TRANSNATIONAL RISK FROM ELECTROMAGNETIC PULSE

Clear and Present Risks to Industrialized Nations

EMP Impact:

Sudden Unplanned Outage of Computers, Electrical Grid, Critical Infrastructure, Health System and Water

Gary Lehman
Professor Maras
Contemporary Issues in Security Management, PMT754 Spring 2016
Gary.lehman@jjay.cuny.edu

Table Of Contents

Transnational Security and Electromagnetic Pulse

From *The Turner Diaries*: "*November 9, 1993* […the 70th anniversary of the Munich Beer Hall Putsch]…still three hours till first light; all systems are 'go'. It's a one-way trip to the Pentagon for me…the warhead is strapped into the front seat of the old Stearman crop duster airplane [hidden in a suburban barn], and rigged to detonate either on impact or when I flip the switch… Hopefully I will manage a low-level air burst directly over the center of the Pentagon…by the time I hit the defensive perimeter, I'll be making around 150mph, so that's about 70 seconds to the target; it'll be overcast, plane is painted to be nearly invisible, and I will be too low for radar-controlled fire. Considering everything, I believe my chances are excellent…" (Macdonald, 1978)

The FBI believes that *The Turner Diaries* was the blueprint for the Oklahoma City bombing on April 19, 1995, killing 168 and wounding close to 700 people. White supremacist McVeigh had a copy of the book in his getaway vehicle. *As the above 'doomsday scenario' portrays, in literature - and in actual experience - a committed, creative enemy – in particular an enemy intent on self-sacrifice for their cause – can be a devastatingly effective foe against which (under normal circumstances and levels of preparedness) there may be little defense*. It has been twenty-one years since the Murrah Building bombing. The 100th anniversary of the Munich Putsch is a mere seven years away. There may already be at this moment plans for a 'commemorative attack' by domestic or foreign national terrorists, either here in the US or somewhere on the European continent. Let us hope that life does not in this instance imitate art; this has happened too often and it is usually results in destruction of one kind or another. And if the attack takes the form of an electromagnetic pulse blast (EMP) blast, then all of us in the industrialized Global North will quickly and painfully understand first hand through bitter experience the full import of the term "transnational".

Professor H. Maras in her text *Transnational Security* advances the following definition: "Transnational security issues encompass military and nonmilitary threats that traverse borders around the globe, threaten the social, political, and legal order of nations, and adversely impact the quality of

life of the population of nations". (Marie_-Helen_Maras, 2015). With this definition, Professor Maras succinctly calls out the transnational impacts of EMP. Any consideration taking in the full reach and range of the transnational security challenges the world faces today is not for the faint of heart. Maras' book includes WMD's, transnational terrorism, organized crime, cybersecurity, natural disasters, human-made disasters, infectious diseases, and environmental security – all of which indeed fulfill the terms of the definition. Our challenge in this short paper is to pick 'the *greatest* transnational security threat'. It is a daunting challenge to pick *one* of these categories, or a particular threat included within the rubric of one of these categories, as the '*greatest* transnational security threat'. No further 'filtering' or directives were conferred, so our challenge and opportunity is to make a case for one particular threat of transnational scale. The selection here is the electromagnetic pulse blast, or EMP. For in all its immediate, short-term, medium-term, and long-term consequences, EMP rears up as a hydra of the Apocalypse combining all four Horsemen of the Apocalypse: conquest, war, famine & death. (The_New_Testament--New_Life_Version, 1969)

Risk and EMP Backgrounder

The first order of business is to define 'risk'. Risk has many variations of definition, but we can use the commonly-agreed upon 'Risk = Threat x Vulnerability x Consequence'. EMP is the disruptive electromagnetic field primarily associated with nuclear explosions or solar weather. The likelihood of EMP events occurring are significantly lower than that of conventional terrorist attack (involving the use of more-accessible technologies such as small arms, explosives or WMD), and also lower than dangerous hurricanes, seismic events, solar storms or possibly even supernovae. However, due to lack of prior significant, deadly experience with EMP (in the industrialized West, none at least of which we have actually been informed) and the public's *sense* in the recent past that EMP is not really a clear and

present danger, industrialized countries are highly and increasingly vulnerable with limited (although growing) understanding of the risk. And the life-safety *consequences of EMP is where this risk goes 'off the Richter scale'* [1] however. The next sections will discuss exactly what EMP "is", and the consequences of an EMP event.

What is EMP? How does it work, what are the causes?

EMP is a wave (usually radiated from the source, but in some military applications focused and aimed) of electromagnetic radiation which can cripple electrical and electronic devices which are in range. Electromagnetic threats can be caused primarily by a nuclear air burst, solar weather, or supernovae. Such natural events have occurred in the past and have been disruptive, and while they cannot be prevented, their effects can to some extent be mitigated. The disruptive effects of nuclear air bursts' electromagnetic radiation floods have been observed in the early stages of the above-ground nuclear testing programs of the United States and the former Soviet Union.[2]

The warning signs in the modern era have been there since the beginning of the proliferation of modern telecommunications. Louis J. Lanzerotti, a retired Distinguished Engineer on the technical staff at Bell Laboratories and former editor of the journal *Space Weather* 'became aware of the effects of solar geomagnetic storms on terrestrial communications when a huge solar flare on August 4, 1972, knocked out long-distance telephone communication across Illinois. That event, in fact, caused AT&T to redesign its power systems for transatlantic cables…' (NASA_Science_News, 2011)

[1] This is an idiomatic reference – there is no specific seismic component to an EMP attack. This is intended as an attempt to convey the profound consequences of EMP; with an implication by reference that seismic events are patently not 'avoidable' per se but can be mitigated, and similarly for EMP.

[2] Above-ground nuclear testing was terminated by the three signatories (the US, Soviet Union, and England) in October 1963 when the Nuclear Test Ban Treaty went into effect. France and China (non-signatories) continued atmospheric testing until 1974 and 1980, respectively. Below-ground nuclear testing continued by India and Pakistan until 1998 and as recently as January 2016 by North Korea. Below-grade testing results in subsurface contamination and radioactive releases into the lower atmosphere through radioactive dust clouds.

It may sound like a long shot that entities or events in space can affect us here terrestrially, but in 1859 a severe solar flare sizzled telegraph lines and ignited paper with sparking electrical arcs in the US; and on March 13, 1989 a big utility transformer was disabled in New Jersey and power was knocked out in Quebec (affecting six million people by interrupting power for nine hours) by a geomagnetic storm caused by solar weather. The 1859 event was called "The Carrington Event" after the British astronomer Richard Carrington who studied and charted the event, and is the modern benchmark for a major Coronal Mass Ejection (CME) event. What we are dealing with here (colloquially speaking) is the possibility that solar weather (or a supernova) can fry electronics on Earth. On July 23, 2012, a Coronal Mass Ejection (solar flare) narrowly missed the Earth. (NASA_Science_/_Science_News, 2014). [3] This event featured an ejection of a wave of solar plasma traveling at over 3,000 km/second towards Earth. It narrowly missed the Earth, hitting a NASA orbital spacecraft called STEREO-A (yielding a treasure trove of space weather data with STEREO-A acting in the role of a 'space weather buoy'. Had the wave directly hit the Earth's atmosphere (and depending on the magnetics involved) this likely would have disrupted the Earth's magnetic field, wreaking havoc on multiple terrestrial human technological artifacts. (Univ_Colorado_Professor_D._Baker, 2016). Upper latitudes (the Global North), littoral areas, and areas built on granite bedrock (which of course prominently includes Manhattan) are most vulnerable. (Kansas_City_Star, 2014). Similar effects would result from a supernova (Drs._Colgate_and_Miekle, 1978). Dozens of supernovae are detected each year by astrophysicists; most are too feint to be detected without visual augmentation. However, on

[3] Professor Baker of University of Colorado commented: "It is our belief that the conditions portrayed in this paper give power grid operators and emergency preparedness officials the kind of scenario they need to now model how extreme space weather might affect us all. We should waste no time in playing this extreme event through our technological "war game" scenarios"

January 7, 2016, and on February 9, 2016 two were detected and tracked by the Sydney Observatory (Australia) (Museum_Applied_Arts_and_Sciences, 2016). “Fortunately for us (one commenter noted), there is no <known> existing or possible candidate supernova within 10 parsecs of us, because the sheer power of such an event would become really dangerous to all life on Earth.”

From a military dimension, high altitude nuclear air bursts are the presumed primary means of EMP attack. A High Altitude Electromagnetic Pulse (HEMP) would result from such an airburst at 100,000+ feet. Three pulses would be emitted; E1 (short-term, high impact, creating very high voltages which will damage or destroy electrical equipment); E2 follows E1 (similar to lightning effects; E2 is expected to destroy circuitry which might have been only damaged by E1 and not outright destroyed; and finally E3 pulse (longer in duration; and the most dangerous effect for vulnerable power grids, because power lines and antennae serve as receivers, propagating the surge through the entire network power infrastructure). E3 is most similar to solar flares, CME’s and supernovae with the expected results on power grid discussed above (COLONEL_ROBERT_ORESKOVIC, 2011). A HEMP was depicted in the film *One Day After* (1983), whose story line involved a full nuclear exchange between the US and the Soviet Union in the early 1980’s. In fact, war fighting scenarios *anticipate* a high atmosphere nuclear detonation as a prelude to a nuclear attack, as it is intended to ‘blind’ the target’s communications infrastructure, leaving the target in a compromised condition unable to effectively retaliate and thus exposed to nuclear blackmail.

The effects of high altitude atomic blast HEMP was first observed in 1962. Multiple above-ground nuclear atmospheric tests at varying altitudes up to 250 miles high were conducted at Johnston Atoll, approximately 825 miles southwest of Hawaii. (Global_Security, 2016). A variety of test explosions were conducted: the ORANGE, TEAK, KINGFISH, CHECKMATE, and STARFISH nuclear tests

were completed between 1958 and 1962 of varying yields and at varying altitudes. (R.Pfeffer_and_D._Shaeffer, 2010). [4] During a temporary period of lessening of superpower tensions following the breakup of the Soviet Union, several Russian nuclear physicists attended the 1996 National EMP (NEMP) Conference in Albuquerque, NM to be inducted as Fellows in the NEMP Honor Society. These physicists did poster presentations detailing the findings of HEMP testing over Kazakhstan during a similar time period. Their results were difficult to closely compare and interlock with US testing owing to divergent measurement methodologies (and the land vs. sea environments of the tests), but generally similar results were observed. The Russian reported results were consistent with CIA findings acquired through national technical means.[5]

Spectacular visual evidence of the blasts was seen in Hawaii (over 800 miles away), along with more mundane physical effects including electronic and electrical systems failure, street lights failing, circuit breakers tripping, and telecommunications relays failing. (COLONEL_ROBERT_ORESKOVIC, 2011). Given that land mass (in particular that with a granite shield, such as exists throughout portions of the Global North) intensifies the magnetic field effects, the observed effects in Hawaii were less pronounced than would otherwise have been noted. The extent of the damage was thought to be higher over the Kazakhstan land mass (which proved to be the case), although differences in measurement methods made detailed conclusions speculative.

There are other military weaponry models involving EMP. Directed waves of EMP is a different means of delivery, and can be administered by aircraft or UAV's with loiter capability to selected

[4] It is interesting to note the Russian spy vessels were dispatched to the Johnston Atoll vicinity to observe US atomic weapons testing. Russian monitoring and measuring methodologies were perfected during these observations, and the resulting HEMP measurements on subsequent Soviet HEMP experimentation on land environments in Kazakhstan remain secret.

[5] Please see Appendix Two

targets such as enemy command locations, individual buildings or neighborhoods, battlefield assets or naval task forces. Indeed, the military efficacy of EMP is such that the DOD has funded EMP weapons systems and battlefield survivability tactics, and is thus aware of the military potential. Many military assets already have levels of EMP protection as a function of ABC (atomic, bacteriological, and chemical) survivability. In the next sections we will review EMP consequences and the Navy and Air Force weapons systems under development.

Consequences: Why this is the greatest transnational security threat

The apocalyptic dimensions of HEMP due to high altitude nuclear explosion (HANE) or solar weather events has been the subject of a huge literature of technical journals by scientific/engineering organizations, US and foreign governments, proceeds of government hearings and of course, popular culture. *One Second After* by Dr. Forstchen, is a story about one man struggling to save his family and his small North Carolina town after American loses a war that sends American back to the Dark Ages. It begins with the quotation from Bhagavad Gita, popularized by Robert Oppenheimer (father of the atomic bomb as head of the Los Alamos Laboratory in WW2), "Now I am become Death, the destroyer of worlds." (Dr._William_Forstchen, 2008). Underlying the apocalyptic vision is the loss of electricity and disruption of electronics. Among the first people likely to die under an abrupt loss of electricity and electronic appliances are those under life support without adequate or sustained backup, and those in aircraft which are in final landing patterns and which are relying on instrument landings. The narrative of apocalyptic consequences of EMP continues from that grim starting point.

Before we launch into an enumeration of EMP circumstances and consequences, we can take a look back at the Russian EMP testing. Russians conducted unfettered land testing of HANE, with an army of scientists and monitoring equipment in place, which resulted in substantial documentation

about the effects of HEMP on land line power transmissions. (V.N.Greetsai, 1998). Most of that information is still a state secret. To put into context the following discussion of 'consequences' of EMP, we should review the findings (to the extent which they have been published at any rate) at a high level of the Russian HEMP testing over Kazakhstan. The following observations were reported from the 1962 "Test 184" with detonation 290 kilometers over Kazakhstan (300 kilotons - the atomic bombs used in WW2 were approximately 13-15 kilotons each): a fire was started in a power plant (reportedly destroying the plant); shielded electric cabling buried three feet underground was destroyed; dielectric breakdown caused diesel generators to fail; overhead telephone lines destroyed; all overvoltage protectors were set on fire; all fuses on the 570 kilometer line were blown; radios were damaged up to 600 kilometers from the origin, and a radar about 1000 kilometers distant was knocked out. These results are generally consistent with expectations from the US testing at Johnston Atoll extrapolated to testing over a land area. So the effects on power lines (and even on *underground* power lines three feet under the surface) are not hypothetical or "*modeled*" -- but have actually been *observed*, as has similar results from solar flares as discussed above.

It should be noted in this context that electrical transformers, which are required to operate the power grid, are for the most part unique, custom-built, not built in the United States, expensive, and need to be individually designed and built. Such was the case with the PSE&G Metcalf power station in California, which was attacked in April 2013 by snipers with assault rifles who took out radiators, causing the transformers to overheat and become destroyed. 120 shots were fired over seven minutes after removing two 75lb manhole covers and cutting fiber-optic cables connecting to surveillance cameras, and with impunity, took out 17 custom-built transformers. The snipers aimed for equipment componentry which would NOT cause any flashes or sparks or explosions, which would

have attracted attention. This was clearly an informed (and possibly inside) job. This is all the more worrisome, given that we know that domestic and foreign national terrorist sleeper cells exist, including Timothy McVeigh analogues and the San Bernardino shooters. (Halper_and_Lifscher, 2014)

Radiation Impacts on Large Scale Integration (LSI)

There is an important underlying concept in computer science and operations – with implications not only for transactional information technology but also power grids, industrial automation tied to SCADA systems and large scale integration (LSI) – 'chips' or integrated circuits – which are fundamental to our 21st century way of life in the Global North... The concept involves resiliency engineering. The concept is colloquially known as the 'sick but not dead phenomenon' or more generally, 'soft errors'. One source of such errors is radiation, and IBM pioneered research into this subject with its influential January 1996 IBM Systems Journal of Research and Development article entitled "IBM experiments in soft fails in computer electronics (1978-1994)" (IBM Corporation, 1996) which examined the effects of radiation on Very Large Scale Integration (VLSI). An array of other technology organizations and academic institutions continued the research in the same and expanding directions. Many examples of unexplainable, transitory corruption and intermittent unreliability were considered and documented both in the United States and in Europe, and these effects were distributed across a cross-section of vendors and situations. After much perplexed study by many technical and product engineering teams, radiation effects on LSI were at last determined to be the culprit. (One can only imagine the exasperating circumstance of transient cache contamination for transaction processing in the financial or brokerage industry!). These conditions are discussed at length in *Soft Errors in Modern Electronic Systems* (Nicolaidis, 2011). Continued IBM focus on these issues, in particular as relates to the power grid, led IBM to research means by which the power grids in the

European Union and the United States could be secured. These efforts resulted in publication of research findings and recommendations in IBM Systems Journal of January 2016, *Securing the electric power infrastructure* (IBM_Journal_Research_&_Development, 2016).

Many computer networks with redundancy/resiliency engineering respond well to abrupt network disconnection and conclusive hardware 'down hard, casters up' conditions – i.e. when the connectivity and/or hardware is 'dead' and non-revivable. In instances like that, the redundancy kicks in upon detection of loss of 'handshake', the redundant components under those circumstances will automatically assume the workload – to such an extent that systems thus configured can recover and complete distributed database, high transaction rate operations and 'transactions in flight' (in-process transactions involving program to program and real-time database updating which are not yet committed). (This capability is particularly important with, for example, money transfers). Problems surface however when the underlying supporting infrastructure is moribund and 'stalled'. Without a 'down hard' condition, the redundancy will not kick in, contributing to queuing of transactions without database commits and orphaned 'transactions in doubt', as well as loss of designed workload management/rebalancing/rerouting capabilities. (Karla Arndt, IBM z/OS Predictive Failure Analysis, 2010). Thus an IT network, storage systems, or processor complex 'brown out' can be far more disruptive (and destructive) to databases than a 'down hard' condition, precisely because the system is not declared 'dead' and thus the protective/redundancy measures are not invoked. We can expect that an unexpected solar weather event to an unprepared land environment will experience varying impacts over a wide area in a highly-interwoven IT or industrial virtual campus or commercial region, resulting in intermittent outages and 'brown outs' of both power and IT connectivity. Leading inevitably to multi-dimensional catastrophe in our society.

Consequence Identification: Risk = Threat x Vulnerability x Consequence

The apocalyptic effect on society of EMP with its resulting telecommunications, power, electrical and electronic disruptions should be coming into focus. It is not just 'state of the art electronics' which will be disrupted, but even diesel generators will fail due to dielectric breakdown; and even toilets won't flush. The exhaustive discussions above stepping through the EMP effects with deliberation will serve to validate the following horrible consequences.

For easier readability, EMP consequences will be enumerated via a list (which is not a comprehensive one):

- Intermittent failures throughout the power grid over an extended area, possibly as large as 1/3 the contiguous 48 states in size, depending on height, magnetic characteristics and megaton range of the nuclear bomb used to create the HEMP, as well as what (if any) shielding is present on power facilities
- Those on life support systems which do not have functioning electronic monitoring and/or adequate power back up will perish
- Passengers and crew on aircraft which are on final approach under instrument landing are at grave risk, unless the pilots are really on top of things and are effective under pressure
- Radar controlled airport operations and landing instructions are impossible resulting in aircraft running out of fuel, many will attempt to land at once, potentially creating accidents on runways (with no functioning firefighting equipment) which will potentially strand all airborne aircraft with no viable landing sites
- Refrigerators will cease to work, with food rotting
- No waste processing
- Cell phones? There are no satellites, so there will be no cell phone service. Land lines? Those land lines are all fried, so no land line telephony communications
- Radio? No, even if hand cranked, the EMP will have likely corrupted the radio circuitry
- No email No TV No Social Media NO INTERNET No First Informers
- No drugs for those with chronic conditions when supplies run out
- Gas line explosions with no water or functional firefighting equipment to battle the blazes
- Food shortages, starving millions; water shortages due to no water purification capability, with untold numbers killing and dying for water
- Biblical pestilence from rotting food and garbage (no refrigeration or functioning garbage trucks for haulage)
- Rampant criminality
- Gas supplies for cooking and heating will be unavailable
- Potential exists for runaway nuclear reactor with SCADA systems compromised
- Spent fuel rods from nuclear facilities may overheat their structures without cooling available, causing radioactive plumes
- Mass scale industrial catastrophes are possible with SCADA systems in a failed state

- Logistics will be damaged or disabled due to vehicles relying on microprocessors and will eventually run out of fuel, with no fuel pumping capability and no fuel refining
- People don't know how to grow food, and have no implements to do so even if they did

The objective of this section of the paper was to establish that the 'consequence' component of the Risk equation was so significant as so to direct all reasonable-thinking persons to agree that exposure to EMP is one of the – if not *the* – greatest transnational security threat. Furthermore, it was intended to develop how and why EMP and its consequences match the definition advanced by Professor Maras, viz: "Transnational security issues encompass military and nonmilitary threats that traverse borders around the globe, threaten the social, political, and legal order of nations, and adversely impact the quality of life of the population of nations". This is especially the case when considering the '*One Second More'* Scenario Extensions offered in Appendix Three.

Threat Summary

We can summarize the threat of EMP to the United States and to the rest of the Global North along the following lines:

- Solar weather / Solar flares
- Supernovae
- High altitude nuclear explosion to disable the US retaliatory capability
- High altitude nuclear explosion by a rogue state such as North Korea and/or Iran
- Targeted non-nuclear EMP weapons systems

By enumerating these EMP threat sources we can plainly see that we have limited to ability to prevent some of these threats -- and yet we are crucially responsible to define and implement mitigations. The first policy issue will be to determine which of these threats to concentrate on first; and to also via analysis ascertain whether or not mitigations for one of these threats will serve dually to mitigate one or more of the other EMP threat sources.

As indicated by recent experience with Islamic sectarian attacks and those against the West (and for that matter the fictional crop duster attack with which we started this assignment), it is by now clear that an ideologically-committed foe will stop at nothing - not even their own demise - to prosecute their attack. *One Second After* conceptualizes an attack no less creative than the 9/11 attacks: a collaboration between Iran and North Korea in the simultaneous launch of modified SCUD missiles from offshore containerships targeting Korea/Japan, the US (detonated over Utah, Kansas and Ohio), and Eastern Europe and Russia with high altitude nuclear explosions, with the objective of initiating existential EMP consequence chains in the targeted regions. In the book, the US responded with nuclear strikes against Iran and North Korea. If policy makers decide that the threat of an EMP attack by a rogue state or states is a credible threat, this will then add a whole new layer of complexity into the plan to detect, mitigate or prevent such an attack. Surveillance – with potential boarding, search and seizure of shipping in international waters is a tricky maneuver. However, given that both Iran and North Korea have sophisticated space programs with successful histories (in Iran's case) of twenty-five years of rocket launches and putting satellites into space, assuming away the capabilities of potential (or for that matter avowed) adversaries – ruled by leaders sharing behavioral traits with Caligula – would be ill-advised.

What are the Government and the DoD Doing About This?

What is being done about all this? The answer depends on whom you ask. The Air Force will report that Boeing and the Air Force strategic planners are fielding an electromagnetic pulse weapon capable of targeting and destroying electrical systems without any collateral damage (and with no human danger). It's a CHAMP, literally (Counter-electronics High-powered Microwave Advanced Missile Project) which can take out the electricity and electronics in a building or neighborhood and take it back to the 12th century. CHAMP reportedly took out seven targets on one mission in 2012. (Boeing, 2016). Current status therefore would presumably be significantly advanced from that point. Obvious applications include interdiction of enemy electrical supplies and assets. Of course this presumes that you have a discrete target; it is a little challenging however to

conceptualize how to use this weapon to fight ideas such as those expressed in *The Management of Savagery* by Abu Naji, the Islamic State strategist. However, it is good to have this kind of weapon in the inventory in the event that Putin decides to make additional land grabs or to have this system available for pinpoint operations, or to secure ingress/egress routes for inbound/outbound strike packages and to complement other systems designed for that purpose. From the standpoint of protecting Americans from an EMP attack, the Air Force doesn't seem to have much to offer with this weapon, nor is it intended to. Owing to early experiences with EMP at Johnston Island, the Air Force has implemented EMP survivability hardening on ICBM sites since the beginning of Minuteman.

The EMP attack scenario proposed by *One Second After* directs that SCUD missile(s) are launched from otherwise innocuous freighters, tankers or containerships and are lobbed up into the atmosphere and detonated in the general vicinity of the northeast corridor of the US or somewhere way up above the 'middle' of the continental 48 (no specific targeting is required). This offers the approach that the US Navy could play a signal role in maritime domain awareness and via *Aegis* (or any follow on architecture), have interdiction capability of any short range missiles launched off our shores. H. Cooper and R. Pfaltzgraff propose a layered defense utilizing this system to protect the US (H.Cooper_and_R.Pfaltzgraff, 2010). The white paper includes the provisioning of UAV's with advance sensor capability and anti-missile missiles to identify and intercept enemy launches in the boost and ascent phase after launch. There is no information readily available to assess whether such a program exists or what the status is, if it does. Other key questions relate to policy decisions and implications of interdiction of non-combatant, non-belligerent vessels on the high seas during peacetime. However, there are aspects of the white paper which warrant closer examination within the context of an architected defense against EMP attack.

Moving in that direction from a Department of Defense standpoint is the CBRN Survivability Oversight Group (CSOG) DoDI 3150.09 established in 2008 (Department_of_Defense_Instruction, 2015) and which is missioned to assess and improve new and legacy equipment vulnerability and survivability in a nuclear weapons

effects environment (including EMP). This effort is both appropriate and necessary. However, it falls short of a holistic approach with the risk to civilian infrastructure in mind; nor is that or should that be the mission of DoDI programming. It is hoped that findings which are relevant to the civilian sector (if these findings do not breach security boundaries) will be shared to the appropriate departments and directorates.

With the wealth of information and data out in the public domain (and also all the data and knowledge contained in our federal intelligence agencies), and the 'clear and present nature of the dangers' of EMP attack, it is reasonable to expect that our government has set forth a series of policies and directives backed by responsibilities and accountabilities which are intended to secure a safer future from EMP events for the citizenry of the United States. This is unfortunately not the case.

EMP Commission…and… The Importance of Being Earnest

In the wake of 9/11 the EMP Commission was established, whose Charter and Mission Abstract are listed in Appendix Four. (EMP_Commission, 2004). A review of the Report and findings indicates a detailed knowledge of the problem with an important series of recommendations, mitigations, and responsibilities for the various critical infrastructure sectors examined, which included "electric power, telecommunications, banking and finance, fuel and energy, transportation, food infrastructure, water supply, emergency services, space services, and government". Thus the Report contains an encompassing capture of the full range of foreseeable threats in the event of an EMP attack. One wonders then *why* EMP hardening of civilian infrastructure is still so misunderstood with such spotty-at-best actual *support*, other than supportive hand-wringing and pious pronouncements! It is high time for our policymakers to collectively and with determination to take an earnest, hard look at this danger and do what they are entrusted to do – look after the well-being of the US. Perhaps the

following offers us a lifeline to getting to the bottom of the question about why this issue has failed to gain much traction:

> **"<there is> a tendency in our planning to confuse the unfamiliar with the improbable. The contingency we have not considered looks strange; what looks strange is therefore improbable; what seems improbable need not be considered seriously." —Thomas C. Schelling, Foreword, in Roberta Wohlstetter, *Pearl Harbor: Warning and Decision*, Stanford University Press, 1962, p.vii.**

There has been some (glacial) progress on this issue. One of the major stonewalling structures has been the energy industry. There was some positive traction in 2013 when the Federal Energy Regulatory Commission (Federal_Energy_Regulatory_Commission, 2013) directed the North American Electric Reliability Corporation (NERC) to draw up standards for power infrastructure reliability in the event of EMP. NERC has undertaken this responsibility and has proposed standards to FERC. The proposals for those standards have however run into resistance at FERC, and work presumably continues to resolve the NERC and FERC differences in this regard. (NERC_via_F._Koza, 2016). Development of these standards is crucial because without them, there is no baseline for assessment of progress towards resiliency goals. ("If you don't know where you are going, any road will get you there…").

One of the other big problems in the matrix of US governance and policy around this issue of EMP is the lack of focal point and accountability/responsibility. The nation will turn its lonely eyes to Department of Homeland Security for leadership and guidance on the issue of electric grid resiliency, however DHS "has no statutory authority whatsoever to regulate the electric grid". (Subcommitt on Cybersecurity, 2014). Therefore, DHS has been in an 'advisory' capacity. In June 2015 however, that started to change course towards a more positive direction with the passing of the Critical Infrastructure Protection Act (CIPA) by the Committee on Homeland Security. (Homeland_Security_Committee, 2015). "CIPA directs and empowers DHS to harden and protect our

critical infrastructure including power production, generation and distribution systems. I'm encouraged by this movement and expect my colleagues in the House of Representatives to take this decisive step to protect our nation when CIPA comes to the Floor for a vote" (Congressman Trent Franks, R. Arizona, 6/26/15). The die is thus cast and this thread is set for progress into the House of Representatives.

In the last section of this paper we will return to this subject, in section "What Is To Be Done NOW?"

Role of Private Security Agencies

Private security agencies cover many industries and geographies, and provide a wide range of services from consulting to security staff augmentation to technology implementation/systems integration (Booz_Allen, 2016), to strategy consulting (Bain_and_Company, 2016) and facilitation services. As such, there are many opportunities for consulting / private security firms to participate in the efforts to mitigate the risks of natural and man-made EMP. Much of the defensive work effort will be in the realm of pure scientific research (to better understand the physics and consequences of EMP on electronics and hardware-based defensive technology); and some will be deep investigations (G4S, 2016), HUMINT, national technical investigation and surveillance, and cyber-surveillance; and some of the effort will be in risk assessment, policy formulation (McKinsey, 2016) , enforcement, and site life support and operational continuity under adverse circumstances (Academi, 2016).

One of the traditional areas of security agency product and service offering is security staff augmentation and management; these services would not have a notable role to play. However, there are many opportunities for private security firms and management consulting firms to engage clients in EMP risk management.

For example, security or management consulting firms whose senior members have experience in government procurement, federal procedures/regulatory environment, and generally “federal ways and means” will have many potential roles (Boston_Consulting_Group, 2016). These could include facilitating planning sessions to set technical direction and facility protection priorities; site infrastructure risk assessments (Risk_Mitigation_Consulting, 2016); industry-wide means of collaboration; partnership identification and development, and similar planning and strategy functions. One of the risks of scientific research from a product or service standpoint is that scientists are driven by the impulse for scientific discovery and product or technology exploitation. Therefore , private security firms which also have significant systems integration and complex systems project management skills could *provide continued focus for extended technology-based solution development* and *focused direction* of otherwise ‘pure science’ efforts towards actionable defensive technologies (in order to avoid pure science for science’s sake) (PWC, 2016). Many private security firms have a particular knowledge and expertise in specific critical infrastructure sectors (Tyco_Security, 2016) and as such, can provide guidance and leadership role under the sponsorship of the client’s senior executive team.

One of the recurring themes of ‘big government’ is the duplication of effort between different organizations, combined with exculpatory impulses aligned with the organizational Prime Directive of “Preserve Self”. This is furthered by the “not invented here syndrome” which tends to marginalize and undermine positive ideas from across the aisle or from a “competing” organization or entity (and conversely the tendency to either highlight poor performance of the partner agency or at the very least to disavow ownership or participation in it). This is a key area that external agents can bring to the table in helping with complex project management; being aware of and calling out siloed behavior

which is counterproductive to the government's overall mission of providing for the well-being of the citizenry.

The *biggest contribution* that the private security/consulting industry could make in this space is to keep the pressure on the US government to stay focused on this problem, and project managing progress towards (and achieving) an appropriate level of 'EMP-hardening' of key elements and nodes of our power grid. It is axiomatic that government is 'session-driven' and 'Administration-driven'. The exigencies of the moment – the 'crisis du jour' will often 'trump' attention and focus, often (usually) to the detriment of sustained progress towards medium and longer-term goals. This is especially the case where there is fragmentary or non-existent responsibility or accountability. This is where a skilled consulting organization with experience in complex systems management (and granted the authority to not sweep problems under the rug) can make an important contribution to our national security. In a democracy, our politicians sometimes respond to human services and education needs in the 'here and now', and will prioritize budgets and staffing to those initiatives, instead of to vague and distantly-possible virtual threats. (The preeminence of EMP in popular culture in science fiction may well be undermining a popular conception of the reality of EMP threats from solar weather, and certainly from HEMP pulses owing to rogue nation attacks against the US homeland). Private consulting firms should be engaged to perform a critical role in directing and facilitating sustained focus and progress in this crucial security area.

What Is To Be Done NOW?

The 'digital divide' is diminishing in the United States; that is, the digital have's and have-nots documented in the late 1990's. (Stanford_University, 2016). Access to computers and digital

technology between rich and poor has been rapidly fading as an obsolescent concept with the advance of cheaper computers and all kinds of digital technology, combined with an increasing familiarity with digital processes as a function of exposure among younger portions of the population. Appreciably close to 100% of City University of New York students have broadband connected smartphones, up from 90+% three years ago. (Professor_Adam_Scott_Wandt, 2016). We all rely heavily upon our smartphones and digital assistants and electricity is required for these to operate. Thus the reduction of the digital divide *is a good thing*, providing positive social justice and generally speaking improved opportunities for personal advancement, but also adds dimensions of catastrophe to the society as a whole in the event these services become suddenly unavailable. Commensurate with a sea change in reliance upon personal digital technology is the increased reliance on industrial automation and systems, which are susceptible to failure with loss or damage to electricity. So the threat spectrum has grown immeasurably with the advance of digital technology in every dimension. This is not a problem which is "going away" any time soon. The 'clear and present' nature of the threat and vulnerability increases day by day.

It also should be noted that our electric grid is in constant state of change and being continuously upgraded to keep pace with surging demands. This presents an important opportunity for *intelligent* upgrades; that is, upgrades not to just replace capacity, but to also improve resiliency to blackouts and in particular, brownouts which can result in the soft errors previously discussed.

These considerations make all the more urgent a series of urgent imperatives.

The issue of EMP and mitigation/defense against natural and man-made attacks using electromagnetic weaponry is complex and far reaching. A leadership decision needs to be made to protect our infrastructure comprehensively, in the same fashion of President John F. Kennedy

proclaiming "... We choose to go to the Moon in this decade and do the other things, not because they are easy, but because they are hard; because that goal will serve to organize and measure the best of our energies and skills, because that challenge is one that we are willing to accept, one we are unwilling to postpone, and one we intend to win ...". There is little question that the expense of hardening our critical infrastructure will be high, but we don't *know how high* unless standards are developed as to how much infrastructural hardening is actually required to provide reasonable protection against anticipatable coronal mass ejection/solar flare events and HANE attack.

We see part of the puzzle starting to come together. There is general recognition that our potential adversaries can be creative, deadly and will think outside the box to harm us. Rogue states currently (or soon will) have the capacity to manufacture (or steal or purchase) nuclear weapons which can create EMP damaging to the US critical infrastructure and way of life. Technical planning to interdict and if appropriate destroy ships, aircraft or medium-range nuclear-tipped rockets is proprietary, and belongs safely secure inside the US intelligence community; it would be comforting to learn that a multi-layered robust defense already exists or is in the advanced stages of development, but this is unlikely to be the case. We *do* know that individual military systems are hardened against EMP attack, but we also know that no ratified standards exist at the Federal Energy Regulatory Commission-level to be directed towards the energy critical infrastructure private sector. Thus we have - and are going to continue to have for the foreseeable future - a vulnerable electrical grid. Even if the country had a survivable electric grid, many components would be rendered temporarily or permanently disabled by EMP in the event of a massive solar event or a high altitude nuclear airburst.

The flip side of this discussion is that 'national security' is defined not exclusively by the security of our critical infrastructure, but by the vitality of the people of the country. Towards this goal, every

country has to assign and apportion priority, attention, effort and funding towards those sectors deemed most critical; and human services and education will often represent immediate community needs and thus take precedence over measures to mitigate *possible* future attacks or natural events. Our elected officials, in collaboration with community leadership, will have to provide guidance in these tradeoffs.

In March 2015 the General Accounting Office delivered as assessment on current efforts to date since the 2008 EMP Commission report. (General_Accounting_Office, 2016). This study tied together many of the actions taken - and challenges ahead - to secure a more resilient critical infrastructure. The report acknowledges the attention given and incremental progresses which have been made since the publication of the EMP Commission Report in 2008. However, the report calls for increased collaboration between the DOE, DHS and FERC to create the standards towards which the industry must make progress. In addition, GAO call for DHS to be on point to structuring the effort and defining internal roles/responsibilities and collect additional risk inputs to further inform assessment efforts. The National Infrastructure Protection Plan has called for identification of critical energy assets, and this remains a work in progress. GAO calls upon DHS to articulate the 'threat, vulnerability, and consequence" factors so as to put all efforts going forward into a concrete context which is responsive to the task and accessible to those who seek to review the plans and programs (and funding) which need to be put in place to progress from the currently-vulnerable state. DHS and DOE are tasked to collaborate to develop risk management activities addressing EMP risks. These could include directing research and development activities, leveraging the data already in-house from the early era of atmospheric testing. While the time might not be right at the moment, efforts should also be made to leverage the data collected by the former Soviet Union during its many years of above-ground nuclear

testing. In particular, some highlight recommendations include the following, which have been also been combined/expanded/enhanced with observations and insights resulting from the research for this paper:

- Build community awareness through education of the risks of EMP from solar activity and EMP weapons; this will put EMP resiliency investment into context for the public
- Complex interdependency modeling and simulation in 'Smart Grids' to assess propagation of overloads and 'sympathy sickness' in interconnected networks
- SCADA systems remain vulnerable in all parts of the private sector and efforts to date to protect SCADA systems have focused on cybersecurity aspects, which have absorbed the bulk of attention and funding. It is time to broaden the effort and funding and develop hardware and software resiliency in the face of CME/solar flares and HANEs
- Increased focus on Space Weather to better identify and predict solar flare activity
- Space Weather protection, mitigation and response guidelines are lacking with DHS's FEMA on point to provide these
- FEMA and DOE to collaborate on long-term power outage plans and procedures
- DHS, FERC, NERC, state regulatory bodies and private sector must collaborate on liability and funding for private and government power facility EMP protection and redundancy facilities
- DHS needs to further develop emergency management plans and procedures for solar or man-made HANE events, which will provide contemporaneous status to centralized locations for enhanced reportage and incident management
- Develop a joint-military task force doctrine to deal with the potential of rogue states conducting HANE attacks against US territory
- Independent efforts by DOE and DHS to determine complex systems interdependency and cascading effects/failure analysis should be interlocked and mutually validated and verified
- DHS is tasked to complete the in-process Power Outage Incident Management process
- Pre-siting of tested, current maintenance-level equipment which has been tested for interoperability is essential for effective redundancy and reduced downtime in the event of a hardware or network service disruption. DHS is further tasked to define what spare parts/equipment inventory is essential by each FEMA Region, with objective to minimize downtime and service recovery for both power and critical infrastructure facilities
- 'Simulate, train, exercise, and test recovery plan' is essential for having a successful plan in the event it is needed. The Secure Grid and GridExII plans, exercises and drill should be conducted every year to ensure a maximal state of readiness

These are encouraging developments. An involved, earnest, informed process of discovery and policy formulation is essential to progress a complex problem such as EMP vulnerability for our society. The extent to which Departments collaborate and undertake the shared mission will determine the

level of positive progress. This is a multidimensional problem with competition for funding, attention, staffing and resources; and involves not just the federal and state agencies but also the private sector and human services advocacy organizations which are not likely to be fully-supportive of costly efforts to improve resiliency of critical infrastructure for an event stack that suffers from the remoteness of experience and understanding noted above by Roberta Wohlstetter noted above. The recent passing of the Critical Infrastructure Protection Act (CIPA) by the Committee on Homeland Security (which will now go to the House) will continue the country's positive journey towards a more resilient critical infrastructure.

Perhaps then, by the time the 100th anniversary of the Munich Beer Hall Putsch, our country will have achieved enduring infrastructural resiliency against EMP attack here at home, and that it will have sufficient capability to deter any potential adversaries from testing it; knowing that if they *do* test it, they shall be bringing in on themselves the inevitable and decisive response.

References

Karla Arndt , IBM z/OS Predictive Failure Analysis. (2010). *Detecting Soft Failures Using z/OS Predictive Failure Analysis.* Rochester, Minnesota: IBM Corporation. Retrieved from http://www.gsebelux.com/sites/default/files/GSE%20Defecting%20Soft%20Failures%20using%20zOS%20PFA.pdf

Academi. (2016). *Managed_Support_Services_-Life_Support*. Retrieved from Academi: https://www.academi.com/pages/managed-support-services

Bain_and_Company. (2016). *Bain_and_Company*. Retrieved from Strategy: http://bain.com/consulting-services/strategy/index.aspx

Boeing. (2016). *CHAMP - Lights Out*. Retrieved from The Boeing Company: http://www.boeing.com/features/2012/10/bds-champ-10-22-12.page

Booz_Allen. (2016). *The System Integrator*. Retrieved from Booz Allen: http://www.boozallen.com/envoi-articles/starts-with-characters/the-systems-integrator

Boston_Consulting_Group. (2016). *Boston_Consulting_Group*. Retrieved from Boston_Consulting_Group: http://www.bcg.com/expertise/industries/public-sector/solutions.aspx

COLONEL_ROBERT_ORESKOVIC. (2011, March 24). *ELECTROMAGNETIC PULSE – A CATASTROPHIC THREAT TO THE HOMELAND*. Retrieved from U.S. Army War College: http://www.dtic.mil/dtic/tr/fulltext/u2/a547355.pdf

Department_of_Defense_Instruction. (2015, April 8). *The Chemical, Biological, Radiological, and Nuclear (CBRN) Survivability Policy*. Retrieved from DoD Defense Technical Information Center: http://dtic.mil/whs/directives/corres/pdf/315009p.pdf

Dr._William_Forstchen. (2008). *One Second After.* New York : Tom Doherty Associates.

Drs._Colgate_and_Miekle. (1978, Supernova radio pulse searches and possible improvements in sensitivity). Supernova radio pulse searches and possible improvements in sensitivity. *The Astrophysical Journal*, 1076-1086. Retrieved from The Astrophysical : http://adsabs.harvard.edu/full/1978ApJ...220.1076M

EMP_Commission. (2004). *Report of the Commission to Assess the Threat to the United States from EMP Attack*. Retrieved from EMP Commission Executive Report: http://empcommission.org/docs/empc_exec_rpt.pdf

Federal_Energy_Regulatory_Commission. (2013, May 16). *FERC Orders Development of Reliability Standards for Geomagnetic Disturbances*. Retrieved from Federal_Energy_Regulatory_Commission: http://www.ferc.gov/media/news-releases/2013/2013-2/05-16-13-E-5.asp#.V0HlwY-cF9A

G4S. (2016). *G4S_Corporate_Intelligence_and_Investigations*. Retrieved from G4S: http://www.g4sriskconsulting.com/en/What%20we%20do/Services/Strategic%20Risk%20Advisory/Corporate%20Intelligence%20and%20Investigations/

Global_Security. (2016). *Weapons of Mass Destruction*. Retrieved from Global_Security: http://www.globalsecurity.org/wmd/facility/johnston_atoll.htm

H.Cooper_and_R.Pfaltzgraff. (2010). *Countering the EMP Threat - the Role of Missile Defense*. Retrieved from The Institute for Foreign Policy Analysis: http://www.ifpa.org/pdf/IWGWhitePaper.pdf

Halper_and_Lifscher. (2014, February 10). *Attack on California Electric Grid Called 'Terrorism'*. Retrieved from Emergency Management: http://www.emergencymgmt.com/safety/Attack-Electric-Grid-Raises-Alarm-EM.html

Homeland_Security_Committee. (2015, June 25). *Critical Infrastructure Protection Act (CIPA) Passage Out of Homeland Security Committee is Decisive Step to Protect the Nation*. Retrieved from U.S. House of Representatives | Washington D.C.: https://homeland.house.gov/press/critical-infrastructure-protection-act-cipa-passage-out-homeland-security-committee/

IBM_Corporation. (1996, January). IBM experiments in soft fails in computer electronics (1 978-1 994) . *IBM Journal of Research and Development, 40* (1), 3-18. Retrieved from http://www.pld.ttu.ee/IAF0030/curtis.pdf

IBM_Journal_Research_&_Development. (2016, January). Securing the electric power infrastructure. *IBM Systems Journal of Research and Development, 60* (1). Retrieved from http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=7384571&url=http%3A%2F%2Fieeexplore.ieee.org%2Fstamp%2Fstamp.jsp%3Ftp%3D%26arnumber%3D7384571

Kansas_City_Star. (2014, february 15). *Could a Giant Sunburst Unplug Earth?* Retrieved from Kansas_City_Star: http://www.kansascity.com/news/politics-government/article339245/Could-a-giant-sunburst-unplug-Earth.html

Macdonald, A. (1978). *The Turner Diaries.* (L. Stuart, Ed.) Fort Lee, New Jersey, USA: Barricade Books.

Marie_-Helen_Maras. (2015). *Transnational Security.* Boca Raton, Florida, USA: Taylor and Francis .

McKinsey. (2016). *McKinsey_Digital_Disruption*. Retrieved from McKinsey and Company: http://www.mckinsey.com/global-themes/digital-disruption

Museum_Applied_Arts_and_Sciences. (2016). *Seeing a Stellar Cataclysm*. Retrieved from Museum of Applied Arts and Sciences: https://maas.museum/observations/2016/02/06/seeing-a-stellar-cataclysm/

NASA_Science_/_Science_News. (2014, May 2). *Carrington-class CME Narrowly Misses Earth*. Retrieved from NASA Science / Science News: http://science.nasa.gov/science-news/science-at-nasa/2014/02may_superstorm/

NASA_Science_News. (2011, September 11). *A Super Solar Floare*. Retrieved from NASA Science News: http://science.nasa.gov/science-news/science-at-nasa/2008/06may_carringtonflare/

NERC_via_F._Koza. (2016, March 1). *Prepared Statement of Frank J. Koza to the FERC Technical Conference on GMD*. Retrieved from Federal Energy Regulatory Commission: http://www.ferc.gov/CalendarFiles/20160301081536-Koza,%20PJM.pdf

Nicolaidis, _. (2011). Soft Errors in Modern Electronic Systems. (M. Nicolaidis, Ed.) *Frontiers in Electronic Testing*. Retrieved from https://books.google.com/books?hl=en&lr=&id=WCqrOkMExu8C&oi=fnd&pg=PR3&dq=france+electromagnetic+pulse&ots=E5DTxceGyQ&sig=VqwpSFiIg732XA1yQM2FykePpI0#v=onepage&q&f=false

Professor_Adam_Scott_Wandt, M. J. (2016, May 5). Class lecture, Criminal Justice 750 Public Administration 750 Security of Information and Technolog. (C. Notes, Interviewer)

PWC. (2016). *Price_Waterhouse_Coopers_LLC*. Retrieved from Price_Waterhouse_Coopers_LLC: http://www.pwc.com/gx/en/industries/technology.html

R.Pfeffer_and_D._Shaeffer. (2010). A Russian Assessment of Several USSR and US HEMP Tests. *Combating WMD Journal, United States Army Nuclear and CWMD Agency*, 33-38. Retrieved from US_Army_Nuclear_and_CWMD_Agency and Lawrence LIvermore Nat'l Labs: http://www.futurescience.com/emp/CWMD_Journal_No_3_Jan09.pdf

Risk_Mitigation_Consulting. (2016). *Risk and Security Program Support*. Retrieved from RMC_Risk_Mitigation_Consulting,Inc.: http://www.riskmitigationconsulting.com/core-capabilities/risk-security-operations

Stanford_University. (2016). *Digital Divide*. Retrieved from Stanford University: http://cs.stanford.edu/people/eroberts/cs201/projects/digital-divide/start.html

Subcommitt on Cybersecurity, I. P. (2014). EMP's Threat to Critical Infrastructure. In C. 2. Session (Ed.), *Subcommitt on Cybersecurity, Infrastructure Protection and Security Technologies. Serial N. 113-68*, pp. 1-39. Washington, DC: U.S. Government Printing Office. Retrieved from https://www.gpo.gov/fdsys/pkg/CHRG-113hhrg89763/pdf/CHRG-113hhrg89763.pdf

The_New_Testament--New_Life_Version. (1969). *The_Holy_Bible_-_The_New_Testament.* Uhrichsville: Barbour.

Tyco_Security. (2016). *Oil_and_Gas_Security_Solutions*. Retrieved from Tyco: http://www.tyco.com/markets/oil-gas

Univ_Colorado_Professor_D._Baker. (2016). *A major solar eruptive event in July 2012: Defining extreme space weather scenarios*. Retrieved from J.Wiley and Sons: http://onlinelibrary.wiley.com/doi/10.1002/swe.20097/full

V.N.Greetsai. (1998). Response of long lines to nuclear high-altitude electromagnetic pulse (HEMP). (IEEE, Ed.) *Central Institue of Physics and Technology, 40*(4).

Appendix One: Popular Culture

Frankenstein, The Final Countdown, Cast Away, Oceans 11, Star Wars, Star Trek, & BEAM ME UP

Hollywood and 'electricity' go back a long way. In fact, they go back even further than Hollywood. Mary Shelley's *Frankenstein* (1818) was the first science fiction story of a very long line involving the use of electricity. Frankenstein of course was a recreation of a human compiled from deceased human componentry animated back to life via chemicals and bioelectromagnetics / electrophysiology. (Mary Shelley probably got the idea watching dead bodies twitch when muscle contractions resulted from electrical impulses. And who knows what all went on when 18-year old Mary Shelley was ensconced with drunken and wildly promiscuous Lord Byron at Chateau de Chillon on Lac Leman (Lake Geneva), which was near summer camp at Lausanne, Switzerland long ago…) The following is just a short list…

- *The Final Countdown* occasioned USS Nimitz (CVN-68) to hit a violent lightning storm, which transported the ship back to December 6, 1941 while on patrol off Pearl Harbor, with predictable results!
- *Cast Away* saw a Federal Express cargo plane get disabled by lightning; crew member Tom Hanks survives, washing up on an uncharted little island - where he didn't live happily ever after - because he manages to escape on a raft and gets rescued by a passing containership
- *Oceans 11* is a film comedy which involves taking out the Las Vegas Bellagio's vault using an EMP device to take down the casino's electrical power and effecting a major 'heist'
- *Star Wars* uses EMP mechanisms in many manifestations as battlecruiser armaments and personal weapons to stun starships, electrocute druids, and immobilize this, that, and the other
- *Star Trek* predated Star Wars in many implementations of EMP weaponry. There were/are phasers, photon torpedoes, disruptors (and probably others too) used for the same purposes
- *Goldeneye* (where James Bond/Pierce Brosnan rampages around St. Petersburg destroying military and police Ladas and UAZ's in a T55 disguised to look like a T72 main battle tank which he has pinched, in order to chase after and liberate a pretty agent in the protective custody of a vodka-guzzling senior Soviet military big shot) has a premise of getting a secret code first, before the enemy to control ….an orbiting EMP cannon codenamed 'goldeneye'

- *The Day After* (1983) was about a full nuclear exchange between the US and the Soviet Union. (And this is entertainment?). The Soviets create an EMP blast to blind the US and it works
- And my neighbor's teenage son advises that just about every science fiction video game in his inventory has some type of EMP device with which to zap all manner of aliens, zombies, cretins and ghouls

I am sure that Lord Byron would have been fascinated by the reach and range of consequences across time and space of his dalliance with Mary Shelley!

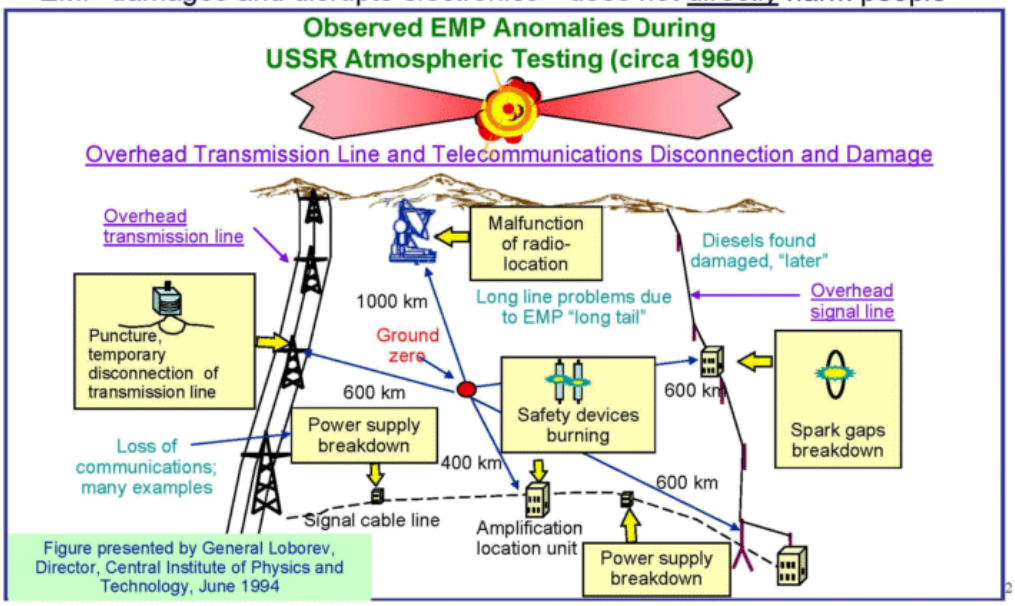
(However, one has to wonder if all the popular culture exposure in science fiction film has trivialized the clear, real and present threat of EMP damage to our way of life.)

Appendix Two Threat: Historic Evidence

EMP Commission

Threat:
Historical Evidence

- EMP observed during US and Russian atmospheric test programs
- EMP damages and disrupts electronics—does not directly harm people



Appendix Three *One Second After* …Scenario Extensions

- Rumors of cannibalism start circulating
- China embarks on a mission to colonize the US
- Mexico occupies southwestern US establishing buffer security zone against the Chinese
- Lack of antibiotics and unsanitary living kills the weak, elderly and vulnerable first and those with chronic illnesses
- Gangs and violence take their toll, and parents starve themselves to feed their children; mounting suicides
- Heavily-populated urban areas suffer 95% die-off in one-year with food-rich(er) Midwest maintaining a 50% die-off rate

Appendix Four
Charter and Abstract of the EMP Commission, 2004

Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack Volume 1: Executive Report 2004\

Public Law 106-398, Title XIV
SEC. 1402. **DUTIES OF COMMISSION**
Review of EMP Threat. The
Commission shall assess:
(1) the nature and magnitude of potential high-altitude EMP threats to the United States from all potentially hostile states or non-state actors that have or could acquire nuclear weapons and ballistic missiles enabling them to perform a high-altitude EMP attack against the United States within the next 15 years;
(2) the vulnerability of United States military and especially civilian systems to an EMP attack, giving special attention to vulnerability of the civilian infrastructure as a matter of emergency preparedness;
(3) the capability of the United States to repair and recover from damage inflicted on United States military and civilian systems by an EMP attack; and
(4) the feasibility and cost of hardening select military and civilian systems against EMP attack.

Recommendation: The Commission shall recommend any steps it believes should be taken by the United States to better protect its military and civilian systems from EMP attack. The findings and recommendations presented in this report are the independent judgments of this Commission and should not be attributed to any other people or organizations. This report presents the unanimous views of the Commissioners.

ABSTRACT
Several potential adversaries have or can acquire the capability to attack the United States with a high-altitude nuclear weapon-generated electromagnetic pulse (EMP). A determined adversary can achieve an EMP attack capability without having a high level of sophistication. EMP is one of a small number of threats that can hold our society at risk of catastrophic consequences. EMP will cover the wide geographic region within line of sight to the nuclear weapon. It has the capability to produce significant damage to critical infrastructures and thus to the very fabric of US society, as well as to the ability of the United States and Western nations to project influence and military power. The common element that can produce such an impact from EMP is primarily electronics, so pervasive in all aspects of our society and military, coupled through critical infrastructures. Our vulnerability is increasing daily as our use of and dependence on electronics continues to grow. The impact of EMP is asymmetric in relation to potential protagonists who are not as dependent on modern electronics. The current vulnerability of our critical infrastructures can both invite and reward attack if not corrected. Correction is feasible and well within the Nation's means and resources to accomplish.

APPENDIX FIVE

EMP Commission Graphics[6]

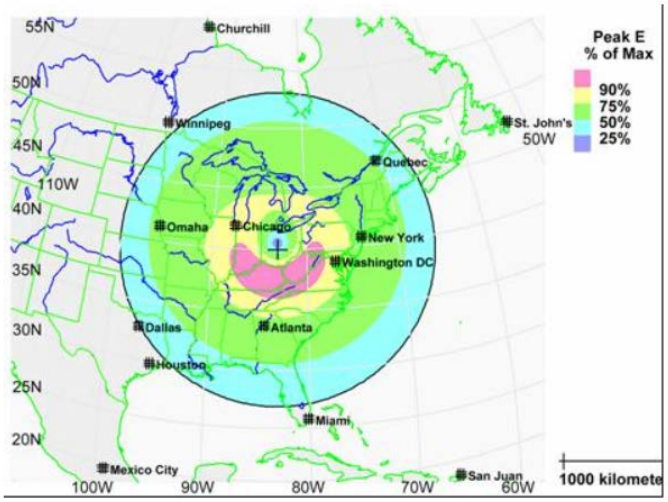


Figure 2. Illustrative EMP Effects – Fast Pulse

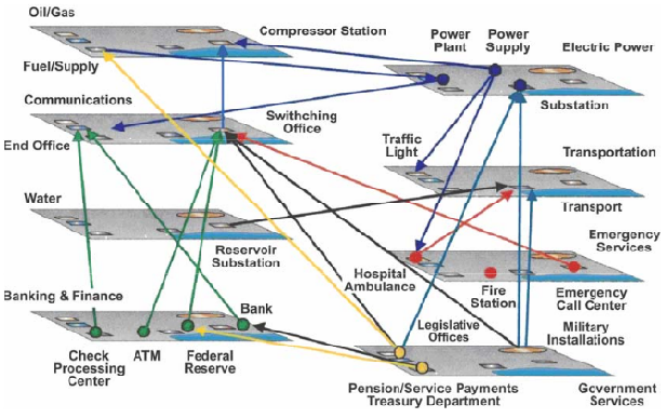


Figure 4. Interdependent Infrastructure Sectors

Most critical infrastructure system vulnerabilities can be reduced below the level that potentially invites attempts to create a national catastrophe. By protecting key

[6] http://empcommission.org/docs/empc_exec_rpt.pdf