 years.

"Responding to the EMP Commission report, **The Wall Street Journal editorialized on August 12, 'All we can say is, we hope someone in Washington is paying attention.'"** [emphasis added]

Letter from Congressman Roscoe G. Bartlett, Ph.D. (R-MD)
http://www.house.gov/hensarling/rsc/doc/Bartlett--EMP.pdf

Have We As a Nation Been Paying Attention To These Warnings?

- Unfortunately no. For example, the report of the Congressional Blue Ribbon EMP Commission* came out the same day as the Congressional 9/11 Commission report, so unfortunately the findings of the EMP Commission largely got "lost in the noise."
- Three years later, while many key recommendations of the 9/11 Commission have been implemented,** the equally important (or more important!) recommendations of the EMP Commission have largely been overlooked. Evidence of this can be seen in the fact that most Americans don't know about EMP -- they don't know what EMP is, how EMP occurs, or how critical infrastructure can be protected from it.

* See www.globalsecurity.org/wmd/library/congress/2004_r/04-07-22emp.pdf

** "Implementing the 9/11 Commission Recommendations Act of 2007," July 27, 2007, http://homeland.house.gov/SiteDocuments/20070727182653-51415.pdf

Why *Hasn't* The Government Worked to Harden Civilian Infrastructure Against The EMP Threat?

- Some people haven't believed that electromagnetic pulse is a real threat. For example, in 1997, General Robert T. Marsh, Retired, Chairman of the President's Commission on Critical Infrastructure Protection stated,

  "I do not see any evidence that suggests capabilities seriously threatening our critical infrastructure. [...] There are many easier, less costly, and more dramatic ways for terrorists to use nuclear weapons than delivery to a high altitude. Such an event is so unlikely and difficult to achieve that I do not believe it warrants serious concern at this time. The administration's policy is to prevent proliferation and unauthorized access."

  http://www.fas.org/spp/starwars/congress/1997_h/has197010_1.htm

Not Everyone Agrees With General Marsh

"If you had a few or perhaps only one or two nuclear weapons, you probably would want to use them in the fashion which imposes the largest damage expectancy on the United States and its military forces.

"If you are going to go after the military forces and you only have a few, by far and away the most effective way that you could potentially use it is an EMP laydown. If you were going against the American civilization itself, again, the largest damage you could expect to see by far is that associated with EMP laydown.

"As I said earlier, a large laydown over the lower 48 States has a damage expectancy which can be reckoned in trillions of dollars. Not 10 trillion, but well above a trillion dollars. So what you get the most bang for your nuclear buck out of, you get it out of most heavily damaging your adversary in either the military sense or the sense of civilian infrastructure. EMP is the attack mode of choice."

Dr. Lowell Wood, LLNL, Congressional Hearings on the Threat Posed by Electromagnetic Pulse (EMP) to U.S. Military Systems and Civil Infrastructure, July 16, 1997, www.fas.org/spp/starwars/congress/1997_h/has197010_1.htm

Defense Threat Reduction Agency (DTRA) Report to the Defense Science Board (DSB) Task Force on Nuclear Weapon Effects Test, Evaluation, and Simulation, April 2005

Ten Likely, High Consequence Nuclear Threat Scenarios
Thermonuclear 3rd party asymmetric – high alt
Fission asymmetric against U.S. – high alt
Fission 3rd party parity – high alt
IND terrorist against U.S. - surface
IND terrorist against 3rd party - surface
RDD terrorist against U.S. - surface
HE against nuc/rad terrorist against U.S. - surface
HE against nuc/rad 3rd party parity - surface
HE against nuc/rad 3rd party asymmetric - surface
HE against nuc/rad terrorist against 3rd party - surface

A recent analysis of possible nuclear threat scenarios against U.S. interests by experts in the field revealed the extent that the landscape has changed since the Cold War ended. Whereas the Cold War demanded that we address massive use of large yield nuclear weapons by peer adversaries and survivability of retaliatory strategic assets, the current environment emphasizes low yield terrorist or rogue nation use and survivability of infrastructure and mission capability. By analyzing a broad range of possible scenarios in terms of probability and consequence, experts concluded that the threats the U.S. should be most concerned with ranged from single, high-altitude use to terrorist devices in cities and conventional explosives at nuclear sites. The nuclear weapon effects community is fairly well equipped to predict high-altitude nuclear effects, but confidently predicting effects from terrorist use in cities and explosions against nuclear sites represents a new direction that must be addressed. However, in all areas, including the high-altitude effects area, U.S. capability is dwindling as experts age and retire without significant influx of new personnel.

http://www.acq.osd.mil/dsb/reports/2005-04-NWE_Report%20_Final.pdf at pdf pp. 121

Foreign Entities Are Also Clear About the EMP Threat

- *Peter V. Pry wrote:* Chinese military writings are replete with references to the dependency of United States military forces and civilian infrastructure upon sophisticated electronic systems, and to the potential vulnerability of those systems. For example, consider this quote from an official newspaper of the PLA: "Some people might think that things similar to the 'Pearl Harbor Incident' are unlikely to take place during the information age. Yet it could be regarded as the 'Pearl Harbor Incident' of the 21st century if a surprise attack is conducted against the enemy's crucial information systems of command, control, and communications by such means as...electromagnetic pulse weapons....Even a superpower like the United States, which possesses nuclear missiles and powerful armed forces, cannot guarantee its immunity...In their own words, a highly computerized open society like the United States is extremely vulnerable to electronic attacks from all sides. This is because the U.S. economy, from banks to telephone systems and from power plants to iron and steel works, relies entirely on computer networks....When a country grows increasingly powerful economically and technologically...it will become increasingly dependent on modern information systems....The United States is more vulnerable to attacks than any other country in the world." (Zhang Shouqi and Sun Xuegui, Jiefangjun Bao, 14 May 1996)

  Comments by Dr. Peter V. Pry, EMP Commission Staff, before the US Senate Subcommittee on Terrorism, Technology and Homeland Security, March 8, 2005; see http://kyl.senate.gov/legis_center/subdocs/030805_pry.pdf at page 3.

Isn't There At Least Some Federal Agency Tasked With Explicit Responsibility for EMP Issues?

- The National Communications System, a branch of DHS which was formerly an office under the Department of Defense, is the focal point for EMP preparedness in as it relates to telecommunications. See Part 215, Title 47, Chapter II, Code of Federal Regulations, http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?c=ecfr&tpl=/ecfrbrowse/Title47/47cfr215_main_02.tpl
- You can visit the National Communications System website at http://www.ncs.gov/ EMP is **not** the focal point of that site. The most recent major EMP-related document I found there was NCS Directive 4-2, dated January 31st, 1992 and signed by Brent Scowcroft. Among other things, it defines telecommunications as excluding power transmission systems, and directs that "The NCS will support development of appropriate protection from EMP effects on telecommunication facilities."

Unfortunately NCS Appear To Be Primarily Concerned With Telephones, Not the Internet, and They May Be Rather Overly Optimistic

- "We have tested thoroughly our current generation of core telecommunication switches and have determined that there is minimal lasting EMP effect on these switches. Furthermore, most of our core communications assets are in large, very well constructed facilities which provide a measure of shielding. This situation will evolve as we move to Next Generation Networks, NGN, but we are monitoring this network evolution by testing critical components of the NGN and leveraging DOD testing."

  Dr. Peter M. Fonash, Acting Deputy Manager, NCS, March 8, 2005, "Terrorism and the EMP Threat to Homeland Security," Subcommittee on Terrorism, Technology and Homeland Security of the Committee on the Judiciary, available online at http://www.terrorisminfo.mipt.org/pdf/s-hrg109-30.pdf at pdf pp. 5 9.

Speaking of Civilian Telecom System Tests...

- "I am familiar with some of the civilian telecommunications tests, in particular a number five electronic switching system test that was done in the Aries simulator, which I did the preliminary design for in 1968. The cables that normally extend hundreds of miles into that system were represented by cables coiled up and placed under the mobile vans it was carried in. So, as we mentioned earlier, that is certainly not a good representation of the stress that the system would receive. I am not trying to say that this is the complete work that has been done, but it is indicative of the concerns that a review of the subject by your committee might find both informative for you and beneficial for the defense authorities."

  William Graham, President and CEO, National Security Research, http://commdocs.house.gov/committees/security/has280010.000/has280010_0.HTM October 7th, 1999

What About EMP and Power Delivery?

- Because power transmission is explicitly excluded from NCS' EMP responsibilities, who in the federal government would logically have responsibility for insuring the security of that area? That would be the DOE (see HSPD-7 at paragraph 18 (d), www.whitehouse.gov/news/releases/2003/12/20031217-5.html).
- Looking at DOE's structure, I believe the relevant office would be the DOE Office of Electricity Delivery and Energy Reliability Infrastructure Security and Energy Restoration Programs, see http://www.oe.energy.gov/infrastructure.htm (although other DOE activities, such as national lab resources, would obviously also be relevant to dealing with the EMP threat to civilian power infrastructure). Unfortunately, I see no evidence that protecting civilian power infrastructure from electromagnetic pulse is a public priority for that office. If I've missed it, my apologies, and if folks would let me know where I can find public info about federal EMP power hardening activities, that would be great.

Non-Public DHS Sector Specific Critical Infrastructure Protection Plans

- At this point I should also acknowledge that there are a number of Department of Homeland Security Critical Infrastructure Protection Sector Specific Plans which are NOT publicly available. These documents, classified For Official Use Only, are mentioned at http://www.dhs.gov/xprevprot/programs/gc_1179866197607.shtm
- The Communications Sector plan and the Information Technology plan, along with most others, are unclassified, and anyone can review them, but the Energy sector plan, in particular, is not available due to its FOUO classification.
- It's possible that that plan includes explicit coverage of EMP-related threats, but since that plan is closely held, we really have no way of knowing, and I think we as Americans deserve to know if the EMP-related threats to our power delivery systems are being aggressively and conclusively addressed.

III. Technical Aspects of EMP

Electromagnetic Pulse Effects, in One Page

- Electromagnetic pulse (EMP) effects are typically caused by the detonation of a nuclear weapon at high altitude, typically burst altitudes of 40 to 400 kilometers.
- Prompt gamma rays from such an explosion travel outward and are captured in the uppermost atmosphere in what's known as a "deposition region."
- Within the deposition region, those gamma rays interact with air molecules via multiple effects, with the largest number of high energetic free electrons being produced via the Compton Effect.
- Those highly energetic free electrons, generated within an extremely short time and interacting with the earth's geomagnetic field, can result in voltages in excess of 50kV capable of upsetting or killing sensitive electrical and electronic gear over a wide area.

Chapter XI, Glasstone & Dolan, "Effects of Nuclear Weapons,"
http://www.princeton.edu/~globsec/publications/effects/effects.shtml

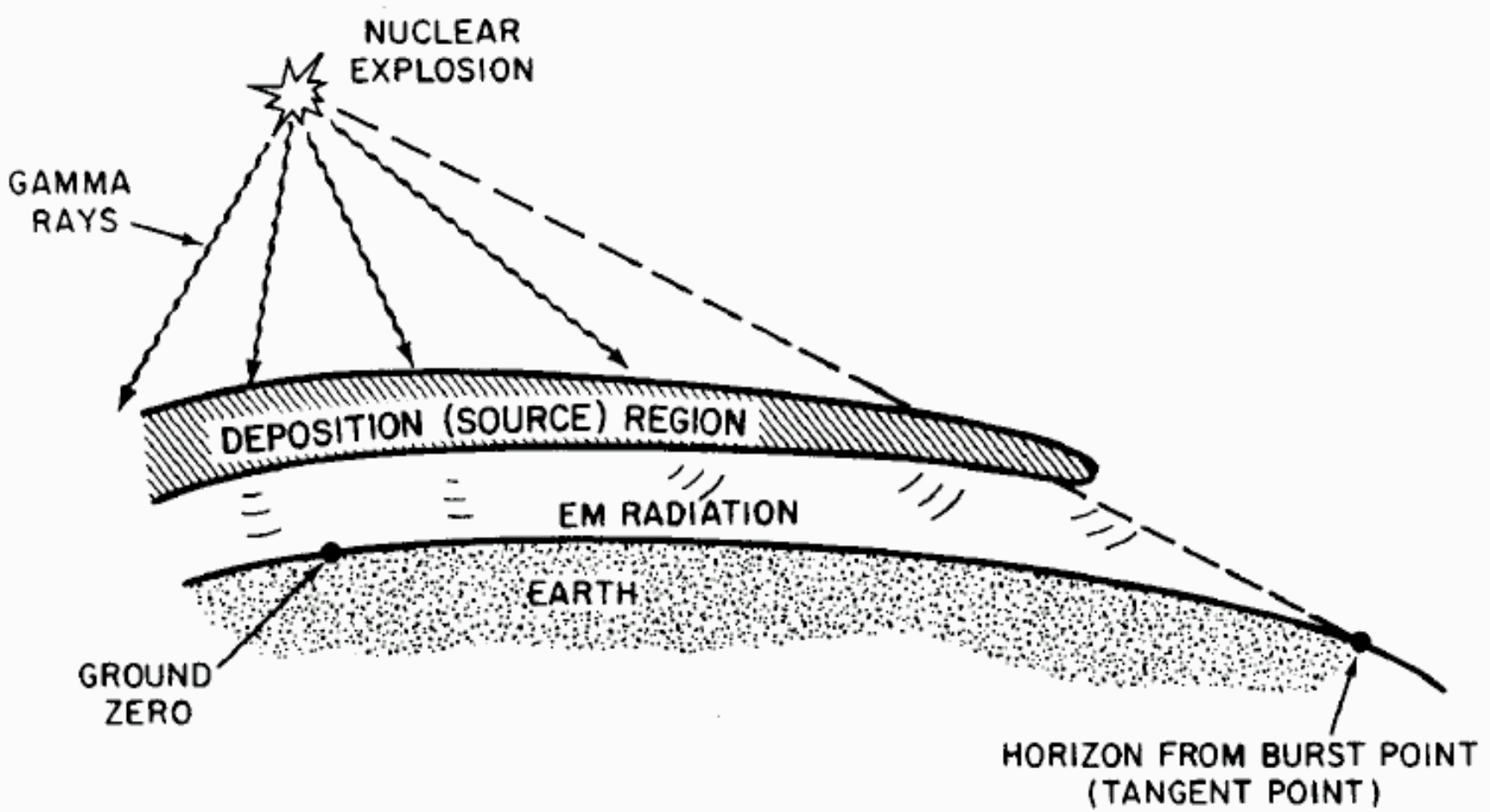


Figure 11.13. Schematic representation of the EMP in a high-altitude burst. (The extent of the deposition region varies with the altitude and the yield of the explosion.)

Source: http://www.princeton.edu/~globsec/publications/effects/effects11.pdf

EMP: A Line of Site Phenomena

- These effects all occur within **line of site** of the burst. To compute the extent of the effect, calculate the tangent radius as:

  $R(\text{tangent}) = R(\text{earth}) \cos^{-1} (R(\text{earth}) / (R(\text{earth}) + \text{HOB}))$
  where R(earth) equals approximately 6371 km

Height of burst:	Approximate effects radius:
40 km	712 km
50 km	796 km
100 km	1,121 km
200 km	1,576 km
300 km	1,918 km
400 km	2,201 km*

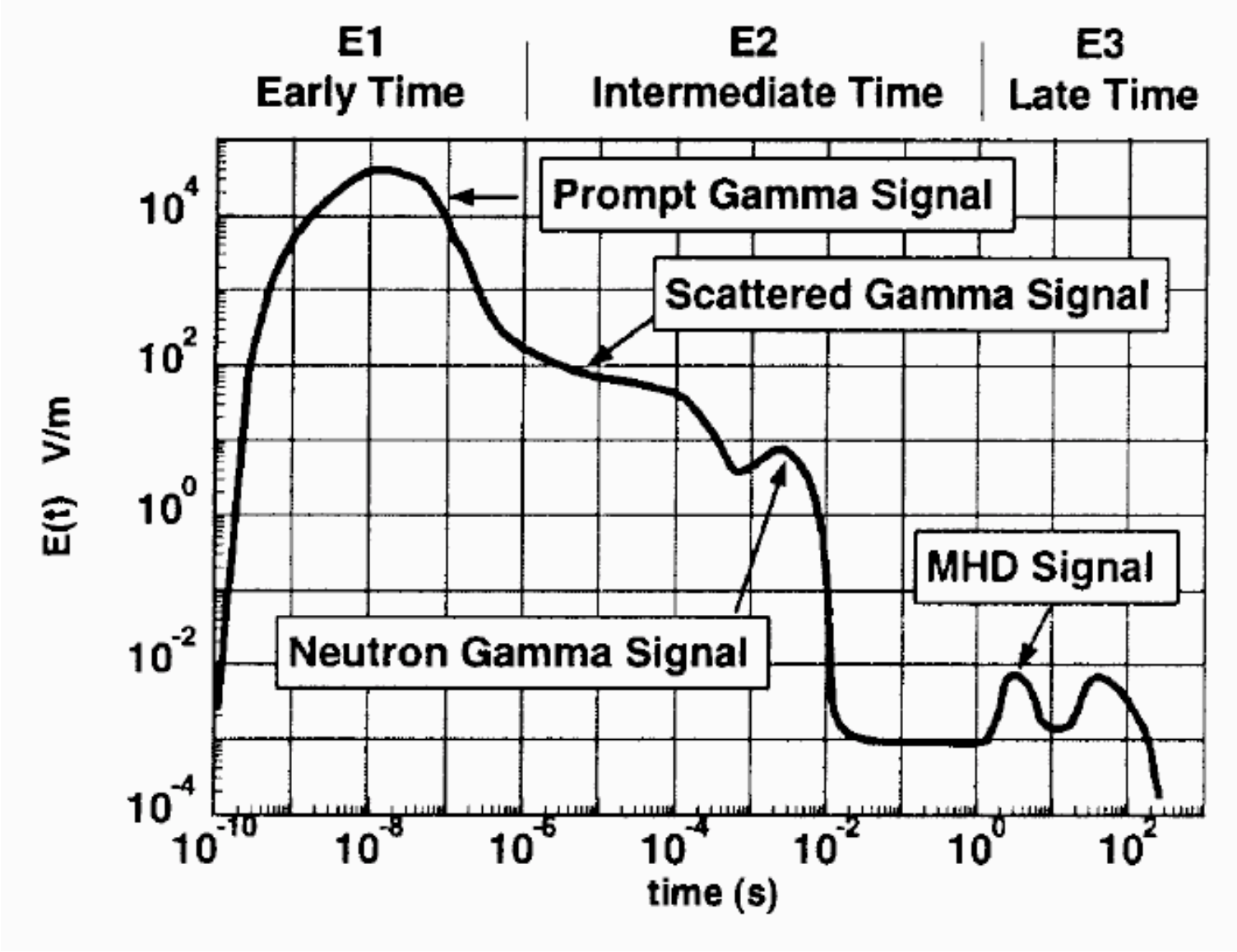
* Note: assuming detonation occurred over Kansas, a 2,201 km radius would include virtually the entire continental U.S.

Figure 2. Illustrative EMP Effects – Fast Pulse

Source: Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack (burst height unspecified, but apparently on the order of 100km given the coverage extent shown)

A 50kV and Nanosecond Rise Time Threat

- MIL-STD-2169, a classified document, apparently provides detailed information about the EMP threat wave forms. For all of us (including me!) without access to classified documents like that one, an unclassified version of the EMP threat wave form has been released, and it describes a 50kV potential which develops in literally just nanoseconds.
- This is important because:
  -- 50 kV is a very high voltage, more than enough to zap sensitive unprotected electronic devices
  -- a few nanosecond rise time is so fast that most conventional surge suppressor technologies (aimed at much slower-building pulses, such as lightning), typically wouldn't have time to react
- It is also worth noting that besides the prompt ("E1") high voltage threat, there's also a longer duration wide area magneto-hydrodynamic ("E3") component which is also important.

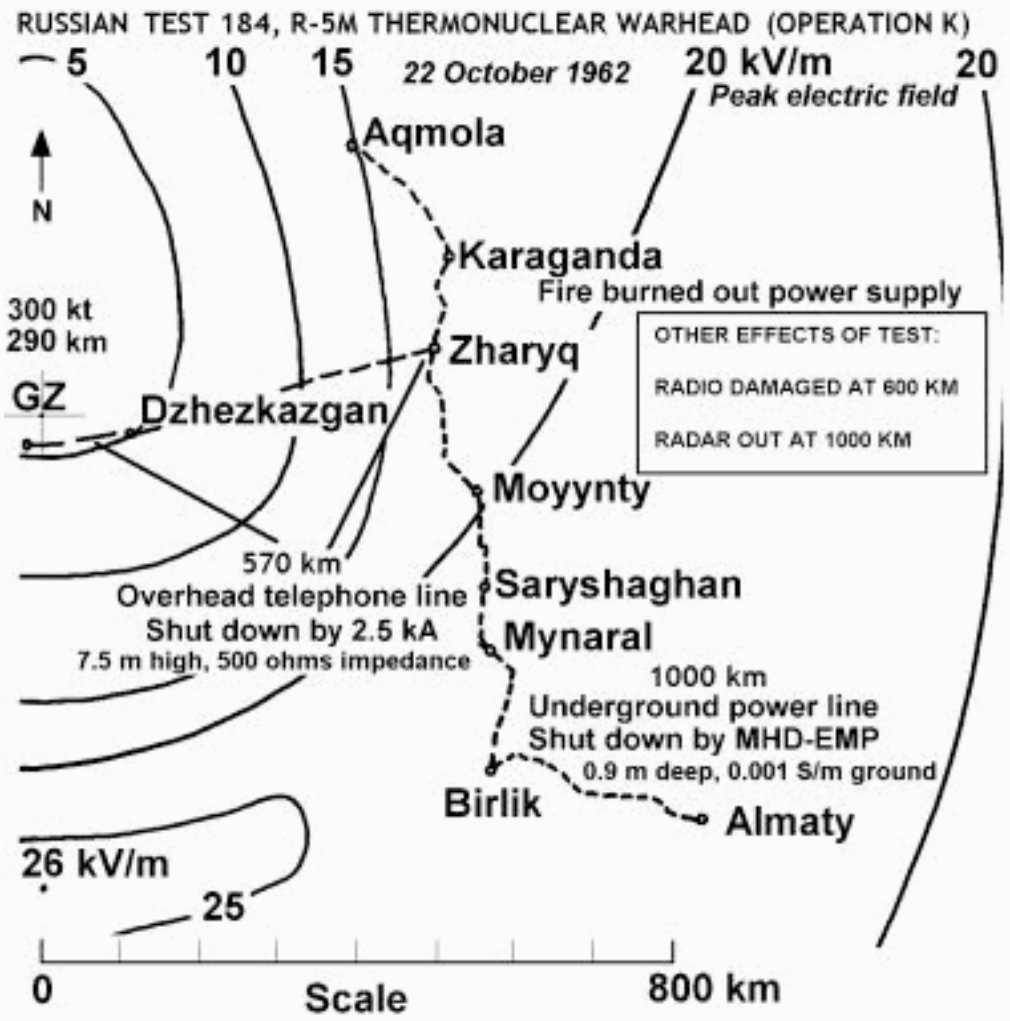


Source: EMP Environment (MIL-STD-464, "Electromagnet Environmental Effects Requirements For Systems", http://www.tscm.com/MIL-STD-464.pdf).
Note log-log axes used on this graph.

MHD-EMP ("E3" or "Heave") Signal

- "MHD-EMP is the late time (t > 0.1 second) component of EMP caused by a high-altitude nuclear burst. [...] MHD-EMP fields have low amplitudes, large spatial extent, and very low frequency. Such fields can threaten very long landlines, including telephone cables and power lines, and submarine cables."
  from "Engineering and Design - Electromagnetic Pulse (EMP) and Tempest Protection for Facilities," DA EP 1110-3-2, 31 Dec 1990; http://www.fas.org/nuke/intro/nuke/emp/toc.htm , Ch. 2, pdf pp. 5

  [See also:
  (1) "Nuclear Magnetohydrodynamic EMP, Solar Storms, and Substorms," http://arxiv.org/ftp/physics/papers/0307/0307067.pdf
  (2) "Solar Storm Threat Analysis," http://personals.galaxyinternet.net/tunga/SSTA.pdf and
  (3) "EMP radiation from nuclear space bursts in 1962" http://glasstone.blogspot.com/2006/03/emp-radiation-from-nuclear-space.html -- see also the next slide]



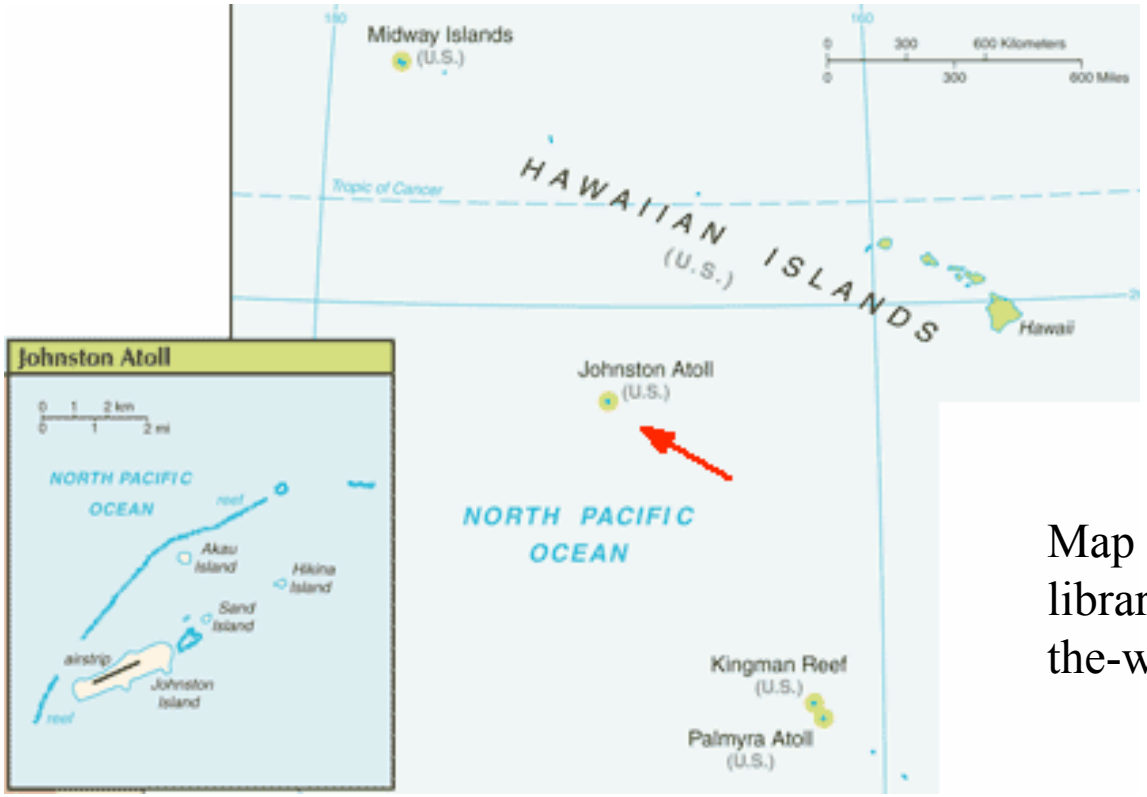
Above: USSR Test '184' on 22 October 1962, 'Operation K' (ABM System A proof tests) 300-kt burst at 290-km altitude near **Dzhezkazgan**. Prompt gamma ray-produced EMP induced a current of 2,500 amps measured by spark gaps in a 570-km stretch of overhead telephone line to Zharyq, blowing all the protective fuses. The late-time MHD-EMP was of low enough frequency to enable it to penetrate the 90 cm into the ground, overloading a shallow buried lead and steel tape-protected 1,000-km long power cable between Aqmola and **Almaty**, firing circuit breakers and setting the **Karaganda** power plant on fire.

Some Other EMP Effects We're Not Going to Consider…

- For the purposes of this talk, we're not going to consider other electromagnetic pulse-related effects, such as source region EMP and system generated EMP effects.
- Surface burst effects, such as source region EMP, are likely to be practically dominated by direct weapon effects such as thermal and shock wave damage, so we will not consider SREMP further in this talk.
- System generated EMP (SGEMP) effects require the affected system to be directly exposed to the impinging gamma and x-rays from a high altitude detonation, and thus would primarily apply to military systems and spacecraft aloft, components which are beyond the scope of this talk.

So Where Does US Empirical Data About EMP Come From?

- Virtually all US empirical information about electromagnetic pulse comes from high altitude nuclear testing done 45 years ago in remote areas of the Pacific, such as the 1962 tests done near Johnston Atoll, over 700 miles southwest of Hawaii:



Map source: https://www.cia.gov/library/publications/the-world-factbook/geos/um.html

The Starfish Prime Shot, July 8th, 1962

- The most important of those nuclear tests was the Fishbowl Event series, part of Operation DOMINIC I. Those nuclear tests were done to evaluate the potential of high altitude nuclear explosions as a possible defense against incoming ballistic missiles, and weren't focused on EMP effects *per se*. The Starfish Prime shot of that series took place at 2300 Hawaiian time, July 8th, 1962, and consisted of a 1.45 MT warhead which was carried aloft to an altitude of 400 km by a Thor missile, 32km south of Johnston.
- "At zero time at Johnston, a white flash occurred, but as soon as one could remove his goggles, no intense light was present. […] No sounds were heard at Johnston Island that could be definitely attributed to the detonation."

See "A 'Quick Look' at the Technical Results of Starfish Prime. Sanitized Version," August 1962, http://handle.dtic.mil/100.2/ADA955411

Thor Missile; Starfish Prime Skyglow

Credits: Thor missile image courtesy Boeing. Starfish Prime sky glow image from AtomicArchive.com

Weapon Effects… a Long Ways Away

- In Hawaii, over 700 miles from Johnston Island, some resorts were reportedly holding "rainbow bomb" parties the night of the Starfish Prime shot, anticipating a spectacular auroral light show.*
- What was not expected was:
  -- to have about 300 streetlights go out in Honolulu
  -- to have burglar alarms go off
  -- to have inter-island microwave communication links fail or
  -- to have telephone systems fail.
- **The government promptly clamped a lid on these unexpected weapon effects**, and in fact, high altitude nuclear weapons effects info even has its own chapter in the declassification manual.**

---

* "Nuclear Explosions in Orbit," Scientific American, June 2004.

** Department of Energy "Historical Records Declassification Guide," CG-HR-1, Chapter 8, October 16, 1995.

Some Comments to Congress in 1997

- 'The first American high-altitude nuclear weaponry experiments after the Soviet breaking of the nuclear test moratorium of '58-'61 revealed a wealth of phenomenology of completely **unprecedented - and largely completely unanticipated** - character. Most fortunately, these tests took place over Johnston Island in the mid-Pacific rather than the Nevada Test Site, or "electromagnetic pulse" would still be indelibly imprinted in the minds of the citizenry of the western U.S., as well as in the history books. **As it was, significant damage was done to both civilian and military electrical systems throughout the Hawaiian Islands, over 800 miles away from ground zero. The origin and nature of this damage was successfully obscured at the time** - aided by its mysterious character and the essentially incredible truth." Testimony of Dr. Lowell Wood, http://www.fas.org/spp/starwars/congress/1997_h/h970716w.htm

Some Aspects of Electromagnetic Pulse Effects Continue to Be Sensitive Today...

Los Alamos
NATIONAL LABORATORY

Classified colloquium to explore threat to U.S. from electromagnetic pulse attack

By Todd Hanson

December 12, 2005

The potential threat to the United States from an electromagnetic pulse (EMP) attack is the topic of a classified Director's Colloquium Wednesday by Laboratory weapons scientist Michael Bernardin.

Bernardin, of Thermonuclear Applications (X-2), will speak at 1:10 p.m., in the Administration Building Auditorium at Technical Area 3. Bernardin's talk is entitled, "Threat to the United States from Electromagnetic Pulse (EMP) Attack."

A recently completed congressional commission study assessing the nature of the high-altitude electromagnetic pulse (EMP) threat to the United States has found that EMP is one of a small number of threats that can hold our society at risk of catastrophic consequences. The commission found that EMP has the potential to damage electrical power systems, electronics and information systems upon which American society depends -- to the point where an attack could have irreversible effects on the country's ability to support its population, according to Bernardin. Furthermore, the commission concluded that an EMP attack might result in the defeat of U.S. military forces.

In his talk, Bernardin will review the nature of high-altitude EMP, the fields generated from various classes of nuclear weapons, and the effects that EMP can cause. He will then discuss the commission's findings and the assessed threat to the United States.

For the last 20 years, Bernardin has working in the Laboratory's Applied Physics (X) Division. During this time, he has focused on areas of nuclear weapon design, weapon outputs and effects, advanced weapon concepts and on enhancing scientific predictive capability for thermonuclear secondaries. In addition, he has worked for many years in modeling high-altitude electromagnetic pulse (EMP) and is a recognized national expert in the field.

Michael Bernardin *enlarge image*

In 1996, Bernardin co-founded, with Harold Rogers, the Theoretical Institute for Thermonuclear and Nuclear Studies (TITANS), a post-graduate institute at Los Alamos for teaching the physics of nuclear weapons to new staff. Currently, Bernardin is the acting group leader for X-2. In 2002, he was appointed to serve as the Laboratory's official representative to a congressionally-mandated EMP Commission. The commission met for two years and issued its Executive Report on July 22, 2004.

Bernardin's talk is limited to Q-cleared badgeholders with sigmas 1-10. The talk will be at a Secret-Restricted Data classification level and excludes foreign nationals.

Coming Back to the 1962 Tests, Those Tests Also Impacted Operational Satellites...

- The 1962 high altitude nuclear explosions pumped the Van Allen belts, creating persistent bands of radiation from the explosions. That radiation negatively affected satellite electronics, causing multiple satellites to prematurely fail:*

  -- Satellite Ariel, launched April 26, 1962; died four days after Starfish Prime due to deterioration of solar cells.
  -- Transit 4B: stopped transmitting 25 days after Starfish Prime.
  -- Research Satellite Traac, in operation 190 days, ceased transmitting data 34 days after Starfish Prime.

---

* United States High-Altitude Test Experiences: A Review Emphasizing the Impact on the Environment, LA-6405, Issued October 1976, http://www.fas.org/sgp/othergov/doe/lanl/docs1/00322994.pdf

An Aside: Satellites Remain Vulnerable to Lingering High Altitude Radiation Today

- "Perhaps the most devastating threat could come from a low-yield nuclear device, on the order of 50 kilotons, detonated a few hundred kilometers above the atmosphere. A nuclear detonation would increase ambient radiation to a level sufficient to severely damage nearby satellites and reduce the life time of satellites in low earth orbit from years to months or less. The lingering effects of radiation could make satellite operations futile for many months. Even nuclear detonations in the 10-kiloton range could have significant effects on satellites for many months […]
  To execute this mission, all that is needed is a rocket and a simple nuclear device. "
  Report of the Commission to Assess United States National Security, Space Management and Organization, Donald Rumsfeld (e.g., future SECDEF), Chairman, Jan 11, 2001
  http://www.fas.org/spp/military/commission/report.htm

IV. EMP Shielding

Our Primary Focus Today Isn't On Satellites, It's On Managing Terrestrial EMP Effects

- Are current electrical and electronic devices at risk?
- How can they be protected?
- What have empirical nuclear EMP high altitude tests since Starfish Prime shown us?

- At least one of those questions, the last question, is an easy one to address – there haven't been further atmospheric high altitude nuclear tests since Starfish Prime.

Why Haven't There Been Further High Altitude Atmospheric Nuclear Tests?

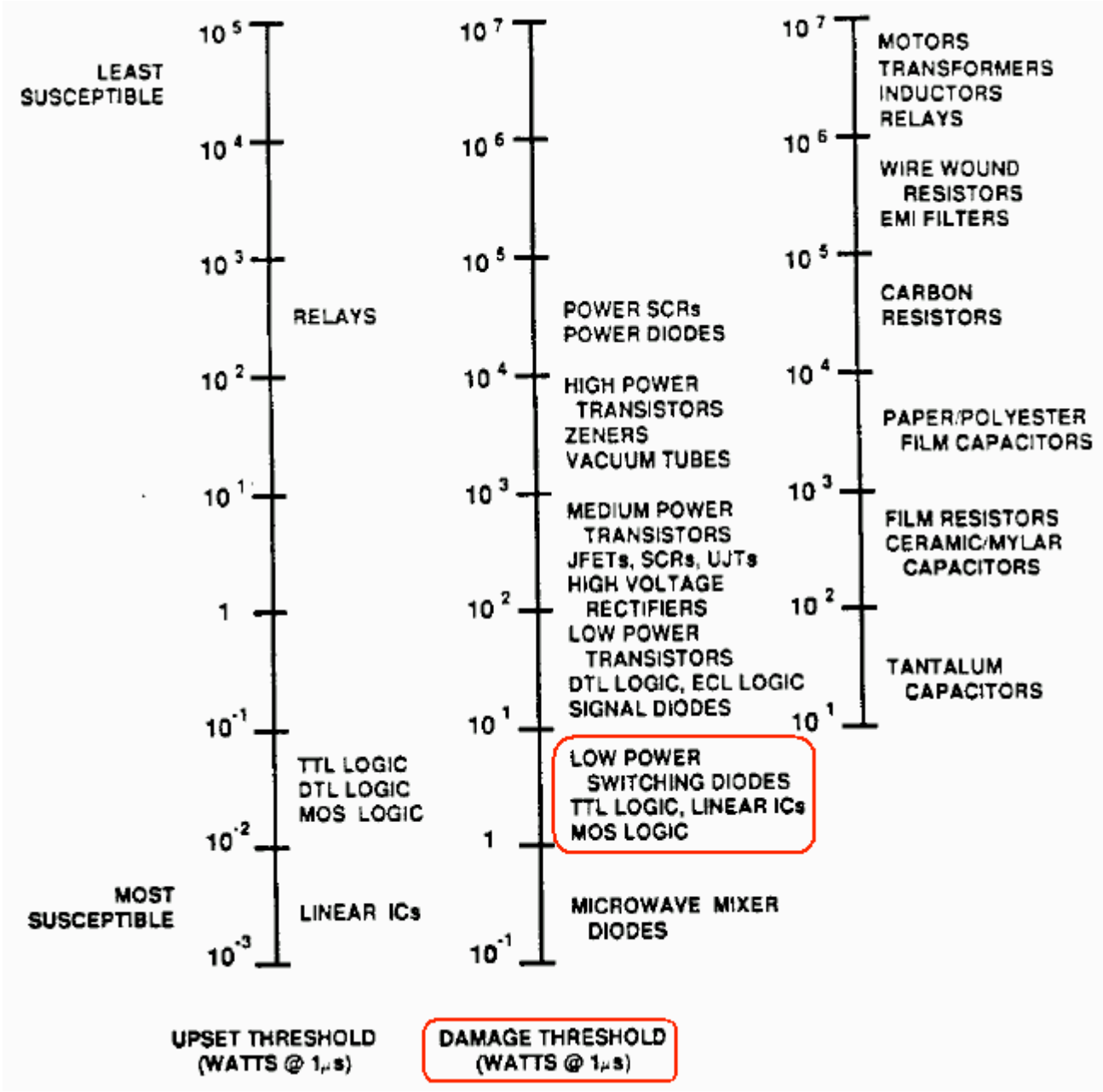
- In 1963, the Limited Test Ban Treaty* was signed, banning nuclear tests in the atmosphere, in outer space and under water. Because of the LTBT, Starfish Prime gave us the "last best" *in situ* US experimental data available.
- An interesting topic for speculation over beers some time: what inspired the United States and Russia to consumate the LTBT? Was it the result of the Cuban Missile crisis (October 14th-28th, 1962)? Growing concern over domestic environmental effects of above ground nuclear contamination? Worries about loss of additional satellites to lingering radiation effects? Or was it recognition that EMP-related effects might just be too serious to explore further?

---

* http://www.state.gov/t/ac/trt/4797.htm

Electrical and Electronic Gear in 1962, and Electrical and Electronic Gear Now

- Ironically, the nation was in better shape, at least with respect to EMP-vulnerable electrical and electronic devices, in 1962 than it is now. Why? Well, in 1962 vacuum tubes were still common, and integrated circuits were virtually non existent. Now, that's reversed, and VLSI integrated circuits are very EMP sensitive.
- For a discussion of the types of electrical components which are most at risk of damage from electrical effects, see Department of the Air Force "Engineering Technical Letter (ETL) 91-2: High Altitude Electromagnetic Pulse (HEMP) Hardening in Facilities" available at http://www.wbdg.org/ccb/AF/AFETL/etl_91_2.pdf 4 March 1991.
- An excerpt from that report is shown on the following slide (boxes added by me for emphasis).


LEAST SUSCEPTIBLE
MOST SUSCEPTIBLE
10^5
10^4
10^3
10^2
10^1
1
10^{-1}
10^{-2}
10^{-3}
RELAYS
TTL LOGIC
DTL LOGIC
MOS LOGIC
LINEAR ICs
10^7
10^6
10^5
10^4
10^3
10^2
10^1
1
10^{-1}
POWER SCRs
POWER DIODES
HIGH POWER TRANSISTORS
ZENERS
VACUUM TUBES
MEDIUM POWER TRANSISTORS
JFETs, SCRs, UJTs
HIGH VOLTAGE RECTIFIERS
LOW POWER TRANSISTORS
DTL LOGIC, ECL LOGIC
SIGNAL DIODES
LOW POWER SWITCHING DIODES
TTL LOGIC, LINEAR ICs
MOS LOGIC
MICROWAVE MIXER DIODES
10^7
10^6
10^5
10^4
10^3
10^2
10^1
MOTORS
TRANSFORMERS
INDUCTORS
RELAYS
WIRE WOUND RESISTORS
EMI FILTERS
CARBON RESISTORS
PAPER/POLYESTER FILM CAPACITORS
FILM RESISTORS
CERAMIC/MYLAR CAPACITORS
TANTALUM CAPACITORS
UPSET THRESHOLD (WATTS @ 1μs)
DAMAGE THRESHOLD (WATTS @ 1μs)

What's The Difference Between "Upset" and "Damage?"

- You may have noticed two different scales on the preceding chart – one for "upset" and one for "damage," and you may wonder, "what's the difference?" I quote from EP 1110-3-2, available at: http://www.fas.org/nuke/intro/nuke/emp/c-2body.pdf at pdf pp. 17:

  > "Upset is a nonpermanent change in system operation that is self-correcting or reversible by automatic or manual means. Damage is an unacceptable permanent change in one or more system parts."

- In the civilian world our focus is obviously primarily on damage, but in a military setting even having systems simply be temporarily upset can be catastrophic if that upset occurs during a critical time, such as while a plane is engaged in crucial flight operations.

Integrated Circuit Density Has Continued to Increase Since That 1991 Report...

- "[...] due to size and power reductions, modern electronics are inherently more vulnerable to some of the effects produced by a nuclear detonation. And each new generation, smaller and needing less power, exacerbates these vulnerabilities. Furthermore, as we make greater use of more affordable commercial parts and components, we potentially introduce new vulnerabilities into our military systems. Additionally, the military's increasing reliance on commercial space-based systems makes it more vulnerable to the nuclear weapon effects being discussed."

  Comments of Dr. George W. Ullrich, Deputy Director, Defense Special Weapons Agency
  http://www.fas.org/spp/starwars/congress/1997_h/h970716u.htm

Just In Case There's Still Any Doubt

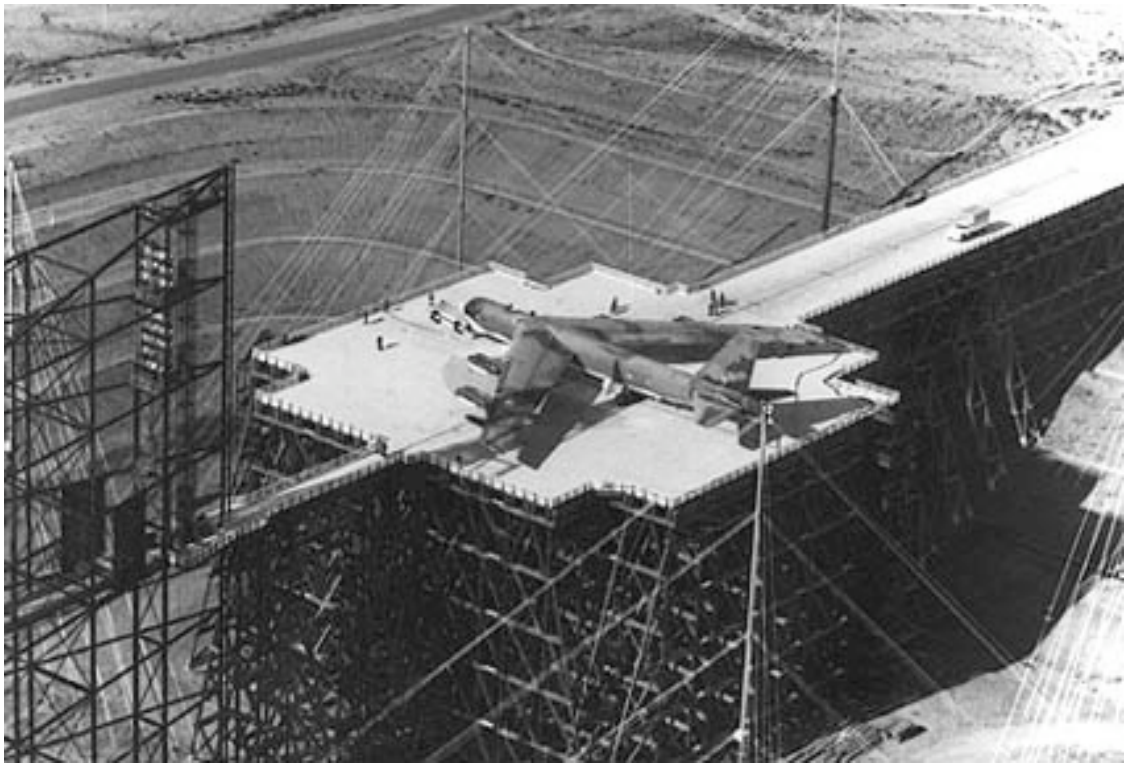
- "It is a reasonable projection that most, if not all, modern computer systems exposed to referenced EMP field levels—which are 50 kilovolts per meter, not just 10—but the very high levels you might see in most of the United States—most modern computer systems ranging from laptops to mainframes would wilt. By wilting, they would at least cease to function. In many cases, they would be burned out. So it would require very major maintenance before they could be restored to operation.

  "Not just computers in aircraft but computers everywhere, other than in this type of very high integrity metallic enclosures that Dr. Ullrich sketched in his opening statement. Computers in any other enclosure than that type would be compromised, if not destroyed outright."

Testimony of Dr. Lowell Wood, http://commdocs.house.gov/committees/security/has197010.000/has197010_1.HTM

But If We Haven't Done High Altitude Atmospheric Testing Since 1962...

- ... how do we know what's vulnerable and what's not, or how to effectively protect critical systems? Answer: EMP simulators, such as the Trestle facility at Kirtland AFB in NM, the largest wood-and-glue laminated structure in the world.



Other EMP Simulation Facilities

- A list of electromagnetic pulse simulation facilities, at least as of 1994, can be found at pdf pp. 8 of http://stinet.dtic.mil/cgi-bin/GetTRDoc?AD=ADA278230&Location=U2&doc=GetTRDoc.pdf , "Test Operations Procedures (TOP), 1-2-612 Nuclear Environment Survivability," 15 April 1994. See also http://commdocs.house.gov/committees/security/has197010.000/has197010_1T.HTM As discussed in that Congressional hearing, it is believed than many EMP simulators have been mothballed or decommissioned, thereby limiting opportunities for empirical testing of equipment under simulated EMP signals (for example, the Trestle facility shown on the preceding page is believed to no longer be operational).

- So have critical core network routers, switches and optronics been hardened, and proof tested for EMP hardness?

There Is No Indication That Core Routers, Switches and Optronics Are EMP Hardened

- After reviewing a number of major vendors web sites for information about the EMP hardening status of routers and switches, and after visiting with a number of vendor staff members, I was unable to find any public indication that any major vendor's routers and switches are EMP hardened by default. (If you are a manufacturer of routing or switching gear, or optronics, and your gear *is* EMP hardened and that information can be publicly shared, please let me know.)

Thus, unless a vendor explicitly tells you otherwise, assume that ALL critical core routers, switches, optronics and other key network equipment will need supplemental shielding for EMP hardening purposes.

Fiber Optic Cable Maybe Immune to EMP, But OEO Equipment Probably Isn't…

- When thinking about critical network equipment, PLEASE don't forget about electronics deployed in support of optical networks.

- While fiber is largely EMP resistant (modulo a reference or two I've seen associated with potential "fiber fogging"), the optical-electrical-optical ("OEO") retime/reshape/reamplify ("3R") optronics probably aren't EMP resistant (again, unless a vendor tells you explicitly to the contrary).

- **Just as you should provide supplementary shielding for critical routers and switches, you should ALSO plan to provide supplemental external EMP shielding for any optronic devices you may use.**

Harden Key Campus Network Support Infrastructure, Too

- Network monitoring and management stations in NOC
- Authoritative and Recursive Name servers
- DHCP servers
- LDAP or Radius servers
- Log servers
- Firewalls
- Intrusion detection systems

Harden Enterprise Mission Critical Systems

- School ERP system (student information system, HR system, A/R, A/P, inventory, grants and contracts, etc.)
- Teaching and learning system (Blackboard, etc.)Campus web presence
- Email infrastructure
- POTS and/or VOIP phone systems
- Library system resources
- Research computing clusters
- Mass storage resources

Ensure Critical Ancillary Services Are Also EMP Resistant and Will Be Available

- Campus power
- Cooling
- Network connectivity (if you don't provide your own connectivity, are all your network service providers EMP hardened?)
- Access control systems (can you use a manual key to override a fried proximity card reader door lock?)

What's Involved in Hardening or Providing External EMP Shielding For Critical Gear?

- The goal is to isolate key equipment from potentially dangerous RF energy by providing a continuous metal shield (such as 10 gauge/3.416 mm or better steel) around vulnerable equipment.
- A very conservative hardening target is 100dB worth of attenuation from 1kHz to 10GHz, with no waveguide beyond cutoff (WBC) penetration (discussed later) larger than 1.0 cm; see, for example "Guide Specifications for HEMP/TEMPEST Shield Doors, Electrical Filter/ESA Assemblies, and Other Shield Penetrations," Rev 1, Jun 1988, at pdf page 120, available online at http://www.custompowersystem.com/images/hemp.pdf
- A less stringent protection EMP hardening target would be 50db from 14kHz to 1GHz, with no WBC penetration larger than 10.0cm

What's "TEMPEST"?

- TEMPEST is "a short name referring to investigations and studies of compromising emanations" according to NCSC-3 (see http://cryptome.org/ncsc-3.htm). TEMPEST and EMP often are discussed together because shielding protecting systems against compromising emanations also provides protection against EMP and vice versa, although required frequency coverage and level of attenuation vary. An example of a publication which considers both together is "Engineering and Design - Electromagnetic Pulse (EMP) and TEMPEST Protection for Facilities," 31 December 1990, Army Pamphlet EP 1110-3-2, see http://www.fas.org/nuke/intro/nuke/emp/toc.htm (467 pages)
- Also see (1) http://www.eskimo.com/~joelm/tempestsource.html (2) UCAM-CL-TR-577, Dec 2003, by Markus G. Kuhn, at http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-577.pdf, and (3) an NSA maintained list of TEMPEST Certified products at www.nsa.gov/ia/industry/tempest.cfm?MenuID=10.2.1.3

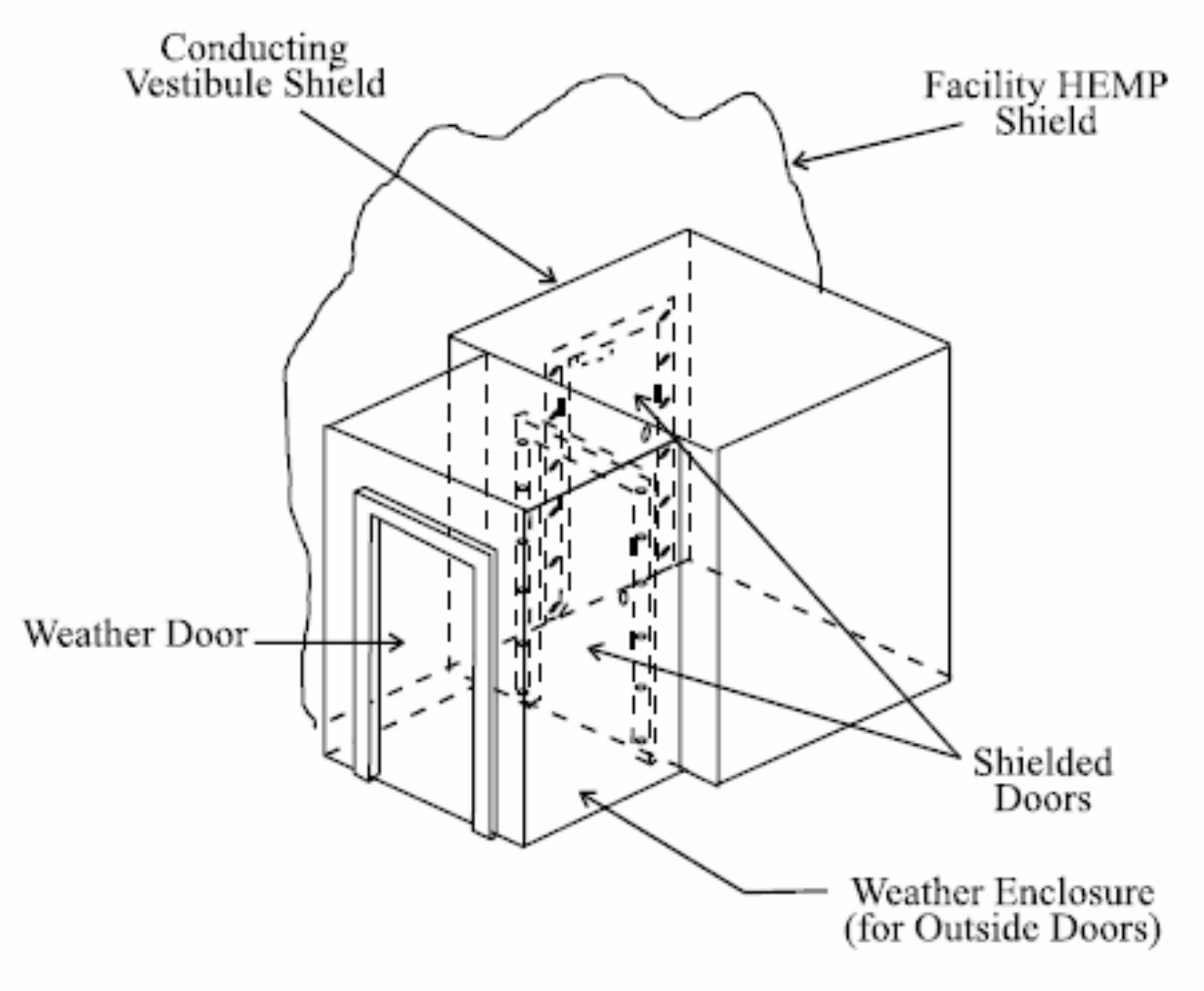
But Coming Back to What's Involved in Providing EMP Shielding For Systems...

- Much of the effort (and cost!) involved in constructing EMP shielded areas is associated with the careful design, essentially perfect craftsmanship, and extensive conformance testing that's required to verify required protection.
- EMP shielded areas also require extra space, which may be an issue for some space-constrained facilities. Ideally there should be at least 3 feet of access space around the shielded area for ongoing EMP testing and for maintenance access to penetrations, plus additional physical control space (PCS) as may be needed to meet other requirement (e.g., in high threat areas you may need to provide 3 *meters* of PCS due to emission security concerns; see section 8.51.5.2 of AFSM 7011, http://jya.com/afssm-7011.htm)
- If you're out of space before you even start, now might be a good time to think about a secondary data center, connected by fiber...

Doors and EMP Enclosures

- Doors are one of the most difficult areas when it comes to providing unimpaired EMP shielding.
- Doors for personnel and equipment access will often be specially constructed to use a double knife edge seal with beryllium copper fingerstock contacts.
- Ideally doors will be configured in pairs, arranged at right angles, separated by a vestibule, and protected from being opened simultaneously by an interlock mechanism (see the illustration on the next slide)

Sample Double Door EMP Vestibule Style Entrance



http://www.wbdg.org/ccb/FEDMIL/std188_125_1.pdf at pdf pp. 31

Sample Modular Steel EMP Enclosure

Photo courtesy ETS-Lindgren.

Sample Welded Steel EMP Enclosure

Photo courtesy ETS-Lindgren.

You May Also Just Want to Shield Gear From EMP On A Rack-by-Rack Basis

- Looking at those previous EMP shielded areas, one might get the impression that they represent the smallest areas which can be EMP shielded. That would be incorrect. You can also purchase EMP hardened enclosures built around 19" telco rack form factors.
- Those enclosures can even be embedded within a GSA approved security container (aka a safe) if physical security of equipment is also a concern (hey, you lock your guns up in a gun safe when you're not using them, right? so why not protect a couple hundred hundred thousand dollar router at least equally well?)

Sample EMP Shielded 19" Rack Enclosure

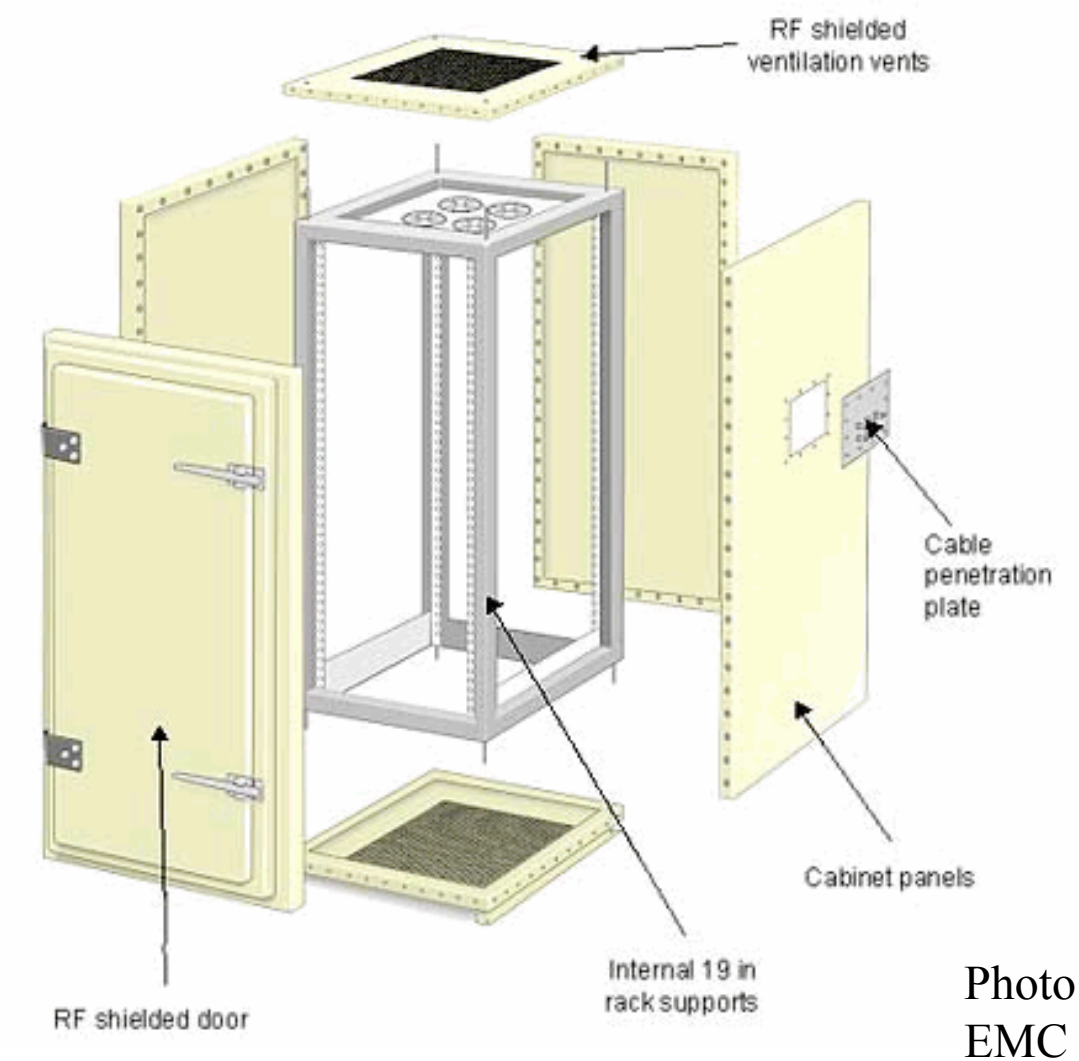


Photo courtesy of European EMC Products Limited

Sample TEMPEST (and GSA Class 5 Security Container) Enclosure

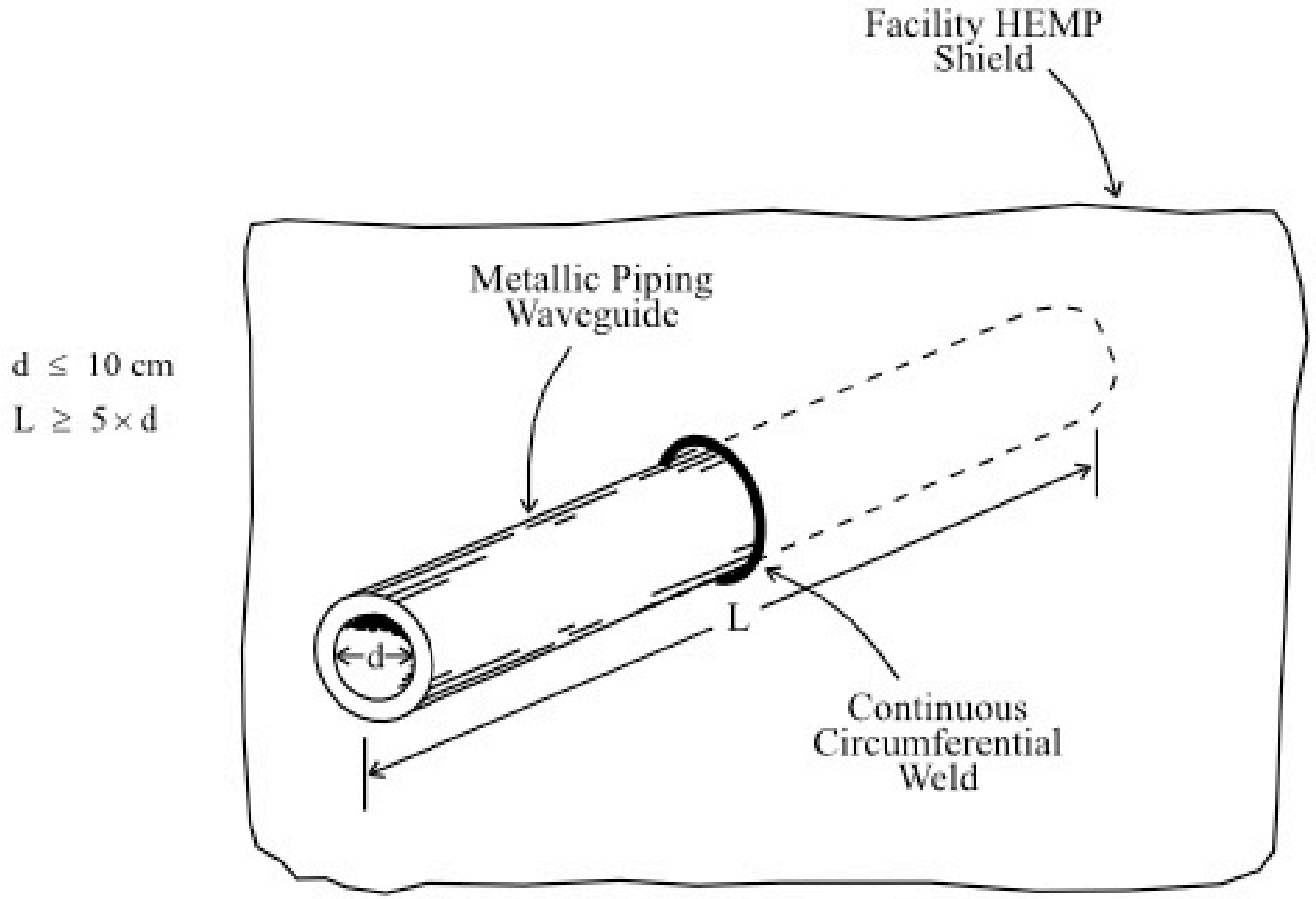
Photo courtesy ETS-Lindgren.

Waveguide Beyond Cutoff Penetrations

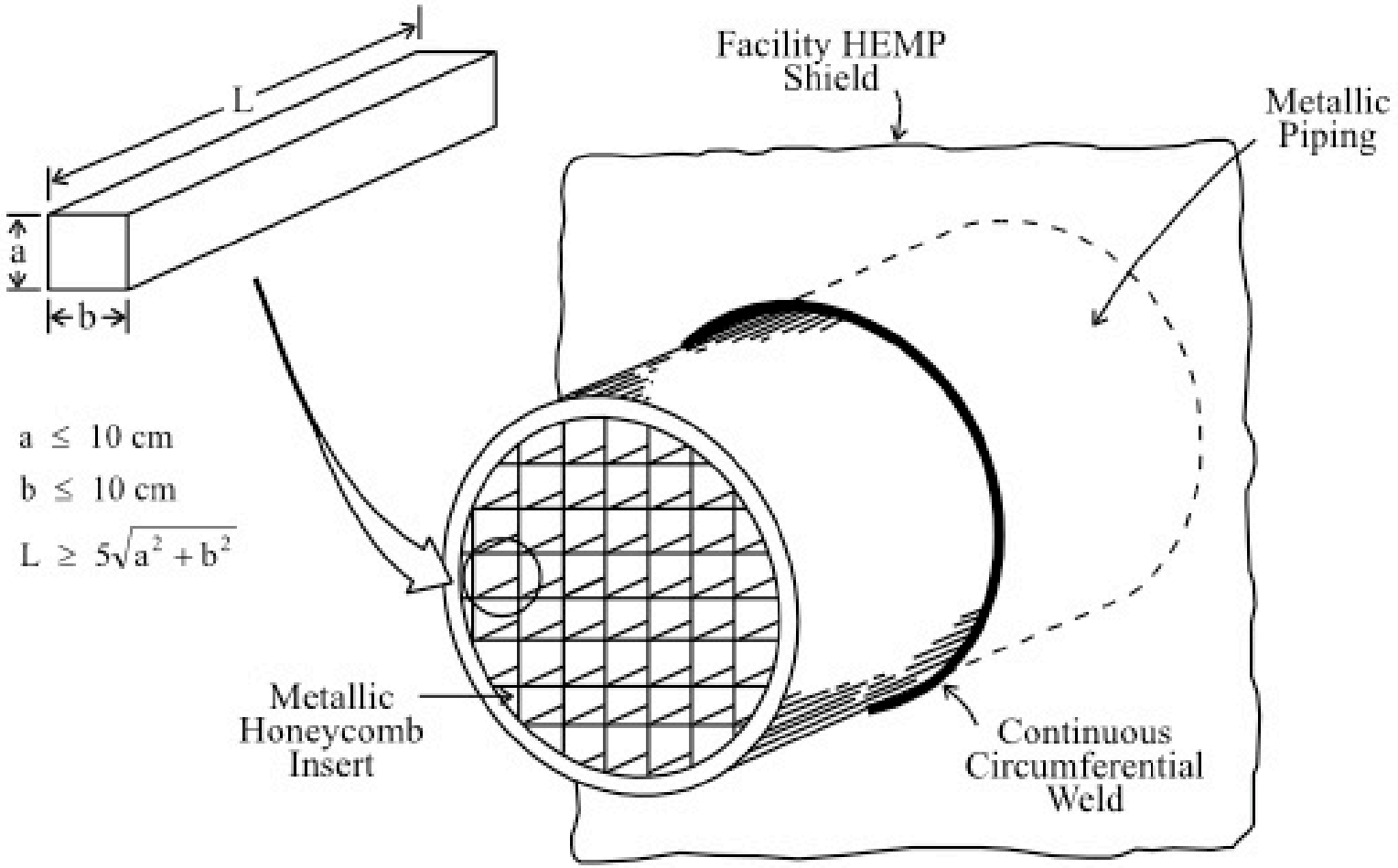
- Shielded enclosures can't be sealed as tightly as a can of soup. :-) Among other things, there needs to be some way to safely pass fiber optic data cables through the shielding of the enclosure, and some way to provide air for personnel as well as ventilation to keep gear from overheating.
- The way this normally gets handled is via "waveguide beyond cutoff" (WBC) penetrations.
- The maximum diameter of the allowed WBC aperture varies with the target cutoff frequency, but a diameter no larger than 10cm is specified by MIL-STD-188-125-1 for protection through 1GHz, with a length that's at least 5 times that diameter. The waveguide must be made of metal, continuously circumferentially welded to the facility EMP shield, and there must be no conductors present within the waveguide. See the illustrations on the following slides from MIL-STD-188-125-1

Waveguide Beyond Cutoff (cont.)

MIL-STD-188-125-1



Honeycomb WBC for Larger Penetrations



EMP Shielded Facilities and Electrical Feeds

- Power for equipment located within the EMP shielded enclosure must be provided via specially filtered lines (e.g., normal surge suppressors don't react fast enough to protect critical equipment against EMP). For some examples of EMP electrically protective filters, see:
  -- http://www.ets-lindgren.com/pdf/N2556.pdf
  -- http://www.ramayes.com/EMI_RFI_Filters.htm
  -- http://www.custompowersystem.com/Efilters/products4.htm

- All EMP shielded enclosures must also be carefully electrically bonded and grounded.

Spares and Recovery

- Review stockpiles of spare parts, including fuses, replacement power supplies, spare fans and hard drives, etc. – do so NOW while you can easily order additional spares which might prove useful. To many products to easily stock spares? Maybe it is time to think about standardizing and consolidating on a smaller number of unique devices!
- When it comes to equipment which has been damaged beyond what you can repair yourself, recognize that the primary source of replacement gear may be out-of-region or from overseas, and that in some cases replacement gear may be effectively unobtainable in any relevant time frame. For that reason, consider stockpiling replacement gear (or even just recently replaced equipment!) in an EMP-secure warehouse for use as replacement gear in the event current shielded gear somehow gets damaged by an EMP strike.

The "Single-Event Fallacy"

- "Avoid the single-event fallacy. In assessments of potential tactical situations, don't assume that EMP will occur once and then be over. The contrary may be the case. An aggressor may initiate a precursor attack with high altitude EMP to initially damage unprotected equipment, and then follow-up with additional high altitude or surface-burst explosions to exploit the tactical situation." (see FM 3-3-1, http://www.globalsecurity.org/wmd/library/policy/army/fm/3-3-1_2/Appc.htm)

- Thus, if you try to "hedge your bets" by not hardening systems in place, but simply caching replacement gear which you can drag out and installed if needed, recognize that your replacement gear might very well end up getting killed by a follow on attack just as your original gear was. Hardening is the only real answer...

V. But Is There Really Even A Threat?

EMP Shielding Isn't Cheap to Build Out

- I'll freely concede that hardening critical equipment in your facility with EMP shielding isn't cheap, either to install or to maintain. You don't want to embark on an expensive program of EMP hardening your facilities if you aren't pretty **dang sure** that there's a real threat out there...

- I encourage you to make up your own mind – this might all be nothing to worry, and you can just ignore this whole talk.

- On the other hand, here are some additional bits of data to chew on while you sit there happily un-EMP-shielded.

Components of a Credible EMP Threat

- For there to be a credible EMP threat, you need five things:

  1) a means to get to the required altitude, such as a missile
  2) a suitable target,
  3) a motive for conducting an EMP attack,
  4) the absence of a deterrent, and
  5) a nuclear weapon for the missile to deliver.

1) Missiles

- The type of missile required to get a nuclear least 40 km above the earth need not be particularly advanced. I quote:

  "The Scud rockets used by the Iraqis [...] flew to altitudes of 150 kilometers, which is imminently satisfactory for the type of regional EMP laydowns I have been referring to. [...] Scud-type rockets exist in copy to the extent of over 15,000 Scud class rockets owned by over 30 nations in the world at the present time. So getting to the threshold of space and carrying a nuclear explosive there is something that, unfortunately, is a regrettably potentially widespread – maybe actually widespread capability."

  Statement of Dr. Lowell Wood,
  http://www.fas.org/spp/starwars/congress/1997_h/h970716w.htm

What Does the Congressional Research Service Think?

"**About three dozen countries have been publicly identified as having ballistic missiles**, and half of those countries are in Asia and the Middle East. About 30 of these countries have, or are developing, ballistic missiles that can deliver a 500- kilogram warhead 300 kilometers or further. Of the non-European countries, fourteen have produced ballistic missiles (Argentina, China, Egypt, India, Iran, Iraq, Israel, North Korea, Pakistan, South Korea, Syria, Taiwan, Ukraine, and South Africa which no longer produces missiles). In addition to these regional powers, which are often discussed as missile proliferators, several Western and Eastern European countries and republics of the former Soviet Union have missiles." [emphasis added]

"Missile Survey: Ballistic and Cruise Missiles of Foreign Countries," Congressional Research Service Report RL30427, Updated March 5, 2004, pdf pages 7-8.

One Scenario Which Has Been Mentioned

- Quoting Peter V. Pye from March 2005:

"Iranian flight-tests of their Shahab-3 medium-range missile, that can reach Israel and U.S. forces in the Persian Gulf, have in recent years involved several explosions at high altitude, reportedly triggered by a self-destruct mechanism on the missile. The Western press has described these flight-tests as failures, because the missiles did not complete their ballistic trajectories. Iran has officially described all of these same tests as successful. The flight-tests would be successful, if Iran were practicing the execution of an EMP attack.

"Iran, as noted earlier, has also successfully tested firing a missile from a vessel in the Caspian Sea. A nuclear missile concealed in the hold of a freighter would give Iran, or terrorists, the capability to perform an EMP attack against the United States homeland, without developing an ICBM, and with some prospect of remaining anonymous. Iran's Shahab-3 medium-range missile, mentioned earlier, is a mobile missile, and small enough to be transported in the hold of a freighter."

http://kyl.senate.gov/legis_center/subdocs/030805_pry.pdf

SCUD-Class Missiles Even Appear to Have Been Available on the Open Market...

- **U.S. seizes Scud missile imported by weapons collector**

  http://www.cnn.com/US/9809/25/missile.seizure/ (Sept. 25, 1998)

  LOS ANGELES (CNN) -- U.S. Custom officials are investigating how an operational Russian-designed Scud B missile was imported into California. […] The missile has been identified as a Scud B SS-1C that was manufactured in Czechoslovakia in 1985. Officials are trying to determine whether the wealthy California weapons collector who they say imported the missile from London falsified customs documents and claimed the missile was "demilitarized." […] the missile was fully operational because it has a guidance system and an engine. It did not, however, come with a warhead or fuel. [continues]

Or Could Even A High Altitude Balloon Reach EMP-Relevant Altitudes?

- http://www.csbf.nasa.gov/balloons.html says

  "Standard NASA scientific balloons are constructed of polyethylene film; the same type material used for plastic bags. This material is only 0.002 centimeters (0.0008 inches) thick, about the same as an ordinary sandwich wrap. […]

  "These very large balloons can carry a payload weighing as much as 3,600 kilograms (8,000 pounds), about the weight of three small cars. **They can fly up to 42 kilometers (26 miles) high** and stay there for up to two weeks."

- So yes, a specialized high altitude scientific balloon could loft a warhead to EMP-effect relevant altitudes.

2) A Suitable Target

- Because of the nature of the EMP effect, electromagnetic pulse effects are not suitable for use against all conceivable targets.
- For example, because a minimum height of burst is needed to achieve EMP-related effects, and because even a 40 km height of burst will affect sites within a 700 km radius, an EMP weapon cannot be used if an target is too close to unhardened friendly assets. [One is reminded of the (unrelated) exhortation to "keep your friends close, and your enemies closer!"]
- EMP effects are not precise/surgical. Atmospheric effects and weapon related effects mean that EMP effects may vary from projections, or from shot to shot, and limited empirical test data means that EMP weapons cannot be treated like a precision guided munition. They are an area weapon, not a point weapon.
- EMP weapons are also obviously not appropriate if a target is pre-industrialized, or widely hardened against EMP.

Coastal vs Mid Continental Use

- Are there considerations which might lead an attacker to conduct a high altitude nuclear burst over one coast or the other rather than attempting to achieve full continental coverage with a high altitude high yield burst over the Great Plains?
- Maybe yes. Consider the following potential factors:
  -- The attacker has a lift vehicle with limited altitude potential, or the attacker has a comparatively low yield weapon. Given those limitations, a mid-continent burst strategy wouldn't be assured of reaching high value areas on the coasts
  -- The attacker might want to launch from offshore, in international waters; coastal targeting would also reduce flight time (and thus exposure to potential anti-missile defenses)
  -- An attacker might want to impede military operations from one coast while being indifferent to those on the other coast
  -- If only half the country has been hit, the attacker can still use threats of attacks against the other half as a potential deterrent

Example of A Possible Coastal Use Scenario

- "Not a movie made for TV" (October 3rd, 2007) http://washingtontimes.com/apps/pbcs.dll/article?AID=/20071003/COMMENTARY/110030040/1012&template=printart

"James G. Zumwalt - An innocent-looking freighter sails 200 miles off the East Coast of the United States. In international waters, it appears to be no threat. However, its true intentions soon become evident. During the ship's transit over thousands of miles from a port in a country unfriendly to the United States, a SCUD missile remained concealed but is now being prepared for launch from the freighter's deck.

"The warhead of the soon-to-be fired SCUD — a relatively inexpensive missile abundant around the world — is not designed to detonate on American soil or to inflict massive civilian casualties via a chemical, biological or nuclear weapon. This warhead's targeted impact is purely economic, for it is armed with an EMP (Electromagnetic Pulse) payload — tailor-made to inflict as much such damage as possible. And, as a recent study concludes, **detonation over the Baltimore-Washington-Richmond corridor could result in economic output losses (exclusive of infrastructure replacement costs) exceeding $770 billion** or 7 percent of the nation's annual gross domestic product." [articles continues]

3) Motive For Conducting An EMP Attack

- Potential motives for conducting an EMP attack are as numerous as our potential enemies, including ideological/political/religious reasons, economic reasons, or military reasons.
- One could even imagine environmental motives -- perhaps we might face an attacker who thinks the US is consuming more than its share of world resources, or is irreversibly damaging the environment, etc. An EMP strike against the United States might be viewed by such a person as something which would cause a reversion to a utopian and somehow economically gentler pre-industrialized era (although it is unclear how that goal would be realized if the rest of the world remained industrialized). [In that regard, it was rather eerie to hear Osama Bin Laden talking about things like "global warming resulting to a large degree from the emissions of the factories the major corporations," see http://www.cnn.com/2007/US/09/07/binladen.tape/index.html]

EMP Attacks Are A Type of Strategic "Cyber" Warfare

- Occasionally people will speculate on the topic of cyber warfare, usually congering up attacks involving distributed denial of service attacks, worms and other sorts of malware, targeted computer intrusions, etc. While all those sorts of cyber attacks are/might be part of the cyber warriors arsenal, they're all fundamentally conventional/tactical attacks of limited scope and scale, and all are subject to mitigation (if only by selective isolation of targeted systems from parts of the Internet which are attacking them).
- What would be the equivalent of a strategic nuclear attack in the context of cyber war? I assert that when it comes to a strategic attack in a cyberwar context, the ONLY true strategic attack that I can think of would be an EMP-based attack, and that's the sort of attack which cannot be easily mitigated by things such as partitioning systems under attack from the Internet.

4) Absence of A Deterrent

- Currently traditional nuclear attacks are deterred by:
  -- pragmatic recognition that a nuclear attack will be met by a withering response in kind, and
  -- world condemnation which would accompany any attack which resulted in widespread direct loss of life.
- Note that attacks employing EMP-related effects would perturb that equation:
  -- They could potentially be conducted in a way which would make attribution, and thus retribution in kind, very difficult
  -- EMP-based attacks may be launched by entities who are largely or completely immune to EMP attacks in return (either because of collateral damage considerations, or their society's pre-industrialized status)
  -- An EMP laydown would not directly result in widespread loss of life (although deaths may be widespread as an indirect effect)

5) Availability of A Nuclear Weapon

- I won't spend time speculating on terrorist access to nuclear weapons; let's just focus on the states known to have nuclear weapons available. There are nine of those: the U.S., Russia, the U.K., France, China, Israel, India, Pakistan, and North Korea (South Africa previously had the bomb, but has disarmed).

  At a minimum, therefore, we are safe in saying that there are nine countries which have weapons would could be used for the purpose of conducting at least a rudimentary EMP laydown.

- Some of those countries are even known to have devoted special attention to producing or maintaining weapons which have been tailored to produce elevated levels of electromagnetic pulse....

Some Nuclear Weapons Have Been Intentionally Designed to Have Enhanced EMP Effects

- For example, we know from Congressional testimony that the United States has developed nuclear weapons which have been intentionally designed to produce enhanced EMP effects:

  "In the late '70s and early '80s, I worked on "Third Generation" nuclear weaponry, a major component of which was nuclear explosive-driven generators of electromagnetic pulses of potentially greatly increased efficiency and military effectiveness; spinoffs involving non-nuclear means of generating potent EMP also engaged my attention."

  Statement of Dr. Lowell Wood,
  http://www.fas.org/spp/starwars/congress/1997_h/h970716w.htm

The Soviets and "Super-EMP" Weapons

- 'In the 1990s, the [Russian] General Staff was aware of U.S. research into super-EMP nuclear weapons, which would generate a particularly powerful electromagnetic pulse capable of destroying even protected electronic systems. "From the early 1980s, U.S. military scientists ... aimed at creating ... a super-EMP [weapon] with intensified electromagnetic radiation output," General Belous accurately observed. "They figure to use it to increase the intensity of the field at the Earth's surface to several hundred kilovolts per meter." [*War Scare: Russia and America on the Nuclear Brink,* by Peter V. Pry]
- Reportedly the Soviets were content with a simpler strategy: they simply retained very large (25MT) thermonuclear warheads in their stockpile for EMP-related use instead. A somewhat crude and inelegant strategy, but one which would certainly do the job.

"So Does That Mean You'd Need A Thermonuclear Weapon To Get EMP?"

- No. Sometimes, when folks notice that Starfish Prime was 1.45MT, or hear that Soviets retained large 25MT warheads for EMP-related purposes, or learn that the US devoted significant effort to tailoring EMP-enhanced weapons, they speculate that lesser nuclear weapons (such as non-thermonuclear fission weapons) might not be enough to produce EMP. Clearly, if that were to be the case, that would dramatically increase the threshold which would need to be surmounted in order to inflict an EMP attack. Testimony of weapons scientists, however, confirms that even modest fission weapons would be sufficient to produce significant EMP effects, and those modest yields might be all that's required to take advantage of the altitudes available from developing world launch vehicles.

Didn't Some Sort of "EMP Bomb" Already Get Used In Iraq or Kosovo?

- You may be thinking of the so-called "Blackout Bomb" or "Soft Bomb" which shorted out power station transformers with conductive carbon fiber or graphite filaments – see the discussion and illustrations at http://www.fas.org/man/dod-101/sys/dumb/blu-114.htm

- There's also an interesting discussion of high power microwave devices in the Congressional Research Service's "High Altitude Electromagnetic Pulse (HEMP) and High Power Microwave (HPM) Devices: Threat Assessments," http://www.fas.org/man/crs/RL32544.pdf

Oh Yes: If You Did Want to Worry About Terrorist Access to Nuclear Material

- Check out GAO 02-426, "NUCLEAR NONPROLIFERATION: U.S. Efforts to Help Other Countries Combat Nuclear Smuggling Need Strengthened Coordination and Planning," http://stinet.dtic.mil/cgi-bin/GetTRDoc?AD=ADA403144&Location=U2&doc=GetTRDoc.pdf discussing 181 confirmed cases of smuggling nuclear materials between 1993 and 2002.

- I'd also recommend PBS' "Loose Nukes: Investigating the Threat of Nuclear Smuggling," see http://www.pbs.org/wgbh/pages/frontline/shows/nukes/

  Fair warning: that site correctly includes a quotation of a Russian proverb: "The less you know, the better you sleep."

In Summary, I Believe All Requirements Which Need to Be Satisfied for An EMP Attack to Be Plausible Have Been Met

- I believe, based on the information currently available, that all the requirements for plausible use of EMP weapons against the United States, either now or at some time in the future, have been met.

- I therefore repeat my earlier recommendation: **harden critical networks, optronics, and enterprise essential systems now.**

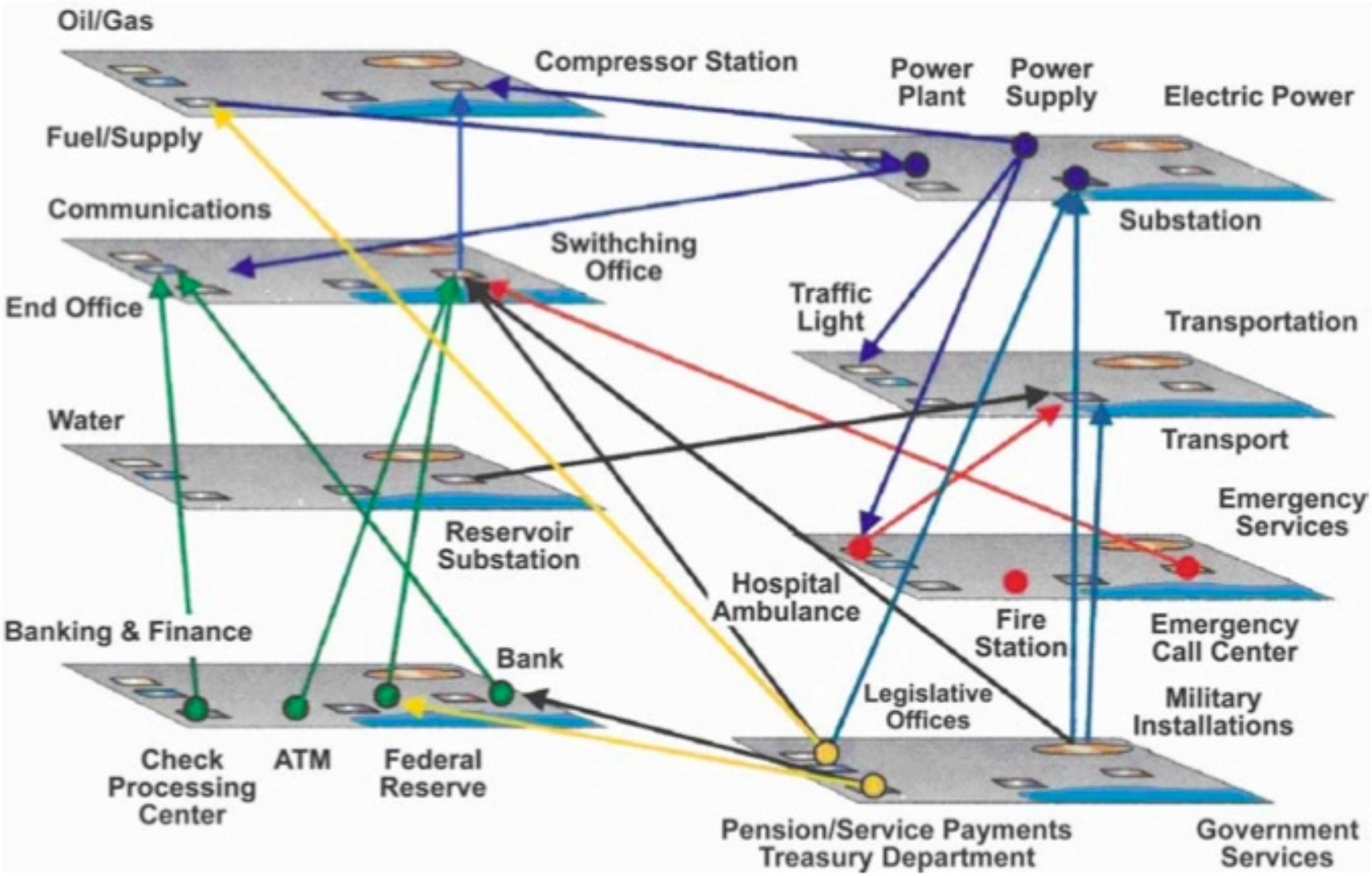
- An EMP strike may not happen today or tomorrow, but I'd be extremely surprised if we don't see an EMP attack within a decade.

VI. Okay, I Believe That An EMP Attack Might Occur, But Would My Crumby Little Network Really Be Something Critical to Protect?

US Critical Infrastructure Is Often Privately Owned and Operated

- Infragard, a joint FBI/private sector meant to improve the security of American critical infrastructure, was created precisely because much our country's critical infrastructure is privately owned and operated, so improving the security of that infrastructure isn't something that the government can do on its own.
- Critical infrastructure includes electricity and energy delivery, telecommunications (including the Internet), transportation, food, water, chemical industry, etc.
- Critical infrastructure areas also often interlock. For example, the food sector relies on the transportation sector to get food to market, and the telecommunication industry relies on the electrical grid.
- Hardening critical infrastructure against EMP is thus something which will require private sector participation.

Critical Infrastructure Interlocks



Nice Example of the Public/Private Critical Infrastructure Partnership

- 'In recognition of the fact that more than **95 percent of government telecommunications traffic traverses the public switched telephone network**, E.O. 12472 also directed the NCS to "serve as a focal point for joint industry-government national security and emergency preparedness telecommunications planning," a principle of public-private collaboration that HSPD-7 calls for all critical infrastructure sectors. '

  Statement of Dr. Peter M. Fonash, Terrorism and the EMP Threat to Homeland Security" March 8, 2005
  http://kyl.senate.gov/legis_center/subdocs/030805_fonash.pdf
  pdf page 6

The Internet2 Network (And Your State and Regional Networks) Are Critical Infrastructure

- We might like to pretend that things like the new Internet2 Network and your state and regional networks are inconsequential, but the reality is that they're ARE now large enough in extent and in capacity to be critical infrastructure.
- A simple proof by example: if the commercial Internet were to be taken down, or federal mission networks were to be successfully attacked, but Internet2 and associated state and regional networks were still up, would there be any attempt to fail that commercial traffic or that federal mission network traffic over onto Internet2?
- Obviously yes. It wouldn't be done without pre-consultation with relevant parties, but I can't see any way this would NOT happen in an emergency situation. That reality alone makes Internet2 and related networks critical infrastructure.

Moving On

- We've spent more than enough time on electromagnetic pulse, and I want to make sure we also get through at least some material on pandemic flu, and then maybe have some time for a question or two.

VII. Pandemic Flu

Previous Salsa Disaster Recovery Topics…

- Increasingly demanding requirements have driven a growing number of universities toward a continuously synchronized **"hot site"** model for IT disaster recovery/business continuity purposes (www.uoregon.edu/~joe/dr-bcp-bof/disaster-recovery-bof.ppt)
- We've also talked about he importance of having a **real time mass notification capability** for use during a disaster/other emergency (www.uoregon.edu/~joe/notification/emergency-notification.ppt)
- Pondering the remainder of the disaster recovery/business continuity space a bit the one thing which keeps popping up is **pandemic influenza.**
- After talking about pandemic flu a bit at Joint Techs in Batavia this summer, I wanted to also be sure to review the material from that talk here.

Why Would A Pandemic Flu Outbreak Impact IT System and Network Operations?

- Information technology impacts associated with pandemic flu may involve either personnel or infrastructure:
  - -- Unlike some other business continuity scenarios, a pandemic is a failure of the **human elements** of the computer/network system. Key IT personnel (just like anyone else) may contract the flu and cease to be available to do mission critical IT-related work; others may simply hunker down in an effort to avoid becoming infected. Absenteeism may be widespread.
  - -- IT-critical infrastructural services (such as electrical power) may become unavailable during the outbreak, potentially causing **cascading failures to occur**. Your facilities may be fine--but you may still end up impacted by failures elsewhere.
- In fact, IT systems and networks may play a crucial role in helping institutions to cope with pandemic influenza…

Got Flu? Move Stuff to the Online World…

- **Academic course work may move largely online,** by preference or by mandate (e.g., if large gatherings of individuals are banned)
- Quarantine measures and the need to provide care for infected family members may drive **increased demand for remote access** (to support work-from-home, etc.)
- Travel limitations will likely drive **increased demand for video conferencing** as a safe/approved alternative to national meetings
- Overloaded health delivery facilities may attempt to use **telemedicine** to meet the surging demand for medical services
- A tremendous amount of **personal messaging** (email, VoIP, etc.) will occur as families attempt to stay current on who's sick and who's well, etc. Many will also turn to the Internet for information about the pandemic, searching the worldwide web for information. **Recreational use** of the Internet may also rise dramatically given a bored, frightened, house-bound population.

Is The Pandemic Flu Really Something Which Will Likely Happen?

- "Will a pandemic influenza occur? If so, when will it happen? Answer: **Many scientists believe it is a matter of time until the next influenza pandemic occurs.** […]" http://www.pandemicflu.gov/faq/pandemicinfluenza/1071.html
- **"More than half of U.S. companies think there will be a global flu epidemic in the next two years.** Two-thirds think it will seriously disrupt their operations as well as foment social unrest. But two-thirds also say they aren't prepared. One-third of executives surveyed say nobody in their organization has been appointed to plan for a pandemic; another one-quarter couldn't or wouldn't answer the question." [http://www.washingtonpost.com/wp-dyn/content/article/2006/05/01/AR2006050101608.html]
- In November 2005, President Bush requested **$7.1 billion** in funding to help prepare for avian influenza (see budget details at http://opencrs.cdt.org/rpts/RS22576_20070123.pdf)

Why Is Pandemic Flu Potentially Such a Big Deal?

- The federal government doesn't make and approve multi billion dollar budget requests casually… Pandemic flu is being treated as potentially a very, very, big deal.

- Let's start with the 10 things the World Health Organization believes you should know about pandemic influenza…

World Health Organization: 10 Things You Need to Know About Pandemic Influenza

1. Pandemic influenza is different from avian influenza.
2. Influenza pandemics are recurring events.
3. The world may be on the brink of another pandemic.
4. **All countries will be affected.**
5. **Widespread illness will occur.**
6. **Medical supplies will be inadequate.**
7. **Large numbers of deaths will occur.**
8. **Economic and social disruption will be great.**
9. Every country must be prepared.
10. WHO will alert the world when the pandemic threat increases.

Each of those points is discussed in more detail at www.who.int/csr/disease/influenza/pandemic10things/en/index.html

The Influenza Pandemic of 1918

- **Worst pandemic in history**, **killing more than 50 million**, perhaps as many as 100 million. [http://www.ncbi.nlm.nih.gov/entrez/queryd.fcgi?cmd=Retrieve&db=PubMed&list_uids=11875246&dopt=Abstract] For comparison, ~19 million died in WW I.
- 50 million deaths from a 1918 base population of 1.8 billion ==> 2,777 deaths/100,000 people. **Extrapolating that fatality rate to today's population of ~6.5 billion ==> 180 million deaths today** [http://content.nejm.org/cgi/content/full/352/18/1839]
- "A total of **ten amino acid changes** in the polymerase proteins consistently differentiate the 1918 and subsequent human influenza virus sequences from avian virus sequences. Notably, a number of the same changes have been found in recently circulating, highly pathogenic H5N1 viruses that have caused illness and death in humans and are feared to be the precursors of a new influenza pandemic." [J. Taubenberger, Nature 437, 889-893 (6 Oct 2005)].

H5N1 Avian Flu as a Candidate Pandemic Agent

- While there are many infectious agents which might cause a pandemic, one of the most discussed ones is H5N1 avian flu.
- The bad news:
  -- H5N1 has infected humans via direct exposure to sick birds or their droppings, etc.,
  -- when humans do contract H5N1, it can be potentially fatal,
  -- treatment and prevention options for flu, a virus, are limited.
- The good news: there's currently no known human-to-human transmission path for H5N1.
- The worry: influenza is known to routinely mutate from year-to-year, and it is possible that one such mutation may yield a version which CAN spread human-to-human. Given high levels of **transcontinental and international travel**, if human-to-human spread becomes possible, spread of the disease may be rapid.

Speaking of Travel, Travel Controls for Potentially Infected Individuals Are Still Far From Perfect

- "TB patient insists he was never banned from travel" http://www.cnn.com/2007/POLITICS/06/06/tb.borders/index.html

- "Measles outbreak reported in Eugene: Officials said it's the second local case; the disease has probably been transmitted to others" http://media.www.dailyemerald.com/media/storage/paper859/news/2007/06/05/News/Measles.Outbreak.Reported.In.Eugene-2911826.shtml

  "[...] this shows you just how ill-equipped we might be for dealing with an illness such as a pandemic influenza case." Officials said the man who was first diagnosed with measles may have exposed people at: United Flight 6406 from San Francisco to Eugene, May 22. [...]"

Additional Facts About Avian Influenza Today

- **Over 220 million birds have died or been sacrificed** in an effort to halt the disease [influenza.un.org/index.asp?PageID=169]
- Countries where avian influenza has been confirmed in birds: Korea, Viet Nam, Japan, Thailand, Cambodia, Laos, Indonesia, China, Malaysia, Russia, Kazakhstan, Mongolia, Turkey, Romania [www.who.int/csr/disease/avian_influenza/avian_faqs/en/]
- There've been 317 cases of human infection with H5N1; 191 died [http://www.who.int/csr/disease/avian_influenza/country/cases_table_2007_06_29/en/index.html] ==> **60% human mortality overall** (but this can vary from country to country -- for example, 81 of 102 cases in Indonesia have been fatal).
- Countries where avian influenza has been confirmed in humans: Cambodia, Indonesia, Thailand, and Viet Nam (plus HK ca 1997) [www.who.int/csr/disease/avian_influenza/avian_faqs/en/]

How Should Sites Be Thinking About This?

- **Pandemic planning should be part of a site's overall disaster recovery and business continuity planning**, but if that's been going slowly, it may be worth starting to plan for pandemic flu as a special project in parallel with general DR/BCP efforts.
- **There's a good general college/university checklist** at http://www.pandemicflu.gov/plan/school/collegeschecklist.html but that checklist doesn't really dig down into the system and network specific side of things.
- **Some sites have been doing a great job when it comes to doing pandemic flu planning**, including in an IT-related context. For example, see: http://safetyservices.ucdavis.edu/emergencymgmt/AvianInfluenza.cfm -- I am particularly impressed by their development of alternative scenarios for "campus open" vs. "campus closed" crossed with different tiers of staff absenteeism (0-33%,34-50%, 51-75%, 76-85%, 86%-up).

Some Specific Questions to Ponder

- **Do you have "key IT people" who do things that "no one else can do?"** Identify them, and consider augmenting staffing for those key roles, and be sure to cross train existing staff members!
- **All routine procedures should be well documented**, so that if a system programmer or network administrator isn't available, others can follow the documented procedure to do routine tasks.
- **What about passwords in particular?** Do you have a process for emergency access to critical passwords (such as enable on routers, or root or administrator passwords on systems)?
- **Are facilities remotely (but securely!) accessible**, so that if travel is limited, or key staff are busy at home with family members, they can still do critical work? Or do systems routinely need remote hands for reboots, backup tape changes, etc.? Are some systems or resources limited to "on-campus-access only?"
- **Can you run unattended for protracted periods of time?**

Are University Faculty/Staff Ready to Work Offsite?

- Do university faculty/staff have **broadband connectivity**? (I would assume that getting broadband installed after a pandemic flu occurs might be tricky…)
- Do they have a **university-provided system** at home? (You don't want faculty/staff routinely doing university business on a system they're sharing with their family members) Are those systems up-to-date?
- Is connectivity between the home system and the university **secure**? If you're using a VPN for that purpose, does it have sufficient capacity?
- How will you communicate with employees who are all offsite? Do remote users have **VoIP and video conferencing** capabilities? Are those facilities tested and routinely being used? (Or is email and POTS enough?)

Will You Try to Have Uninfected Staff Remain On Site in Isolation?

- If you plan to have uninfected staff remain on site, isolated in your facility and away from potential infection, will you have basic requirements to support their sheltering-in-place, such as:
  -- supplies of drinking water, in case potable water supplies fail
  -- reserves of food ("MREs" or canned goods), and cooking gear
  -- sanitation facilities which don't require working sewer systems
  -- backup supplies of any prescription medications which staff may routinely require, such as insulin, etc.
  -- spare clothing
  -- cots and sleeping bags
  -- emergency cash (e.g., if staff need to buy diesel for a generator or handle other unforseen contingencies)
  -- face masks, gloves, hand sanitizer, disinfectant, trash bags, etc.
- Are you adequately provisioned for days? **Weeks? Months?**

Pay Attention to Departmental and Offsite Partners

- When you begin looking at planning for pandemic influenza, don't forget about your departmental and offsite partners… what are they doing to become prepared to cope with pandemic influenza? You should reach out to them and share your concerns and the steps that you're considering taking. Offsite and departmental partners may also serve as a crucial source of emergency temporary staffing…
- Track vendor and other visits, and identify examples where mission critical resources would have been impacted if those visits couldn't have taken place.

Architectural Redundancy

- If you currently rely on human intervention to restore systems or networks post-outage, should you plan to add additional architectural redundancy so that unattended failover can occur, instead?
- Is that redundancy end-to-end, including wide area connectivity, the campus LAN, networked systems, end-user access?

Oh Yes... The Feds Are Continuing to Look at the Pandemic Influenza Issue

- If you're interested, you may want to see the testimony given at

  "Beyond the Checklist: Addressing Shortfalls in National Pandemic Influenza Preparedness,"
  Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, Tuesday, September 25, 2007
  http://hsc.house.gov/hearings/index.asp?ID=89

Are There Any Questions?