The Electric Infrastructure Security Summit III, London

May 14 and 15

The Houses of Parliament, the United Kingdom

Transcripts of the Oral Presentations

Special Note: Only a partial selection of speakers are included in this submittal, due the limited time that was available to our editors. Care has been taken to render the transcripts as accurate as possible, but some deviations from the delivered remarks may have occurred. Please also note that all bold section titles were added by the editor, to enhance the utility of this transcript. The section headings were not delivered by the speakers, but added for the purpose of making this submittal more useful for the Commission.

The Rt. Hon. Philip Hammond MP, Secretary of State for Defence, U.K.

Keynote Speaker, Session 1, Panel 1: The Security and Defense Role of Critical Societal Infrastructures

Rt. Hon. James Arbuthnot: Ladies and gentlemen it's a great honor for me to introduce the Secretary of State for Defense, the Rt. Hon. Philip Hammond. […]

Rt. Hon. Philip Hammond: ***Introductory Remarks:***

[…] It's a great pleasure for me to be here today at this third annual EISS Summit.

[…] One of the most positive aspects of this annual event is that it brings together people from very different professional backgrounds and different skill sets and different expertise who share a common interest; working together to make sure that threats to our infrastructure, whether from natural or manmade sources are investigated, assessed, monitored, and indeed mitigated.

Scientists and security analysts, energy experts, and astronomists, public and private sector, this is a multi-disciplinary problem so it needs all of us working together across traditional boundaries, including across government departments. That's probably going to be one of the most difficult bits. And it's a global problem, so it means countries working together across international borders.

I'd like to give a particular welcome to the representatives from around the world gathered here today. I understand we have representatives from twenty countries working together to address a complex problem demanding a complex set of responses a part of all the intricate web of threats that we face, multilayered, asymmetrical, unconventional. Often requiring defense and security response that is not based on traditional methods, but cannot be met using infantry or jet planes or destroyers.

The need for investment in e-threat grid protection in the UK

Indeed one of the big challenges that we as politicians face, particularly at a time of limited resources, is going to be to make the case for spending on defense and security solutions that cannot readily be seen by the taxpaying public who are financing them; that cannot be shown off on the parade grounds; and sometimes that cannot even be talked about.

I want to talk today about progress that the U.K. government is making since the EISS summit in Washington last year. It's strengthening resilience in the face of specific threats to electrical infrastructure. As Secretary for Defense, I have a particular concern to ensure that we deter and prevent any prospect of a low-scale malicious attack and that the U.K.'s armed forces have the ability to respond to such an event.

But let me first talk about the profile of the threat because in an era of fiscal challenge, limited resources must be deployed with pinpoint accuracy. That means a deep understanding of the risks and the discipline to tailor our response rigorously and proportionately to those risks. The scatter gun is simply not an affordable weapon.

Societal Vulnerability

In the developed world, our connected high-technology societies are massively reliant on electronic networks, and becoming ever more so. In the United Kingdom electronic technology reaches into every part of government, every business, every home, and increasingly, with mobile and Wi-Fi technology, pretty much every pocket in the country.

Dependence creates vulnerability and connectivity compounds that vulnerability. Take away the technology, and our modern life-support system falters. It's not just light and heat. It's the digital computers and automated systems that help run many things we rely on from healthcare, to the transport system; from ATMs and (indiscernible) terminals, to the food distribution network.

Planning for resilience against E-threats

A sustained blackout covering a large geographical area could have crippling consequences and do serious damage to the welfare of our citizens, as well as the functioning of our economy. So the resilience in the systems that help run our society is a concern of our Domestic Civil Contingencies Organization, and assessing the risk to those systems is a matter of national security.

In the U.K. we take a holistic approach to risk assessment. By working through the National Security Council with its multi-disciplinary cross-government approach, we ensure or try to ensure that all avenues are properly explored. The latest National Risk Register for Civil Emergencies was published in January, and the update to the National Security Risk Assessment last time taken as part of the 2010 National Security Strategy will be completed later this year. So we have a robust foundation upon which our plans are laid and resource allocation decisions are made.

E-Threats – Manmade EMP and natural Severe Space Weather

For the purposes of today I want to address two risks to our electrical infrastructure that I know are of concern and which form the basis of a recent House of Commons Defense Committee report, and set out how we are acting to mitigate them.

The first is manmade and hostile. The employment of a nuclear weapon to generate high-altitude electromagnetic pulse or EMP, taking out electrical and digital systems over possibly thousands of square miles. A threat in which I, as Defense Secretary, have an obvious interest.

The second is natural and impossible to prevent, a severe electromagnetic storm caused by solar activity that has the capacity to cause significant disturbance to communication and power systems.

Let me deal first with the issue of an EMP attack using a nuclear weapon. Let me be crystal clear; an EMP attack using a nuclear weapon against or affecting the United Kingdom or our vital interests or those of our allies would be considered a nuclear attack on the U.K. The consequences for the perpetrator of a nuclear weapon being used as an EMP device would therefore be severe and any potential aggressor should be aware that we would respond proportionately against any step that launches or enables such an attack. The U.K.'s nuclear weapons are an important element of our capability so to respond.

[…]

With cyclical solar activity set to peak next year, we should prepare for the possibility of some level of disruption. The question is when and how much, not if. Low-level disruption due to solar activity of course is a fact of life. The question is how we prepare for an event of sufficient magnitude for widespread damage caused to satellite systems or electrical circuits, leading to sustained interruption of power and communications.

The need for monitoring and modeling

We need to have in place monitoring systems and predictive models that deliver sufficient warning of severe events to enable us to take preventative action. We need to have a far better understanding of the vulnerabilities (indiscernible) expected to deploy our mitigation effort. This will enable systems to be hardened only where they need to be, and for resources to be used wisely.

By focusing on the most critical systems, we can minimize the cost and maximize the effect. The U.K. has a world-class scientific base and so we are well positioned to contribute to the collaborative efforts taking place internationally. The British Antarctic Survey has a leading role in the EU Space Weather Forecasting Project (indiscernible). The British Geological Society is working with European partners to assess the threat posed by magnetic storms to power distribution networks in Europe.

The growing partnership between the U.K. Met Office and the U.S. National Oceanic and Atmospheric Administration is particularly encouraging. The memorandum of understanding signed by the Met Office and the NOAA last year has paved the way for the creation of a space weather model capable of indicating where, when, and for how long space weather effects will persist.

This summit can of course contribute greatly to the understanding of the issues we face in common and help to focus the work that is ongoing. In the U.K., government departments have been working extensively with space

weather scientists and engineers, industry, and regulators to gain the best available quantitative assessment of the risks to U.K. infrastructure.

Breadth of focus on E-Threats in the Government

This is a broad and diverse program of work. The government has worked with external experts to review the national risk assessment to make sure new and emerging risks are detected and the understanding of current risks is up-to-date. The Energy Emergency Executive Committee keeps contingency plans up-to-date, and has provided the national grid and the Department of Energy and Climate Change with a solid body of work to help analyze the impact of space weather events and build predictive models that would improve contingency plans.

Changing transformer requirements, sparing and monitoring

Super grid transformer requirements have changed as a result. Strategic reserve holdings of transformers are being increased. The national grid is working with the British Geological Survey to make sure there is robust, real-time network monitoring in place. The National Space Security Policy is due to be published later in the year, and will look all these risks in a much wider context, to make sure all parts of government are working effectively together.

Much of Britain's military equipment is designed to work in challenging electromagnetic environments. The shielding developed in this context, against interference, discovery or detection for example, can provide some protection against electromagnetic effects. Critical military infrastructure can of course operate independently of the national grid.

The MOD Science and Technology Laboratory has a great deal of expertise in working with industry, hardening and assessing electronic systems. And I want the MOD to contribute actively to the improvement of the U.K.'s civil infrastructure resilience.

Sharing MOD's EMP Standards to help Infrastructure Providers in planning protection

There is quite a lot of information on EMP protection from the government and others that is already in the public domain, for example that are published by the International Electrotechnical Commission and the MOD itself. But the MOD will now explore with others in government whether there is more that we can share with civilian infrastructure providers including, for example, sensitive elements of the defense standards on EMP.

Collectively, we have to change the way people think about defense and security. This is a challenge for us all. It is about recognizing the new dependencies and vulnerabilities that flow from the way people now live their lives. It is about recognizing solutions may require committing resources to

defense that you can't see or hear or touch, and explaining to our taxpayers that that course of action makes sense.

Protecting the high-tech networks that power our global society is part of this new way of thinking and new way of acting: predicting and monitoring, preparing and mitigating, nationally and internationally. Assessing risk and responding proportionately. I hope that this conference today is another step forward in helping us banish any lingering complacency and that we can continue to work together to ensure that the dependence on electrical infrastructure that have so enhanced our quality of life and standard of living does not become our Achilles Heel.

Thank you.

The Rt. Hon. James Arbuthnot MP, Chair, House of Commons Defence Committee, UK

Electromagnetic Threats and National Security:

Current Realities and Trends

Rt. Hon.

James Arbuthnot: ***Introduction***

Secretary of State, you've got us off to an absolutely cracking start with this conference. We are extremely grateful to you. But we do know also that you have a full day and while you've been able to demonstrate a really subtle understanding of the vulnerabilities we face and the need for more work between different government departments and between departments and governments of different countries, recognize also that you have to work on the Ministry of Defense Budget. And so we are extremely appreciative and would like to allow you to leave now.

Well ladies and gentlemen, as I say I'm James Arbuthnot, the Chairman of the Defense Select Committee and since I'm chairing the first session of this morning. […]

The Defense Select Committee decided last year to do an inquiry into a series of developing threats. Now we're into the middle of an inquiry into the solar threat that the entire world faces. Yet the very first of this series that we did was into the issue we are discussing today, the threat of electromagnetic pulses caused either by space weather or by deliberate act of man.

The recent UK Defence Committee E-Threat Report

We reported in February this year.

[…] In our first paragraph we drew attention to our increasing reliance on electronic systems which are themselves becoming increasingly delicate. And we went on to talk about our increasing vulnerability, a key word during these two days of our conference, to space weather and other electromagnetic activity. We went on to consider a range of actions we felt the U.K. Government and other governments should take to ensure more work is done on this matter.

The need for clear technical guidelines

Tomorrow I shall offer more detail to the recommendations being made about what to do about all of this, about the need for the expert community to agree on things; to agree for example exactly how serious the threat is. We need to have expert agreement on that; to agree exactly what different effects might be felt by different countries because of their different electronic infrastructure; to agree about what it would really cost to harden our electric infrastructure, whether it would be a good thing or a bad thing. We want

agreement on all of this, how to go about it, and also whether it would be the right thing to do. Just spending money is not the answer.

The Government has elevated Severe Space Weather to the no.1 Risk Category

As the Secretary of Defense has just said; we have to solve the problem or at least mitigate the risk. The government responded last month and I'm pleased to say it has placed severe space weather into the highest category at risk in the National Risk Register of Civil Emergencies.

It is time for government action – and to take responsibility ourselves to act

[…] I have a sense that all of this is somehow beginning to come together. I have the sense that we here are part of an international gathering representing the United States, roughly half of Europe, many people from India, Southeast Asia, Israel, and we are the world leadership that knows and cares about an issue which is extremely important; an issue which could be important enough to mean the difference between modern existence as we now know it, and sending the world back to a pre-industrial nightmare.

I think it's up to us. There are some countries that have yet to wake up to the threat. My hope is that we together, here in this room, will realize that it is in our hands, if it's in anybody's hands, to do something about this. And in the next day and a half let's try to get this information, let's try to begin to form these agreements within the expert community, and make the decisions that will allow our nations to begin working effectively together to fix it. Thank you very much.

Session 1, Panel 2: Electromagnetic Threat Impact and Risk to Critical Infrastructure

Rt. Hon.

James Arbuthnot: Okay now we move on to the first panel of the day. I am going to call on John Kappenman, Peter Pry, General Ashok Mehta, Bill Bryan, and Dr. Shlomo Wald to come on up please.

John Kappenman: ***Space weather can have global impact***

[…] I just want to show everybody, give some perspective of the dimensions of the problem that we're facing. Power grids are built very reliably, built to encounter normal terrestrial weather sort of threats that challenge their operation. But these sorts of threats we're talking about here truly can emerge very quickly; can have continental and even planetary wide impacts.

In the upper picture there is regions of red that are denoting areas of severe geomagnetic disturbance that occurred in a March 1989 storm, and essentially those disturbances in this case are driven by an enhanced electrojet current that is in the lower ionosphere and kind of in cartoon depicted below; these are millions of ampere sort of structures. They generate their own magnetic field. That magnetic field interacts with and disturbs the earth's magnetic field. And in a sense becomes a big [00:02:43.3] machine, in that it induces currents that begin to flow into the power grid through the multiple transformer neutral to ground connections across the power grid.

When you have these geomagnetic induced currents, or GICs flowing through transformers, that is the root cause of all the problems that begin to occur for the power system itself and ultimately for society. If you could go to the next slide please and go ahead and click that a few times.

Defining the scope of the problem

Let's talk about the dimensions at risk here. In order to talk about risk we need to talk about the threat. What we now know of geomagnetic storms is that there's been a very good reassessment over the last decade or so that now tells us more about the extremes of the environment. In the case of the experiences that we've had in the U.S. power industry, March 1989 was a particularly important storm that caused a blackout; caused transformer failure, things like that. We now know that storms four to ten times larger than that are within the realm of what has occurred before and is certain to occur again.

As far as vulnerability, if you look at today's modern power grid, they essentially span coast-to-coast. They're continental grids that internationally connect across Europe, across North America and so forth. They become a massive antenna that is ever more coupled to disturbances in the geomagnetic storm or space weather sort of effects.

They have also been designed with no rational design code that has ever checked or been in place to try to counter that growing vulnerability.

The consequences of course are loss of electric power which can be devastating to society. In fact, electricity in the U.S. constitutes more than forty percent of all energy that is consumed by society. This is more than twice as important as oil, which commands a tremendous amount of geopolitical attention in the world.

Then of course if you lose electricity, nearly every other infrastructure will either experience immediate or subsequent failure within a short period of time. Electric energy is very much like the keystone of all of the infrastructures. If you could advance it one more please.

So we get to looking at what are the risks. Certainly the risks are enormous for society. Something that could have immediate effects to our society, could literally put at risk the lives of millions. Next slide please. And go ahead and advance that a couple more times.

Severe space weather efforts expanding internationally

There's been quite a bit of effort since the last meeting that we've had within the U.S., within England, also we've started within Israel and other locations around the world, the European community and so forth, to begin to do a more rigorous, scientific, and engineering evaluation of this.

I'll touch a bit upon some of these areas, and where the discussion is going. Next slide please.

Severe space weather may be estimated from historical research, but the extremes could be even worse

Reassessing or assessing the risk of extreme threats or extreme storm scenarios; certainly we've got a lot of good data from more contemporary storms that allow us to piece together what the dimensions of that threat have been for storms that have occurred, where we've got a lot of good data. This is an example from the March 1989 storm.

You can see each of these red areas here are associated with either an eastward or westward electrojet, these ionospheric enormous current structures that drive some of the geomagnetic storm processes. If you could click it one more time. But in addition to electrojets, there's a lot of other processes that can also be equally troubling for power grids. We really don't have any good assessment on what the extremes of those other processes would be. But for electrojets let's look at this next slide please, and go ahead and click it one more time. Just looking at the eastward electrojet of the March 1989 storm, we had good, high-quality digital data there. We also had the same set of observatories available to us from the 1921 storm.

Having that dual set of data, we can do a very good approximation of what the dimensions of the 1921 storm would have looked like for the eastward electrojet. We know that the westward electrojet would have experienced a similar sort of dramatic expansion in geographic lay down as well as intensity. Next slide please.

EMP threats of course will also present a very large footprint, very troubling sort of scenario of widespread consequences to the power grids as well. Next slide.

Threat assessment details

There's been some work, obviously the work that I performed for the U.S. government depended heavily upon precise, detailed engineering analysis of the North American power grid, and others that are beginning to also do this. If you could advance it one click there.

In order to do that I'll just give you a quick run-through of the sort of details of this. A lot of factors go into how we assess the threat. Click one more slide here. What I'm showing you here, these little vector arrows are the geoelectric field intensity and orientation. Both of those aspects drive what is the nature of the coupling of the storm environment that affects the power grid, just like wind velocities would be for terrestrial weather and so forth. Next click.

There's going to be little blue balls that I'll show you there. Those indicate flow of GIC in specific transformers, the bigger the ball the bigger the GIC, the bigger the potential impacts to the power grid and the transformer. Next slide.

I'll show you some little red boxes here. These indicate actual recorded events from the March 1989 storm that were significant, you know, things tripping off line, other reports of serious voltage loss and so forth. So let's go ahead and look at how rapidly a storm event could happen. You know, we think that terrestrial weather changes rapidly; well, space weather poses a whole new paradigm for how rapidly things can evolved.

The Quebec 1989 Blackout

You can see here, within just four minutes we went from very quiet conditions to an intense geomagnetic field disturbance that essentially lays down across the entire U.S./Canada border. We can see transits of disturbances that are traveling at the speed of about 1,000 kilometers per minute sort of rates of speed, unheard of for terrestrial weather. It was actually during this four minutes that the Quebec grid collapse occurred. If we go to the next slide.

I'll walk you through just those four minutes, looking at the Quebec grid and the U.S. grid in detail. Next slide please. This is showing you one minute later. You're noticing contingencies already beginning to happen on the power grid there. Next slide. And at this point, in particular in the Quebec region, they're already at an N-7 condition. The grid itself is only designed to allow for N-1 sort of contingencies and maintaining its viability. Next click there.

We're already entering into a complete province-wide blackout at this point. The grid itself is beginning to fall apart and by the next slide, you'll see that we've gone into complete power grid collapse. All of this occurring arguably much faster than allows for meaningful human intervention let alone assessment of what's about to occur. If we could go to the next slide.

We'll look at a substorm a little bit later this [00:11:49.3]. It was actually during one minute of this particular substorm that a large transformer at a nuclear plant in New Jersey was damaged. If you could click a couple of times, we'll show you here again about four or five minutes of rapid evolution. Go ahead and click it one more time please. One more.

And finally at the end of this particular substorm, notice all the red boxes there. These are all significant operating anomalies, contingencies, things like that, that were reported across the North American continent during that particular -- during just this particular substorm that occurred. If you click it one more time.

You can see we came uncomfortably close to a blackout that literally could have extended along these dimensions here. And obviously this sort of experience alone tells us a lot about what could conceivably happen for a storm that could measure four to ten-times larger than this particular storm. If you go ahead and click it one more time.

Obviously you know, models like this are important. They describe for us in an engineering sense what the details are, but realistically just having access to data, measurements, reports of failures, things like this, we can also do very reasonable extrapolations just from that alone that confirm the validity of models, but also confirm for us the potential for large impact that could occur from these type of events. Next slide please. And go ahead and click it.

Equipment damage of course is one of the key areas of discussion. And there is certainly a lot of divergence on that topic area. There's other equipment besides transformers that we need to be concerned about: large generators, circuit breakers. We know even less or understand even less about those damage issues.

How bad could a GMD be: Considering the "unknown unknowns"

Certainly a GIC or EMP impact has a unique ability to cause damage unlike sources of other power grid blackouts. When we have widespread catastrophic damage to the infrastructure itself, the power-grid infrastructure, then we get concerned about what is going to be the prospects and length of restoration from that sort of event. If you could click it one more time.

I also have concerns that every major storm that we've had we've learned new things about failures that could that we didn't know could occur in storms. I think there are still a number of important unknown unknowns that are out there. These unknown unknowns are also increasing with time, as we go to more sophisticated applications. Datacenters I know are an immediate concern that would come to mind that we have to be mindful of. Datacenters are also an important part of this data system that embedded in the utility infrastructure as well. Last slide, or next slide here.

This is just showing you what we considered to be from these models the location of the important transformers that are at risk. And if you advance it one more time, you'll see that clearly there is impacts across the bulk of the U.S. here from this one particular scenario. And in some of these regions, especially major population areas, we can see impacts that measure more than fifty percent of the existing infrastructure in those regions.

It does bring forward concerns about what would be the recovery prospects from such a scenario. Next slide please.

So what are the things that we should take away from this in conclusion here? Well, arguably we have been through a several decade-long failure to understand how this risk has been migrating into the electric power infrastructure from space weather and related EMP threats.

We certainly know that the sun, the magnetosphere remain fully capable of producing large geomagnetic storms again in the future. They have occurred before. They will occur again.

We know that the power grids have expanded to greatly and unknowingly increase the vulnerability to these same threat dimensions.

We also know that nuclear proliferation is a reality and that some of these tools we are finding to be in the hands of bad actors as well.

We are looking at something here that is an unrecognized systemic risk. We have not ever had a design code that took this risk or threat environment into consideration.

Given sufficient time, the reoccurence of a large storm is certain, only with much more serious consequences for society. And one more click there.

In regards to EMP, the threat consequences will be even larger because it affects larger systems.

Thank you.

Session 1, Panel 2, continued:

Dr. Pry began with a joint statement, authored by himself and Dr. William R. Graham. The statement follows:

ELECTROMAGNETIC PULSE (EMP):

THREATS AND PREPAREDNESS

JOINT STATEMENT

DR. WILLIAM R. GRAHAM AND DR. PETER VINCENT PRY

ELECTRIC INFRASTRUCTURE SECURITY SUMMIT

UNITED KINGDOM PARLIAMENT

WESTMINSTER PALACE

London, England

May 14, 2012

This summarizes key findings of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack, established by the U.S. Congress 2001-2008, and of other subsequent studies. The Executive Summary of the EMP Commission Report is appended.[1]

An electromagnetic pulse is a super-energetic radio wave that can destroy electronics. An EMP can be generated by a nuclear weapon, naturally by a geomagnetic storm, and by non-nuclear radiofrequency weapons.

A nuclear weapon detonated at high altitude (HOB 40 kilometers or more) will generate an EMP that will propagate from the point of detonation to the line of sight on the horizon, covering a vast region with a potentially destructive EMP field. A single nuclear weapon detonated at an altitude of 400 kilometers above the geographic center of the U.S. would cover the entire contiguous United States with an EMP. U.S. critical infrastructures are presently unprotected from EMP. All critical infrastructures depend directly or indirectly upon electronics and electricity, especially upon the electric power grid, that is especially vulnerable to EMP. Thus, a nuclear EMP attack could collapse

[1] See also the more in depth 2008 report by the EMP Commission, *Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack: Critical National Infrastructures* (Washington, D.C.: 2008).

all the critical infrastructures--electric power, communications, transportation, banking and finance, food and water--that sustain modern economies and the lives of millions.

Any nuclear weapon, even a crude first-generation nuclear weapon of low-yield, could inflict a catastrophic EMP attack, according to the EMP Commission. The EMP Commission also found that Russia and China have probably developed what the Russians term "Super-EMP" nuclear weapons--nuclear weapons designed specifically to generate extraordinarily powerful EMP fields. Credible Russian sources told the EMP Commission in 2004 that technology for Super-EMP nuclear weapons has leaked to North Korea, enabling that nation to develop such weapons "within a few years."

Nor is it necessary to have a sophisticated long-range missile to make a nuclear EMP attack. A short-range missile, like a Scud, launched off a freighter would suffice to deliver a nuclear warhead to high-altitude for an EMP attack. Iran has conducted such a launch mode, has detonated missiles at high-altitude, and openly writes about destroying the United States and "the West" with an EMP attack.

Solar flares and coronal mass ejections from the Sun can generate geomagnetic storms on Earth with effects similar to the EMP from a nuclear weapon. In 1989, a geomagnetic storm temporarily blacked out Quebec and parts of the United States, causing costly damage to some extremely high voltage (EHV) transformers. EHV transformers require long lead times to replace and are indispensable to the operation of the electric grid. A 1921 geomagnetic storm, that occurred before most of the U.S. was electrified, if it happened today, according to a study by the National Academy of Sciences, would destroy some 350 EHV transformers and cause a protracted blackout of the United States, requiring 4-10 years for recovery.[2]

The EMP Commission warned that every century or so there occurs a "great" geomagnetic storm, like the Carrington Event of 1859, that caused fires in telegraph stations, forest fires, and destroyed the newly laid transatlantic cable. The Carrington Event posed no threat to civilization because mankind was not yet dependent upon electricity for survival. But if the Carrington Event happened today, power grids and the critical infrastructures that sustain modern societies would probably collapse worldwide.

Many scientists believe that we are overdue for another great geomagnetic storm like the Carrington Event. Many are concerned that there is a heightened prospect for such a catastrophic natural EMP event during the solar maximum, when the Sun emits more solar flares and coronal mass ejections. The solar maximum recurs every 11 years, next in December 2012 through 2013.

[2] National Academy of Sciences, *Severe Space Weather Events--Understanding Societal and Economic Impacts* (Washington, D.C.: National Academies Press, 2008).

Non-nuclear EMP weapons, like radiofrequency weapons, can damage and destroy electronics locally. Such weapons have short ranges, kilometers for some military systems to meters for devices improvised by terrorists or criminals. Industrial EMP simulators, intended to test commercial systems for hardness against interference from stray electronic and radio emissions, are on the open market and can be purchased by anyone. At least one such EMP simulator is designed to look like a suitcase, can be operated by an individual, and is powerful enough to damage or destroy the electronic controls that regulate the operation of transformers and other components of the power grid. Armed with such a device, and with some knowledge about the electric grid, a terrorist or lunatic could blackout a city.

The EMP Commission concluded that it is necessary and affordable to protect the electric grid and other critical infrastructures from nuclear, natural, and non-nuclear EMP threats. Technology and techniques for EMP protection are well understood, having been developed and employed by the U.S. Department of Defense for military forces for over 50 years. The EMP Commission made numerous cost-effective recommendations for protecting all the civilian critical infrastructures from EMP. The Commission recommendations are based on an "all hazards" strategy that would protect not only against EMP, but mitigate the full spectrum of possible threats--including cyber attack, sabotage, and natural disasters.

In September 2010, an excellent interagency study sponsored by the U.S. Federal Energy Regulatory Commission, that included participation by the Department of Defense, the Department of Homeland Security, and the White House, independently reassessed the EMP threat--and arrived at the same conclusions as the EMP Commission. The FERC estimates that protecting the national electric grid from EMP would entail raising electric rates for a period of three years, at a cost to the average rate payer of 20 cents annually.[3]

Dr. William R. Graham was Chairman of the EMP Commission established by the U.S. Congress and served as White House Science Advisor to President Ronald Reagan and Acting Administrator of NASA. Dr. Peter Vincent Pry served on the staffs of the EMP Commission, the Congressional Strategic

[3] Federal Electric Regulatory Commission (FERC) Interagency Report, *Electromagnetic Pulse: Effects on the U.S. Power Grid*, Executive Summary (2010); FERC Interagency Report by John Kappenman, *Geomagnetic Storms and their Impacts on the U.S. Power Grid* (Meta-R-319) Metatech Corporation (January 2010); FERC Interagency Report by Edward Savage, James Gilbert and William Radasky, *The Early-Time (E1) High-Altitude Electromagnetic Pulse (HEMP) and Its Impact on the U.S. Power Grid* (Meta-R-321) Metatech Corporation (January 2010); FERC Interagency Report by John Kappenman, *Low-Frequency Protection Concepts for the Electric Power Grid: Geomagnetically Induced Current (GIC) and E3 HEMP* (Meta-R-321) Metatech Corporation (January 2010); FERC Interagency Report by William Radasky and Edward Savage, *High-Frequency Protection Concepts for the Electric Power Grid* (Meta-R-324) Metatech Corporation (January 2010).

Posture Commission, the House Armed Services Committee, the CIA, and is currently Executive Director of the Task Force on National and Home land Security..

Panel 2: Electromagnetic Threat Impact and Risk to Critical Infrastructure

Dr. Shlomo Wald: ***Introduction***

[…] My name is Shlomo Wald. I am Chief Scientist of the Ministry of Energy and Water Resources in Israel for the last three years. I am a physicist and I work a lot in many things that relate to hydrodynamics and instabilities.

A call for action on EMP: Begin work on mitigation

[…]Basically I would like to see this conference deal with the effects, to deal with the effects and to deal with how to mitigate them. This is the third conference in Electrical Infrastructure Security but we [are] still dealing with politics and the need to mitigate and to deal with this EMP threat.

This is a very grave situation. And so we have various accomplished politicians, secretaries of state, founding members, and other people talking about the need to be prepared and to mitigate this threat. However until now, no one has defined the EMP as a reference threat. Where I'm talking about reference threat, I can give you an example of other things I am responsible for in Israel.

The international community has not yet focused on EMP protection

I am responsible for the Ministry of Earth and Marine Science and we are very tightly connected with all the world and Europe, in order to be prepared against the tsunami effect. And for a tsunami you have many facilities, early warning facilities and other things, and people are training for what happens if a tsunami earthquake or something like that would happen; everyone knows what to do. It is easy to do, and early warning has some effect in the case of a tsunami, [it has] a major effect.

Advanced preparation is crucial, and can prevent an EMP attack

But this is not the case for EMP. We know very well the threat of EMP. We know very well it can be really devastating. I heard this morning that people are talking about early warning against electromagnetic storms or something like that, but if you are not well prepared in advance against EMP, nothing will be -- it will help nothing, early warning.

The point is, if we should consider EMP as a reference threat, then we should be prepared, and develop all the technologies needed for it, and if there is still a lack of technologies to mitigate all the threats of EMP, we shall not be prepared.

And if we shall be prepared, it will be hard for other people trying to attack with EMP threats. So this is a need. This is something which is basic -- it should be put on the table in a very clear way.

Given global instabilities, an EMP strike is a high-probability event

People say that there is a low probability for a malicious EMP attack or nuclear attack. I don't think so. I say it as a physicist. I work a lot on instabilities and our world and our society is based on instabilities. We have our economies laying above a stormy, hot, and very dangerous background underneath, and this is [like] a physical phenomenon: instability prevails and you get some eruptions, we shall get some insanity. The world has lots of experience with insanity erupting, and it is just a question of time, and not too long a time.

To be prepared, I don't believe the calculation of probability. And even if the probability is low, the amount of damage is so huge, [since] we have to count the product of the probability with the amount of damage (which is so high), we can't ignore it.

Our focus must start with the power grid, but go beyond it

[…] I'm not talking just of preparation, for example, of the electric grid which is also my responsibility in Israel. I was very pleased to hear Bill describe the test that they did in Florida, the exercise you did in Florida, and the very serious concern that you dealing with on basic transformers, and to build them from the beginning resilient against an electromagnetic storm

But this is just part of the game. If you don't think in a holistic way on all the subsytems, then nothing will prevail, even if your transformers survive, because the electric grid depends very strongly on communication nowadays. If the communication collapses, the grid itself will fall even though all the transformers survive the attack.

Our military systems – and our deterrent – will be both ineffective and pointless without protection of critical societal infrastructure

[…] DoD spent billions of dollars in order to protect all the military systems. But if you know nowadays the military system is extremely closely connected to the civilian facilities. So if the civilian infrastructure will collapse, there will be no need for striking against someone […], the game will be over before it starts. I am telling you that we shall never be able to put the blame on someone in the case of EMP, and we have to take care to invest a lot in order to be defended against this threat.

Proposing an International Roadmap for EMP protection

Since it is so long-term, the effort to be done. and so large [an] investment […] to prepare the technical capabilities and the logistics and monetary needs for these things, we have to make a roadmap for a holistic way to control the system and subsystems, make priorities and make a roadmap for how to defend ourselves. […] We have to start somewhere, and to start in a logical and well-controlled way.

The last point is that a single country will never be able to do it properly. The challenges are so great and so severe, it will take an international effort in order to go somewhere and to achieve something.

Because of that, I think this is the main purpose of such meetings, when people from different countries share the feeling that our culture is in danger and we have to take care of it the same way that we take care of an endangered species. We are an endangered species.

We have to take care and to make an international effort in order to build a roadmap and plan how to protect our civilization against the inevitable event of EMP. It will happen sometime, unfortunately.

Israel invites international participation in a series of high-level EMP protection workshops, to be hosted in Israel

Because of that, what I propose is to convince people in this community to build a program. I invite whoever wants to be here, and I volunteer Israel to host a workshop or series of workshops of countries that share with us the fear and the need for doing something against the EMP threat.

It will be holistic in judgment, it will look at all the infrastructure involved, make priorities with the group, set work programs, set targets for technological development, and put it on a timescale and allocate budget.

Israel will be happy to host such a workshop – soon, I hope. I am looking forward to participation from as many concerned countries as possible. Thank you very much.

Session 2 Keynote: Managing the Risk of e-Threats: U.S. Policy Perspectives

Hon. Cheryl LaFleur: Thank you so much, I really appreciate the opportunity to be here with such a distinguished audience of delegates and I'm honored to be part of the U.S. delegation for the third time. Secretary Hammond spoke this morning about the fact that when he first took his position he was accosted on this issue very early, and I had a very similar experience. It was fortunate for me that the first Electrical Infrastructure Security Summit was just a couple months after I became a FERC commissioner that I attended on that occasion, and have become quite involved in the issues.

I know FERC is not exactly a household name all around the world. We are generally made up of five commissioners. We have four right now, each independently appointed by the president. We are expressly bipartisan in composition and operation.

FERC is the regulator of the United States that receives wholesale and [00:00:55.2] transmission of electricity. We have other responsibilities related to natural gas pipelines and storage, liquified natural gas, and the licensing of hydroelectric facilities.

Most pertinent to today's conversation, since the Energy Policy Act of 2005, we've been charged with overseeing the reliability of the bulk electric system through the development and enforcement of mandatory standards. I know that Representative Franks and his colleagues are working to give FERC new legislative authority over some of the e-threats we're talking about today, and we will obviously carry out any new authority we're given very diligently. In the meantime we're working as hard as we can to address e-threats within our existing jurisdiction.

With me today is Mr. McClelland, who is the Director of the Office of Electric Reliability for FERC. He's a senior staff member who leads all our reliability work and including technical analysis of this issue. And also in the front row we have Gerry Cauley who is the Chief Executive Officer of the North American Electric Reliability Corporation, which is an organization of the Electric Reliability Organization that works with and under FERC to work with industry to develop the electric liability standards in the United States, Canada, and part of Mexico. NERC sends its standards to us for approval and we work closely together to enforce them. So we share responsibility for identifying and responding to emerging reliability issues, such as these.

I'm also pleased that Avi included in the invitation list for this conference, and are here with us several representatives of the U.S. industry and state government in the United States, which bear important responsibility in this area, and I appreciate all of you making the trip over with us.

My comments today reflect my own views. I don't speak for the commission as a whole.

At the closing of the last summit in Washington in April 2010, I got up and suggested that everyone should begin today by talking about what we've accomplished on this topic in the past year. So I guess it's incumbent on me to do that myself.

In the past year FERC and NERC have focused on assessing the threats related to geomagnetic disturbances caused by solar storms, and beginning to take action to prevent of mitigate those threats. I believe the response to GMD is squarely within our responsibilities and have made it a personal priority.

It also fits within other efforts we're undertaking to develop standards for the electric grid and prepare for other emerging threats, particularly cyber security. This morning I want to report on what I think are two significant events since our last conference, and then talk about action steps from here.

In February 2010, NERC, Gerry's organization released a report, a "Special Reliability Assessment on the Effects of the Geomagnetic Disturbances on the Bulk Power System." It is part of a larger effort that NERC is undertaking to prepare for high-impact low-frequency threats to the electric grid, and strengthen the resilience of the grid in North America.

The report is significant because it considered input form a wide group of participants across the U.S. and Canada, with observers from government and NGOs, transformer manufacturers, and academia. Gerry probably won't say this when he speaks tomorrow, but I'm not embarrassed to admit that I really pressured NERC to make the GMD taskforce a priority and get the report out. My husband would say I'm an excellent nag. It's one of my core competencies to nag about things.

Besides the value of just having the taskforce and doing the report, Joe McClelland and I have been working to increase the visibility of this issue with the United States. I started putting it in all my speeches when I'm allowed, to educate people who know nothing about the issue, and NERC's work is giving me a lot of visibility.

The NERC report has not been without controversy. It differs from some prior reports about the mechanisms through which geomagnetic disturbances would impact the bulk electric system. While all the studies are in general agreement that the major risks to the power system are asset damage primarily involving high voltage transformers, and power system collapse resulting from inadequate reactor power, what differs in the NERC report is the degree of risk that's associated with each of those threats.

The NERC report concludes that the most likely worst case system impact from a severe GMD in North America is voltage disability caused by inadequate reactor power support. This instability will likely lead to system collapse. The report does conclude that a subset of high-voltage transformers, particularly older transformers at the end of their operational life, and those that have high water content and high dissolved gases would experience damage from geomagnetic current.

It is above my pay grade and above my technical abilities to determine standing here whether reactor power would break up the grid first, as the NERC report concludes, or whether the reduced currents would cause widespread transformer damage as Oak Ridge and several other studies conclude. I represent the [00:06:24.3] result and can't allow it to happen.

I do believe we need to have more monitoring, modeling, and study to continue to answer those technical questions. But I'm much more interested in focusing on where the NERC report and the other reports agree, and in large measure they do agree, and that gives us a significant basis to take forward action, which leads me to the second development.

On April 30, FERC hosted a technical conference to discuss geomagnetic disturbances, and I see Avi's group has already published a brochure on it, you can pick up at the desk. You don't have to sit there all day, you can just read the brochure.

I'm pretty positive this was the first time FERC had ever done that. It had about 200 people in person and was broadcast on the web and covered by the press as well. Again, it was part of getting more visibility to the issue.

On that date we heard testimony from experts from NERC, industry, government, and academia including many of those who are here today. We are fortunate to have Mr. Michael Cousins from the U.S. Department of Energy and Climate Change to discuss some of the steps they are taking here to address these issues. I know we can learn a lot from our colleagues in the U.K. Canada, and elsewhere.

At the technical conference the first part was devoted to what is the assessment of risk. Some of the issues I spoke about a moment ago, and what methodology would GMD damage the grid. The second part of the conference was on what should we do moving forward. What actions FERC, NERC, the industry can take to prevent [00:08:05.1] these threats.

The panelists all agreed on several things:

1) more monitoring and modeling of GMD would be very beneficial;

2) that we would benefit from improvements in space weather forecasting and communication of forecasts, something we're going to hear about a little later today;

3) there can be considerable differences in GMD exposure and impacts depending on geography, where you are in the earth, ground conditions, grid configuration, and equipment condition but that we should not assume that any area or system is safe without further study;

4) there are prudent steps that can be taken now to prepare the grid for e-threat disturbances, although the panelists did not fully agree on what those steps were, but they all agreed that either outcome, either grid collapse or widespread transformer losses are unacceptable and that plans have to be put in place to address it; finally, everyone agreed that any mitigation plans or action could not be done in isolation by individual entities because potentially an action that one person took to retrofit their part of the grid could just drive the current to somebody else, but rather there had to be coordinated action and cross-energy connection.

This is part of an ongoing docket at FERC and we are taking comments from the public and anyone on this topic until May 21, and then we'll review our record and all the testimony and comments received, and work on next steps. Next steps could take different forms. They might included coordinated voluntary action, work by FERC to develop standards, or an order from FERC requiring the development of standards, or some combination of those.

I know I said at the start my standard warning that these are my own comments and I don't speak for anyone else, but I want to repeat it here because now what I'm about to express is definitely my own view, based only on my current understanding and reading. Any action that FERC took as a commission would be based on a decision of my colleagues and I as a whole, based on a record that's not yet complete.

Having said that; based on all my study of this issue today and all the experts I've talked to, I believe there's a set of no-regret steps that grid operators can and should take now to understand and address GMD threats. While continuing further study, I don't think we need to wait for more studies to begin these actions. I believe they include the following:

- **First,** increase monitoring and modeling of geomagnetic currents. While recognizing the value of prior work that's been done, I appreciate that NERC recently released open-sort software to industry to increase the ability to do that monitoring.

- Second, I believe we should undertake an assessment now of the equipment on the high-voltage electric grid most vulnerable to GMD disturbances and most critical. Based on this assessment,

transmission owners and operators would be able to develop appropriate action steps. As with any written program to address something that's on the electric grid, and I've lived through quite a few of them, the appropriate action steps will likely vary based on how critical an asset was, where it was located, when it was schedule to be replaced if it's near end-of-life, whether it could be protected by islanding or operating protocols, or whether it needed to be retrofitted in some way with protective equipment. Our understanding of all those options is really still in its infancy and will likely grow as we begin to apply them in practice.

- Third, I believe we should work ideally on an international basis to develop standards for new transformers and work with manufacturers of new technologies that can be built into new transformers to ensure that to the best of our technical understanding and ability, the next generation of equipment is built to withstand these disturbances.

- Fourth, continue to develop emergency plans, just like emergency plans someone spoke of for tsunami, emergency plans for e-threats, and undertake appropriate testing and training as for all emergency plans. It's true that we don't necessarily have warnings of nuclear attacks, but we do have at least some warning usually of solar disturbances and the emergency plan would have to be sharply developed and tested in advance. It couldn't be something made up in fifteen minutes obviously.

- Finally, continue efforts to inventory and share spare transformers and other equipment. This is something the U.S. industry has made great strides on, the Department of Energy has been helping, and it's not a full solution but something that should be part of a coordinated solution.

As I said, these are my thoughts at this time. They will evolve going forward as we look at what everyone has to say on this issue. I want to offer a few closing thoughts.

I know the challenge today we're discussing is complicated, scary, almost too scary to figure out what the first action step is sometimes, and not fully understood. Complicated challenges require complicated solutions, solutions that you start one way and then see how it's going, and evolve. They don't have simple solutions, and I think anyone who thinks there is a silver bullet we can use would be wrong.

During my career I've been involved in may large-scale efforts to refurbish or replace electrical equipment on the grid to improve reliability, to improve safety, and to improve environmental performance. Generally because of the

size, diversity, and continuous 24/7 operation of the electric grid, these efforts are more complicated than you first thought and they take longer than you first thought. So which way does that cut? To me that argues for getting started sooner and figure out how this really works in practice rather than waiting until we have figured everything out. It's always a little more complicated than you think when you're [00:14:41.6] the grid. It's a complex beast

Second, in the United States, as in many other places around the globe, we are in the midst of considerable investment in our transmission grid, driven by a very radical change in power supply due to greater reliance on natural gas, due to new environmental standards, and due to requirements to pursue renewables. It's also driven by replacing aging infrastructure and by greater regional coordination and planning.

The Edison Electric Institute, which is the industry trade group in the United States, has estimated that between 2010 and 2030 the United States could invest as much as 300 million dollars in electric transmission. That means we have a big opportunity now, before we put in the next generation, to work to the best of our ability to make sure that it's built to withstand geomagnetic disturbances, to the best of our ability other e-threats and cyber threats while we're putting it in now rather than me sitting here in 2030 -- it won't be me, but somebody standing here in 2030 trying [00:15:51.0] cost to retrofit what we install in 2014.

Finally, I want to take note of the fact that the problems we're talking about today are by their very nature ones that implicate countries around the globe. It's a planetary challenge. So therefore they benefit from international cooperation. I wish we had the resources to work individually with every country in the globe but we're not an international agency. We're just a domestic agency that does a bit of international outreach, so I am thrilled that Avi and Chris have pulled together organizations like this where we can meet together with folks and one-stop-shopping learn from each other. I think meetings like this are very important.

Tomorrow I'll be signing a memorandum of understanding with our U.K. colleagues at the Department of Energy and Climate Change to work further on this. Thank you Avi for hosting this, and I look forward to working with you all further. I did make you late for lunch, thank you.

Lord Toby Harris: Thank you very much indeed for that overview of U.S. policy and also its very important glimpse, going forward. I was thinking that some of the points that you made in terms of issues which are obviously U.S. energy policy are not dissimilar from some of the ones we have to face in many of the other countries represented here.

We've got eight to ten minutes before lunch. I'm confident there's been more than three hours where there's been no audience participation. I'm very ready to take any comments or questions or points you want to make in the next few minutes before those doors open up over there and your lunch will be available. Anyone want to comment? Perhaps you could indicate who you are and where you're from. I think there are people bringing microphones as we speak.

Audience: Thank you. My name is Harry Dhaul, and I come from India and represent the Independent Bio-Producers Association. I must endorse what [Commissioner LaFleur] has said because we've done some amazing work with FERC throughout 2010 and 2011. My question to you was what can developing countries do today to improve or fortify their systems? I just want a clarification of what you think is something they can do in terms of improving technology in transformer systems and making them more resilient?

Hon. Cheryl LaFleur: I think by the very term of developing countries, generally implies that a lot of infrastructure is being built now so I would think an important priority would be to work with the manufacturers who are probably the same ones we use everywhere, to try to leapfrog -- if you're putting in something new now you must leapfrog over the decades of older equipment that we've put in, and get what's the best out there now as you're developing and putting it in.

With respect to what you already have, I think organizations like this and others, rather than having to do everything yourself, study this and study that, you can let somebody else figure it out. But I would think focusing on what's going in now, there are vendors in the room who are working with some ABB and some of the manufacturers and we need to collectively pressure the manufacturers to put in what we need in the next generation.

I don't have these figures on the top of my head, but if you read that new book that just came out, *The Quest*, which is about the future of energy, if you look at the transformers in the world a lot more are going in, in China and India and other parts of the world than are going in, in the United States right now collectively. So that's where the next generation of transformers should be designed.

Lord Toby Harris: Any other questions?

Hon. Cheryl LaFleur: That can be for anyone else too.

Audience: I'm Joel Mowbray from the U.S. In America as you know we have the problem where we talk about problems ad nauseam, to continue talking about solving problems we know how to solve and oftentimes spend more time and money to have a commission go through to say whether or not we should solve the problem we know how to solve than it would have actually taken to

fix the problem. It seems to me that maybe we have that problem now with this and how do we get around that in this current climate?

Hon. Cheryl LaFleur: I'm afraid you're probably right in your general characterization and sometimes that is caused by lack of clarity as to who has the authority to order a solution and lack of clarity about who's going to pay for it. That could lead to the benefit of job owning rather action.

I think that I'm trying to make a contribution by outlining action steps I think we should take and groups like FERC and NERC can work with industry to try to get started on those steps now. That's why I've been very prone to action. As I said, some of the congressional proposals would jumpstart timing of solutions but that is not an excuse to wait for new legislation. I think we have things we can do with our existing authority that FERC and NERC can start on now. I accept your general criticism that there's just a tendency and particularly with things that are large and unwieldy as this problem is, to want to make sure you know everything before you take any action. I don't think we can.

Tom Bolt Director, Performance Management, Lloyd's, UK

Session 2, Panel 1: ***Impact of Energy Policy on Societal Risk, Resilience, and Security***

Tom Bolt: ***Introduction – Why do we care? "People don't do much about what they don't easily remember."***

[…] Let me take this opportunity and concerns to address the issue of solar weather or solar storms quite, quite seriously, only that's the American version of quite -- you all use quite in a different way here, but it's very serious for us. Why do we care?

The Japanese quake last year in Sendai happened 880 years ago but there was not really a whole lot of economic value at the time, there are not a great deal of records about what happened other than we know there was a similar tsunami and a similar quake.

In Thailand the flooding they had this fall which we think probably cost closer to twenty million dollars than fifteen of insured value; the economic damage was probably thirty-six to forty million. That happened in a flood that happened seventy-seven years ago. People don't do much about what they don't easily remember, so one of the things to remember about this issue about how important it is, is the fact that people pattern off what they've most recently seen. They don't pattern off of stuff from two generations ago or fifty generations ago.

There are abundant examples of catastrophic losses from low frequency disasters

I would assume many of you in the audience didn't know that sixty percent of the world's hard drives were produced in the industrial parks just north of Bangkok. Many of you probably didn't know that of the seven largest industrial parks, which in the U.S. we assume is a few office buildings, was the size of Birmingham, England, as one office park. Many people didn't know that Honda had its big car assembly plant, they moved a lot of production to after the Sendai quake, are right next to a Sony plant. They both are underwater.

Playing the odds with solar weather – "most people buy earthquake insurance after the earthquake happens."

The point is when you think about solar weather, you might say what are the odds; how often will it happen in one area, 1-in-50, 1-in-250 but you have to think about the dramatic change in economic value at risk, and if you do the math and take a low probability, it's a very expensive event. You have to ask yourself would a certain amount of mitigation make an enormous amount of sense. It's very hard to mobilize mitigation -- most people go buy the insurance for earthquake in houses in California after the earthquake happens.

The serious costs from a space weather event would be the contingent business interruption costs

The important thing to know about earthquake coverage – and this is another very important thing about what we're talking about today – we don't cover earthquake except as an express policy or express condition of the policy that we cover the earthquake. What we do end up covering because of legislative initiatives is fire following. You may say how much does the insurance industry have exposed in what we call power generation facilities. That's a reasonable amount to the plants, equipment, and to repair that, and there will be business interruption policies. But what most people don't think about is the notion of contingent business interruption. Because there's no power to the Sony plant, because there's no power to the Honda factory, those guys can't sell cars and those guys can't sell electronics.

And there is a contingent business interruption policy that those people buy, both in the U.S. and abroad that are very much at risk for this. That will be the equivalent of the fire following the earthquake.

Insurance companies are very exposed to space weather costs

We may not cover the electromagnetic pulse but we will pay in a very large way for it. Plus my general attitude living on this side of the pond for eighteen years, is in the U.S. the legal system occasionally decides if bad things happen you will pay. They may not decide whether the contract matters or not. You will pay, if it's a big enough societal problem somehow insurance, being a soft form of taxation, is an easier way to handle the world's problems. So a person can be flippant oftentimes, but I've got some checks to prove that it's right, in terms of what I said about that.

"We think there is plenty of science that backs why we should be worried," and "we think [mitigation] is very prudent."

So if we think solar activity is due to enter its next peak cycle between 2013 and 2014, the piece of work that we published a year ago says actually 2015; we think there is a peak cycle. Whether it will happen this year, there's other people that talk about the eleven-year solar cycles and the rest, people who talk about the Mayan calendar and planning from the guru and all that stuff, (we don't really spend too much time on the guru) [*laughter – ed*.] but we do worry a lot about solar weather. We think there is plenty of science that backs why we should be worried about it. And even if it doesn't happen right now, if there's a reasonably cost-effective way to mitigate some of that loss, we think it's very prudent for society to figure out a way to make that make sense.

Insurance companies are prepared to get involved

One of the ways that can make sense, as I said before, is low probability but enormous cost still means that there's some money that ought to be available to try to mitigate the impact. Because, even if you ask us insurers to pay for it, we'll pay for it, but all I am is a warehouse of other peoples' money. And I

hope to keep a nickel as a non-life insurer. Lloyd's for example writes a little over, between one and one and a half percent of the world's entire non-life insurance premium, right now about twenty-five billion pounds of insurance. We do business in over 200 countries, we write sixty-three different kinds of risk. We're very involved and we have skin in this particular game.

"We should do everything in our power to help incentivize you."

And we care quite deeply that when you get an opportunity to do a sensible initiative to try to mitigate the loss that we should do everything in our power to help incentivize you. Even if we pay for it post loss, everybody is going to share that cost, prices will go up, and it won't be pretty, especially if the cost of repairing the loss is far, far greater than the cost of mitigating. I'd like you, when you here Reto [*Reto Schneder, Swiss Re – ed.*] and others speak, I think you should think about what's the pre and post tradeoff that we can offer.

Lloy'ds published a major space weather report in 2010. We have recent studies addressing freqeuency, severity and vulneraiblities

In 2010 we published a report on the threats. We've been working with AER, the Atmospheric and Environmental Research since last year and we have recently just received studies from them that talk about the quantification of effects, both in frequency and severity of space weather and the vulnerabilities of the North American power grid. We take that [into account] as well as things you all talked about earlier today in terms of the Canadian loss and the South African loss.

Lloyd's is working with other major insurance companies to address this and other emerging risks

We're part of a wider solar storms working group, together with Allianz who's here, and Swiss Re and Zurich as part of a chief risk officers' forum initiative on emerging risk. Trevor Maynard who we'll hear from later who works with us, heads up our emerging risk effort.

This is one of the most serious risks Lloyd's is concerned with now. "We would love to work with you […] to help mitigate the event…"

We probably have cataloged eight-four risks from nanotechnology to any number of other things, and this is one of the most serious ones we think we're concerned with right now, not so much because it's more likely than nanotechnology causing a problem, but because of the quantum and materiality of the impact times a low probability event.

So anything we can do, and we really welcome the opportunity to speak to you today to let you know we have skin in the game. We care. We'd love to work with you and our industry partners to find ways to help mitigate the event, if at all possible.

Lloyd's advice to the U.K. government: A call to action

It's a lot like some of the debates that go on, on climate change and the threats; some people believe it, some people don't. But the point is who's worse off if you try and act as if you do believe it? Generally speaking I think this may not happen during our lifetime, but it could happen next year. And the trouble is repairing it after it happens next year could be at a level of materiality – given the shift in how we all communicate, how we all work together in terms of the electronics and interaction between people -- that it's not to be poo-poo'ed.

So basically what we'd like to recommend in our presentations to the U.K. Parliament, to the House of Commons Science and Technology Committee [in regard to] damage to electrical transformers, they're particularly vulnerable to major solar storms.

Malicious EMP – Insurors will only pick up a portion of the cost impact

A lot of the discussion prior to this has been about the electromagnetic pulse damage. We sell terrorism coverage. We do an aggregation grid but the trouble is the aggregation grid we have might pick up the instance of an electromagnetic pulse in terms of the physical damage; it doesn't pick up the contingent business interruption damage or damage to suppliers.

And we think that's a pretty dramatic risk for us to take on and we certainly learned that from the contingent business interruption of what was not able to be produced in Bangkok last fall. Where that's rippling through the economy, and we're hearing about 100 million here, 300 million there, 500 million there, if you have one of these electromagnetic pulses from the sun and it hits just right, it's going to make that look like child's play. And so we think it's very important to take a good long look at this right now.

Urging regulators, legislators and industry to consider low cost mitigation

I think I've been alarmist enough. Anybody asking for more? [*laughter – ed*.] But basically we think from what we've heard and may hear today through this process, there may be some opportunities to mitigate risk at a very low amount. And I would encourage the regulators, the legislators, and industry to think very clearly about whether or not it makes sense to seriously consider an issue to address them.

Insurors will probably try to find a way to help

And those of us who have a lot of skin the game probably will try to find a way to help because we do basically exist to handle problems other people have. If we can mitigate those problems, we're quite keen to invest in them.

So thanks for that. I'd be happy to answer some questions about that now, or later at your convenience.

Session 2, Panel 1: Impact of Energy Policy on Societal Risk, Resilience, and Security

Reto Schneider: **Background**

[…] Communication across borders could be a recipe at least to overcome part of the problems we're discussing today. This communication issue we call *risk dialog*, involving many stakeholders.

And I think Swiss Re started more than ten years ago the Risk Dialog as a publication called solar wind, no reaction, close to zero, and obviously the time was not mature enough. Completely different situation last year when we issued from the CEO for this publication talking about power blackouts, not solely focusing on solar winds but also on terror attacks and manmade failures.

The role of insurance companies – Responding to a dramatic change in the energy sector's awaress of severe space weather

I guess now something has changed dramatically […]. So how can we, from the insurance industry, add value and maybe help to solve your problem? I guess we are one of the few industries that are involved in all potential industries and businesses we conduct and this allows us to do a risk assessment in all the sectors. We are not just focusing on a single company, on a single industry.

After the financial crisis we all kind of woke up in shock or in paralysis, and after the shock we started to look systematically for systemic risks. A power blackout qualifies in my view as one of the biggest systemic risks we have ahead of us. There are a lot of global or systemic risks that have the potential to shock as well, from a pandemic situation to another financial crisis, which is also looming out there, to a cyber security crisis to social unrest. We have seen recent examples in northern African areas.

100% risk, with severe global impact

But the solar storm – and you have talked in the morning a lot about electromagnetic pulse used as a weapon from terrorists – but I guess the solar storm is kind of unavoidable. Some parties told me it's an act of God and you cannot work against it, but you can prepare and can accept that the probability is one hundred percent that it will happen. I guess that's the difference when we compare a solar storm versus an electromagnetic pulse; there is still hope that we can eradicate the cause of everything but we cannot change the sun, right?

Therefore we have to prepare ourselves to get our infrastructure fit to withstand the solar storms. It's also not comparable to large earthquakes or hurricane events because this despite the fact that there are regions [affected], they are still more or less local. This global scope where at least

there can be a have potential effect in North America and Europe in one event, that makes solar storms unique.

Insights from the insurance industry's risk governance council

I'm also working for the International Risk Governance Council (IRGC), and this organization has issued a publication about the management deficits related to emerging risks and contributing factors to emerging risks. I don't go through the entire list, but I feel tempted to just list some of the contributing factors which I think are important to underlay the problems related to this power outage.

Underinvestment in infrastructure

I think we have a general underinvestment in the infrastructure, and this was reported in the World Economic Global Risk Report several times, that not only the United States but also Europe, we need trillions of dollars investment in making our old fifty, sixty, seventy-years old infrastructure fit for modern times. It's particular difficult to do that in the current financial environment, where we all know about the situations going on, and I doubt that some of the political systems are willing to invest money for the next thirty to fifty years. This is something we have to do in order to sustain the performance of our infrastructure.

Power grid privatization – minimizing consumer costs at the expense of complex interfaces that can sacrifice resilience

Another point is privatization. I'm not talking about free market but the privatization took the systems apart. We have now producers, we have now transporters, we introduced a lot more interfaces and under the assumption that they are well managed it's okay, but under the assumption that every partner wants to save cost to maximize profit, they may scrutinize the robustness and resilience of the systems in order to make profit.

Increased resilience risks due to restructuring and privatization mean an increased need for regulation

This needs to be controlled, and there I'm very clear. For me, power is like the blood in our veins and I cannot understand why we have not or practically not regulated the power industry. We have done many more things in the aviation [industry], we […] regulate the pharmaceutical industry, but we barely trust [regulators] to regulate the power industry. Maybe we have to change that.

Transormer risk: No transparency, little evidence of organized planning for resiliency

Then what else? Repair is only done after failure. I'm trying to find out in Europe and the U.S. where are the old transformers. I had no chance [to do so]. There are no inventories available, and nobody knew which transformers are which age, was it maintained well or not. Basically, it was not transparent.

Operational procedures for power grid shut-down and restart?

I tried to talk to people in Europe – how they coordinate the organized shutdown and restart of the grids. I should have avoided that, because there is not such a body doing that. Maybe they are developing such a body? I know that some of those discussions are going on.

"Generalized amnesia"among power producers

Then I found that we have kind of a generalized amnesia here when it come to remember big events. When I was talking to Swiss power producers they told me a saturation effect in transformers, we have never discussed because we are [in the] south [of Europe] – it only appears in the northern hemisphere [*with no apparent awareness the equatorial reach of the 1859 and 1921 storms – ed. note*] occurred]. There we have to change how risk is perceived among experts.

And the fact that they told me we never have built during my entire professional lifetime – that was a typical answer. Therefore I think we have to expand our memory and we have to make sure that we apply *today's* vulnerability of our complex system, to some of the old events that have occurred, but [when we had] much less vulnerable infrastructures around us.

Then stakeholders; It's a big question whether we are all aligned and whether our incentives are all aligned. Who earns money now? And if we invest money to infrastructure who pays the price? I think power is too cheap. So we have to prepare customers that power in future will be more expensive. This is a cost [for which] there is no workaround procedure.

I already mentioned the ignorance of a historic storm, and more important, I think people are reluctant to talk about worst case scenarios and by worst case I mean *really* worst case scenarios. When I talk to the companies in Switzerland who told me half a day power outage is close to a worst case, one or two days max; when we prepare the scenarios internally in Swiss Re, we conceived of several weeks of blackout in particular regions.

We cannot afford to wait. The problem now is not insufficient modeling. It is insufficient imagination

Now the gap between what I am told from the specialists and our in-house scenario analysis is *huge*. We have to close this gap. And when I hear that we need models, yes I fully support that.

But I don't need to validate these models. Because [more than I need more accurate, better validated models] I need people who believe in the models and are willing to do something. I call this making decisions based on imagination. Because what I see is making decisions based on analytical data only. And I do think we cannot afford to always wait until science has delivered all the solutions and the necessary data.

What should be done now?

What should be done? I think in prevention, intervention, and postvention terms. I expect that we all together, all the parties involved, companies -- private companies, the government, the regulators that we [must] invest in prevention.

We have to make the space infrastructure fit. We have to make sure the ears and eyes in this space can continue to deliver the information we have to assess, the early warning if you want.

We also have to fix ground-based infrastructure; we need it to survive. We need new power transformers. We need new power lines. We need modeling and monitoring. We need incident reporting, and we need transparency. And *we need to renew the systems* but please let us renew the system with the appropriate tools and techniques that are available or must be developed. But we cannot wait ten more years.

Planning for "post-vention"

On the postvention side, around preparation for a positive end, I strongly urge the companies to do a proper business continuity management, business impact analysis and disaster recovery plan. We did a great job at Y2K. Some people said it was a no event, but we don't know whether some of the activities has helped us to survive this without big problems. Let's do it again. Let's invest this money and try to avoid the big bang caused by large power blackout.

A call for reverse stress testing

Let me say some last words.

Stress test: I like stress tests, but usually stress testing is done based on past experience and assumptions deduced from past analytical data. I would vote for the introduction of *reverse* stress testing. And by that I mean that we draft a story that makes sense and we then work backwards and say what is needed to survive in the story and the world we just drafted, by our imagination, and therefore for me reverse stress testing is not an analytical process, it's based on the magination.

A final word: We cannot afford to wait. And don't expect the insurance sector to solve the problem through compensation

My final say would be that *we cannot afford to not invest in the necessary mitigation measures*.

And the last thing, I don't think that the insurance industry as such can compensate the world's economy in case of a big disaster. We will be a tiny little drop on a hot stone, and most of the economic losses would go insured, and must be carried by society, by the companies and governments involved.

I didn't say thank you at the beginning of my introduction. Now I say thank you for giving me time for these short remarks. Thank you.

Session 2, ***Panel 2: Knowledge Base for Electromagnetic Threats:***

The Roles of Government and Industry

Joseph McClelland: ***Introduction***

Thank you for the introduction. My name is Joe McClelland and I'm the Director for the Office of Electric Reliability of the Federal Electric Reliability Commission. Before we begin, I would like you to know that today the views I'm about to express are my views only. They don't remotely reflect the commission or any commissioner or the chairman, any of the U.S. delegation, any other friends and associates and even distant relatives. The U.S. delegation has said loudly "amen."

I should say one other thing, I had a professor from Scotland who used to teach electromechanical stats, he was an electromagnetist in college. He had a very thick accent and he would say this stuff's as dry as the dust maties, everyone up. We would all have to stand up, so if anyone feels they need to stand up, stand along the walls, move around a little, please do so. Don't torment yourselves. I won't take offense to it. Anyone that needs to do that, do that. It's better than dozing off in your chairs.

The power grid is agnostic – failures can come from solar magnetic disturbance or from EMP, and there are mitigation strategies for both

Today's remarks are going to center on solar magnetic disturbances, but I'm not going to limit my remarks solely to solar magnetic disturbances. I am also going to discuss electromagnetic pulse. The reason I'm going to do so is the grid is completely agnostic as to where the threat comes from. It doesn't care. It's just going to simply see the effects, and if the effects are large enough it's going to fail. From that perspective I will address both. I'll also say there are mitigations, careful and deliberate planning mitigations we can address for both events.

The very first thing, we have lots of events in space that we can discuss. There's been a lot done and we've learned a lot and we're about to make, as Commissioner LaFleur has said, we're about to make significant investments in the grid. Let's look at what we've learned and let's look at what we should do on the verge of these expenditures. The very first thing I wanted to discuss was the Carrington Event of 1859.

The Carrington Event, 1859

This was called the largest event ever recorded. The magnetometers of both the Kew and Greenwich observatories were driven off scale. They were paper so we can't know a lot but we know it was large enough for the magnetometers to go off scale.

The telegraph systems in the United States, particularly in the northeast experienced difficulties. It was actually energy inefficiency, if you will, interoperating without batteries. No one complained. The auroras were seen

as far south as Hawaii and El Salvador. What were the lessons there? We learned sort of a singular lesson from that event. We learned that a solar magnetic disturbance can cause profound effects with the electrical system on earth.

The 2nd major historic geomagnetic storm – 1921, caused fires in telegraph systems and failures in railroads, long before the development of the modern power grid

The solar storm in 1921, this great storm was estimated to have been 4800 nanoteslas per minute. The aurora was seen as far south as the Caribbean. It caused fires in the telegraph systems in both the United States and in Sweden. The New York Railroad traffic operations were slowed; it caused disruptions in the operations because switching equipment began to fail. There was a signal systems problem when one of the control towers caught fire.

What did this teach us? I would submit it was sort of a singular lesson at the time. The solar storms and resulting ground-induced currents can play havoc or cause problems. They can damage and destroy systems, electrical equipment.

The history and development of the EMP threat

Now I'll cover the the Starfish Prime 1962 experiment, Dr. Pry referenced that, and also 1984. The U.S. detonated a nuclear device in the upper atmosphere to study the effects. About 900 miles away in Hawaii there were hundreds of streetlight failures, burglar alarms were triggered, and microwave links were destroyed. In that same year where open source reports that the Soviet Union conducted its own upper atmospheric test. The results were more profound, that they were in closer proximity to electrical systems. There were damaged underground cables, overhead cables and lines, and a power station, and there were other pieces of equipment, large and substantial pieces of equipment on the power system that were reportedly damaged or destroyed.

Operator intervention is not a possibility to mitigate an EMP strike

What's the lesson learned here? The damage and destruction can be manmade, and in some cases it mimics the effect of natural disturbances. Operator intervention in these cases is unlikely or impossible. There's no advance warning, and by very definition military actions operate on the element of surprise.

The Synergy Option for overlapping protection:

Automated grid protection equipment can protect against both Solar Magnetic Disturbances and EMP

Also automatic measures such as locking, dampening, or tripping equipment can prevent not only manmade occurrences on the E3 component only, the ground-induced current only, but it also can prevent solar magnetic disturbances. So you have sort of a nice overlap in those two cases.

Lessons learned from the Quebec blackout of 1989

Let's go to 1989, probably most of you are familiar with this also. So in ninety-two seconds the Quebec grid collapsed at the onset of the storm. Most people -- a lot of people don't know it but that collapse caused voltage problems, you can see large blocks of load dropped off, voltage skyrockets. That voltage, that over voltage condition actually destroyed two large bulk power system transformers in St. James Bay, causing that particular generator to go offline until the transformers could be replaced.

The 1989 storm's damage occurred at only one-tenth the level of the 1921 storm.

Quebec Damage: The grid was restored; eighty percent of it was restored within ten hours. The intensity of the storm, however, was only one-tenth of that of the 1921 storm.

U.S. Damage: In the United States, as we heard earlier on, two GSU generator step-up units in the Salem nuclear plant were also destroyed. About 200 miles to the west, my alma mater Allegheny Energy noticed that one of its large bulk power system transformers became very gassy. It was because of ground-induced currents, and it was taken offline to repair it.

Lessons learned from the 1989 storm

Now what's the knowledge base from this? Even short blackouts, blackouts that are a few hours long can be very expensive. I'd like to read you an excerpt along these lines. This is from the 2003, April 2003 blackout.

Now we've been told in some of the testimony we received, and I'll get to the conference in just a bit, that a grid collapse would be very similar to the 2003 blackout. I think the 1989 grid collapse would also be similar. There are going to be transformers destroyed but certainly we would hope wouldn't be hundreds of transformers.

The official U.S. and Canada Joint Government Report on the 1989 Storm

Excerpts from the Introduction to the Report

Let me read this excerpt; this is from the introduction of the 2003 blackout. This was jointly produced by the governments of the United States and Canada.

"The blackout began at 4:00 p.m. Eastern Daylight Time, the power was not restored for four days in some parts of the United States. Parts of Ontario suffered rolling blackouts for more than a week before full power was restored. Estimates of the total cost in the United States range between four billion and ten billion dollars. In Canada gross domestic product went down 0.7% and in August it was a net loss of nineteen million work hours and manufacturing and shipments in Ontario were down 2.3 billion dollars."

A very large wide-scale grid collapse will cost a lot of money.

If we're comparing it to the 2003 blackout, and we're saying that that blackout managed to be larger, it would be profound effects, cost a lot of money, not to mention loss and the human misery imposed upon areas without power for those periods of time.

Lessons learned from the October 2003 storm – "Large bulk power system transformers can fail from very low level storms"

Now we have the October 2003, the October storm, this was also a very significant storm and I think there's some profound lessons learned here.

This was a very low-level storm as far as magnetic fields go. But it was longer in duration and the damage was extensive in South Africa, where over a dozen transformers were damaged in this storm, in addition to reports of damage in Sweden, although I don't have those particulars.

The knowledge base here is that large bulk power system transformers can fail from very low-level storms; in fact the registered storm level was only 100 nanoTeslas per minute. For comparison sake, the 1921 storm was 4,800 nanoTeslas per minute.

Damage and destruction from long, low level storms – with little reactive power -- goes unnoticed until mass transformer failures occur

These long, low-level storms create low-level GICs that don't have much reactive power. So they can remain on the grid, destroying, damaging and destroying those transformers for long periods of time unnoticed until you've got mass failures that surface in South Africa.

The U.S. is more vulnerable than South Africa, which experienced mass transformer failures from a low-level GMD

I think another important factor is we've heard the northern hemisphere is especially susceptible to this phenomenon; it's more than South Africa. So I think the lessons learned are that we should not be too cavalier about the low-level magnetic field that we see or the location of the transformers themselves.

I don't think this is a problem that anyone can afford to ignore.

Not only do we have these events, and by the way I'm going to request that the EIS add in to the materials, a list of articles that are received from our staff. There are very nearly a hundred solar magnetic disturbance effects in this article. These were separate events that occurred since the 1859 Carrington Event and some of them are very significant.

What I'd like you to do is when you get the materials, look at the March 25th, 1940 storm called the Easter solar storm. There was extensive damage from this storm to telegraphy systems, telephone systems all over the world. Also the Transatlantic cable, there was a very large spike in that cable, 2,600 volts according to the reports. I think that's substantial so that should add to our knowledge base.

Recent Government Studies:

The conclusions of recent United States and United Kingdom government e-threat studies:

The 2004 Congressional EMP Commission Report: *An EMP or Severe Space Weather event could cause a blackout lasting months or years*

Starting in studies in 2004, the Electromagnetic Pulse Commission of Congress found "Recovery times of months to years instead of days for an EMP attack on the grid."

They also found that geomagnetic storms can and do affect the power grid in a matter similar to E3. Three effects: E1, E2, E3 -- E3 is geomagnetically induced currents. They recommended critical elements in security be protected. In 2008 a follow-up study they reiterated their findings and also said the cascading effects from even one or two small weapons detonations in space would almost certainly affect seventy percent of the United States.

The 2010 Department of Energy / NERC Report:
A severe space weather event could cause large scale grid damage

In June of 2010 in the North American Electrical Reliability Corporation and the Department of Energy [performed a study]. I would like to call out Bill Bryan and thank him for helping to sponsor our report [which followed this DOE / NERC report]. [This Report from DOE and] NERC found that over 350 transformers could be damaged by a large solar magnetic disturbance. They also found that voltage collapse and long-term damage could lead to prolonged restoration and long-term outages.

The 2010 Oak Ridge Nat. Lab, FERC, DHS, DOE Report:
A 1921-class event could damage or destroy hundreds of EHV transformers

In September of 2010, the Federal Energy Regulatory Commission, Department of Homeland Security and Department of Energy released a study conducted by Oak Ridge National Lab, Metatech and storm consultants that found the following, and their report was consistent with the NERC report. That over 350 large bulk power system transformers could be damaged or destroyed by solar magnetic disturbances the size of the 1921 event. Over 130 million people will be out of power as a result of the grid collapse. Depending upon the level of equipment loss and the location, outage could last for months and even years.

2012 United Kingdom Defence Committee Report:
A severe space weather [or malicious EMP] event could have serious impacts on infrastructure and society.

The Tenth Report of the Session of the House of Commons Defense Committee on developing threats from electromagnetic pulse February 2012 concluded that severe space weather event could potentially have serious impact on the U.K. infrastructure and society and they must proceed with a manner of urgency to identify how seriously the Carrington Event would affect the U.K. infrastructure.

I would submit to the U.K. with all due respect, we should also study some of the low-level but long duration events, the things that for instance the South Africans experienced because if it is a large event indeed reactive power effects may be triggered and that may damage some transformers but it also may cause transformers to trip off.

The risk of that may be low now, at present, but we cannot be complacent. We must continue to assess risk and consider it vitally important that more hardening of infrastructure begins now, primarily because it takes so long to harden the infrastructure against these issues.

Reviewing a recent NERC study

I'll skip ahead to the NERC report of February 2012; it reached very different conclusions from the prior studies in a way. In another way the conclusions weren't so different. Let's go down through them.

NERC Report: GMD will likely cause grid collapse

It said the most likely outcome of a large solar magnetic disturbance would be grid collapse from reactive power requirements. The grid would become unstable, solar magnetic disturbances cause GICs, the GICs then interact with the transformers. They cause reactive power consumption, that reative power consumption then triggers protection equipment that causes the grid to collapse. The collapse would therefore save transformers from damage. […]

NERC Report: Many transformers will be damaged or destroyed

They did conclude however that the most vulnerable transformers and those would be older transformers and transformers at the end of their lives, the transformers that have a bit of gas and oil and a high moisture content would be vulnerable and could be damaged or destroyed in the process.

Assessing the problem and looking for next steps: *The recent FERC GMD Staff Technical Conference*

Because there was such disparity, the Rt. Hon. James Arbuthnot who talked this morning who said we need some consensus. We need consensus in the technical community on both the issue, the problem, and also on mitigation.

The FERC GMD Conference: Two Panels

Because we have a lack of consensus the staff recommended to the commission that we conduct the technical conference and it consisted of two panels. The first panel explored the differences from a technical perspective: What did NERC conclude and why and what did everyone else conclude, and where there are differences and where there are commonalities, and can we resolve some of these issues.

Secondly what should we do moving forward.

The FERC Conference: Finding consensus

From the technical context, if you would flip ahead we found some common conclusions and these were very encouraging.

Consensus: Planning for Grid Collapse is not an option

Everyone said please consider the cost, and consider how we operate the grid.

You don't operate the grid for system collapse, period. It costs billions of dollars. There's going to be, certainly, transformer damage in a sub-grid collapse, there could be prolonged exposure, or exposure before the collapse that causes extensive damage to transformers. So why fight over it? We know it's going to cost a lot of money. If you look at a billion dollars at a hundred thousand dollars a transformer, that would provide mitigation for 10,000 transformers, which is double what I hear anyone talk about. For a fraction of a four to ten billion dollar outage you could mitigate it and be done with it.

Consensus: System-wide planning and coordination are essential

Planning and mitigation must be done on a coordinated and system-wide basis to ensure threat reduction. Why? If area A puts blockers in and area B doesn't, area A just done blocking. It's pushed the ground-induced currents away from itself to area B. So prior to the mitigation, Area B may have concluded and correctly concluded "I don't have a problem. I don't need to take action."

In the absence of knowing what area A did, now they *do* have a problem and they could be surprised and themselves cause themselves a grid collapse. By the way that grid collapse will damage the transformers in area A. They wouldn't be out of the woods just because they protected their own transformers.

Lower latitudes are not immune from GMD effects and you see GMD effects should be included in studies of mitigation initiatives. This is partially because you're pushing the GIC around. It's also partially because lower level GICs […] for a long period of time can also damage the transformers. Texas itself is not immune, that's why we're looking into this. There are subsets of all the critical facilities that can and should be identified, for a geomagnetic storm. Think about your own areas – what would you protect?

The FERC Conference also reviewed other critical issues

Nuclear Power Plants:

Consensus: NRC says problems [nuclear cooling failure] occur after 2weeks without grid power

We discussed some of the critical subsets; servicing nuclear power plants, I think in your materials you'll see that the technical expert from the Nuclear Regulatory Commission said that about two weeks is all you can go without power. If you go longer than two weeks you start having problems with the nuclear power plants. So what should we do to ensure that there is continuity of service at nuclear power plants?

The Risk to military Installations

What about the military installations? That doesn't necessarily mean blocking it, it may mean dampening, but if you get into dampening what to you

dampen to? Do you dampen to a five-year event, a twenty-five year event, fifty-year event, a hundred-year event? I can tell you with a certainly the time you pick, the day after you put it into place is the time you'll find you have the wrong storm category.

"Update" is very correct, you put blockers in, you move that power around. What has to happen is if you look at the interconnection-wide basis plan, maybe […] as an industry, you pick the very most critical facilities, say there will be blockers at these facilities and everyone else has to figure it out. We're going to do the ground current interrupt, and everyone else has to adapt so that we protect these critical facilities.

No-regrets actions are feasible

More information and study is needed, such as correlation between the field strength, and resulting ground induced currents, but some action can be taken now and the commissioner identified no regrets actons. For instance these vulnerable and critical transformers or facilities, why not start on these? Why not begin to look at these, clearly identify what they are, that will take some time, and then start laying out on an interconnect-wide basis what the mitigation plan should be.

Consenus: Common standards are essential

Everyone also said standards are necessary to be sure that effective and consistent action is taken. They didn't necessarily say FERC should pass the standards, but they did say there should be standards to make sure that everyone is on the same page and following the same rules.

As it stands, our plans for power grid upgrade increase vulnerability

I just want to also add here at the end, I think as we move forward as societies, as we look at energy efficiency, as we enter in more renewables, as we change the generation mix, in some ways we're making ourselves much more vulnerable to these threats than we were in the past. Long distance, low-resistance transmission lines act as pathways for ground-induced currents.

New, high-efficiency transformer designs increase vulnerability

More energy efficient transformers can actually drive them into saturation, The saturation curve is actually very low. It means you need little energy to get the transformers working properly which also means that if you add GIC to these currents it takes little ground-induced current to cause more damage.

And we're at the knee of an investment curve here. We've moving to change the generation mix; we're also incorporating equipment that's more energy efficient. If we miss this opportunity it's going to be very costly to go back and figure it out later.

In closing I'd be happy to take any of your questions, that the docket number if anyone is interested, anyone can comment and I encourage you to do so. And the commission -- what commission staff is doing is building a record from both sides. We'll summarize the issue, develop a position, and give that position to the commission.

I cannot guarantee how the commissioners will vote, I do not know. And I don't know what the staff's position will be yet but I do know that staff and commissioners, you're heard Commissioner LaFleur, are very determined to investigate this and get to the bottom of it, And if it needs litigation, press for litigation. As industry has concluded – we've talked to industry about this.

That's it for my comments. I look forward to your questions.

Keynote Speaker: Cascading Infrastructure Risks – National Security Implications
The Honorable Dr. Paul Stockton, Assistant Secretary of Defense, Representing U.S. Defense Secretary Leon Panetta, US

Session 3

Keynote: Cascading Infrastructure Risks - National Security Implications

Honorable

Dr. Paul Stockton: ***Introduction***

Thank you on behalf of the Secretary of Defense, Leon Panetta, who couldn't be here today. I want to thank you for the opportunity to make my problems your problems.

I'd also like to offer my appreciation to our British hosts, Secretary of State for Defense the Honorable Philip Hammond; the Rt. Hon. James Arbuthnot, Chair of the Defense Committee of Parliament, thank you so much; Lord Toby Harris, and a special thanks to Avi Schnurr who has brought together such a great team. Thank you. Congressman Franks, many of us know the vital role that you're playing in Congress in order to build bipartisan support for the kind of progress that's absolutely essential. Let me state my gratitude and also it's great having you as a politician.

DoD's depends on the commercial power grid to execute its core missions

Let me tell you why I'm here. I'm confronting a paradox. On the one hand the Department of Defense is enormously dependent on the flow of commercial electric power. Ninety-nine percent of the power on which we depend in the Department of Defense comes from the commercial grid. At the same time, I have a vanishingly small, virtually nonexistent authority over the commercial power grid. That's why again, I want to make my problems your problems. I want to talk to you about some of the challenges that we face today in the Department of Defense that can only be solved with the leadership of the Department of Energy, the Department of Homeland Security, and above all the private sector so we can execute our core missions in the Department of Defense.

Focusing on three things: the threat, risk assessment and progress through partnership

I'd like to do three things today. First of all I want to talk a little bit about the threat. I'm concerned that we've been far too rosy in our assessment. We haven't been nearly gloomy enough so as part of the race to the bottom in terms of making people afraid, I see particular concerns in the Department of Defense that I'd like to share with you today. That's problem number one.

Problem number two, the Department of Defense does not have the risk assessment methodologies it needs and the strategies for investing in greater resilience in assuring our continuity of operations. That's why I'm so grateful that the insurance industry is represented here, other folks who do parallel kinds of analysis so we can share perspectives.

The third thing I'm going to do is focus on the progress we are making, another [example of] "admiring the problem," but we're also making some terrific progress, both substantively and in terms of the models of partnership that we're now building that reflect the reality that other federal departments and private sector must lead the way if the Department of Defense is going to be able to do its job for the American people.

- ***The 1st question: the nature and impact of the threat – a Pentagon perspective***

Let me turn now to the first question and that is the nature of the threat. Reto Schneider said something earlier today. He said that earthquakes aren't a big concern because they're more or less local. This is still another great advantage of life in Switzerland. Life in the United States, along with cow bells and everything else. Life in the United States, we think about earthquakes all the time, from the perspective of the surety of the flow, of the reliability of the flow of electric power. Let me give you one example.

Long term power outages – an example from a recent exercise

Did anybody here participate in the national level exercise, the New Madrid Fault exercise? Well every year we have an exercise to help us get ready for what could happen at any moment. In 1812 there's an earthquake fault along the Mississippi River. In 1812 there was a sizeable event, 7.7 on the Richter scale. This event caused the Mississippi River to flow north. It was felt in Boston. If this event were to recur today and it could happen at any minute, it could happen right now, my Blackberry would start going off. There would be severe disruption of the grid according to my colleagues in the Department of Energy, over five or six states; massive geographic scope.

And there would be something else very interesting, and that is the length of the power outage. That gets me to a point that Lord Harris made earlier; he'd like us to get ready for a long-term power outage of seventy-two hours. I respect that. Actually in the Department of Defense, we're good at seventy-two hours. We've been working on that for a long time. We're not so good at what New Madrid would cause, a multistate outage potentially of weeks to months.

The real theme of today's presentation:

Keynote Speaker: Cascading Infrastructure Risks – National Security Implications
The Honorable Dr. Paul Stockton, Assistant Secretary of Defense, Representing U.S. Defense Secretary Leon Panetta, US

Cascading infrastructure failures – a DoD perspective

Let me walk you through why this is so troubling from my narrow, worm's eye view from the Department of Defense. First of all, there would be cascading effects on critical infrastructure. That's the real theme of my discussion today, it's the topic of my discussion because when electric power goes out in Memphis which would be near the epicenter of this event, the aquifer is 300 feet below the surface of the city.

A loss of the water infrastructure would be catastrophic

Now people like me who are on the Department of Defense regular feeding program, we're fine without food for a while. No drinking water, that's a big problem. That's a big problem for public health and safety. In Memphis there would be raging urban wildfires because of the breakage of natural gas lines. No water pressure to put those fires out.

The transportation infrastructures fail without power to gas stations

Imagine the cascading failure of critical infrastructure. Here's another example in the transportation sector. People who could flee would be fleeing in a private vehicle although bridges and roads would be severely disrupted. They would be going with their feet. Every gas station in the United States and probably every country represented here, those gas pumps run on electricity. So you're not going to get very far. In fact, the interstates would soon be clogged with private vehicles that are out of gas.

Air transportation – another possible impact on DoD disaster response

At the same time that I'm trying to come in with very large-scale Department of Defense forces in order to save lives and sustain lives in support of the civil authorities who will always be in charge of disaster response in the United States. Just to give you a bit of jargon, I would be worried about receptions, staging onward movement of those Department of Defense lifesaving forces. Are the airports going to be up and running? We're not too sure.

What is it going to take to be able to provide for the onward movement of these forces in an environment where transportation infrastructure, communications infrastructure, all kinds of critical infrastructure components have cascading failures due to that initial loss of electric power. Again my job here today is to make things a bit gloomier. That's a bit of a Department of Defense flavor of the risk factors that we need to take into account, that require some serious analysis and planning.

An symmetric strike on our power grid: "the smart way for an enemy to take down our ability to deploy, sustain and operate our forces"

That gets me to my next challenge, and that is inside the limited world of the Department of Defense, we have a challenge that I call mission assurance, and that is we need to ensure that the Department of Defense can execute its responsibilities signed by the president, both abroad in Afghanistan, and at home should disaster strike, no matter what, even if an adversary were so intelligent as to realize that the way to attack our deployed forces, where they're deployed is the dumb way to go. The smart way to take down our ability to deploy, sustain, and operate our forces is to attack us asymmetrically, attack the electric power grid in the United States that is not owned by the Department of Defense, never will be owned by the Department of Defense, but upon which the Department of Defense is utterly dependent to execute its responsibilities as signed by the president.

Echoing Defence Secretary Hammond: We never before had to invest in protection against such asymmetric threats

We need a mission assurance strategy and we haven't had one. I'll tell you in particular what the risk assessment problems have been. First of all, we never had to invest in protecting ourselves against these asymmetric threats. Secretary Hammond said something this morning that resonated with me. He said we're used to here in the United Kingdom to buying weapons and other shiny objects, and everybody knows what the return on investment is. That's our situation in the United States too.

In modern times, we are not used to spending money on resilience to an attack on critical infrastructure

We are not coming out of the Cold War and post-Cold War era, used to taking our very scarce defense resources and instead of buying F-35's, or what-have-you, spending money to ensure that we can execute our core missions even in the face of these attacks on critical infrastructure. We're not used to spending money on resilience.

- ***The 2nd problem – Coordinated risk assessment***

Second problem, our armed services are absolutely fabulous. They've been waking up to this challenge. They're beginning to develop their own risk assessment methodology to ensure that they can do their jobs, their assigned warfighting missions, and guess what; surprise, surprise, the army, navy, air force and marine corp. all came up with different and in some cases conflicting ways to assess their vulnerability to these kinds of asymmetric attacks and how to assess where they should be investing their dollars in order to provide resilience in order to be able to execute their core missions.

So across the department, we've got these homegrown risk assessment methodologies that have different algorithms, different factors, and make it

impossible for the secretary of all defense, Secretary Panetta to decide on a department-wide basis where should that incremental dollar go to provide for the biggest bang for the buck in terms of building resilience.

- ***The third problem – functional analysis, identifying critical installations***

The third problem, and that is functional analysis. Again we've got terrific installation commanders who on an individual basis, military bases across the United States that are waking up to this challenge that space weather could happen at any moment, EMP, New Madrid fault, I need to build resilience, to be able to execute my core missions.

But we have not adequately in the Department of Defense been able to map almost from a supply chain perspective what is most critical to execute in that very small number of core Department of Defense missions. We haven't been able to rack and stack installations in terms of their criticality, their priority in terms of at the end of the process what are you actually doing to execute the president's guidance in terms of the missions we're given to create? We haven't had this kind of functional analysis of what it takes to execute our core missions and then based on that be able to prioritize (indiscernible) so the most critical facilities are getting the lion's share of the investment.

An example of the problems with critical priorities – warfighting in Afghanistan depends on controls from facilities in the U.S.

The reason this is so difficult, where's Cheryl? We were just talking about this before because every year the Department of Defense finds itself executing these missions more and more in a way that depends on installations inside the United States. The way we operate in Afghanistan now is very different from the way we would have five years ago, because more and more of those operations are controlled minute-by-minute, I'm talking about tactical and operational efforts are controlled in facilities inside the United States. So we don't always know what's critical and what isn't unless we do the analysis. You can't sit at the end of an air field and see whether there are planes taking off or not in order to determine criticality. You have to understand the modern way of war in the Department of Defense. So we need that functional analysis.

- ***Assuring the continuity of electric power: Partnering with the electrc power industry for progress in power grid resilience, to assure DoD can perform its mission***

And then finally it's what I started with; we've had an inadequate understanding in the Department of Defense of how we must be able to partner together with the private sector, above all the electric industry for purposes of today in order to understand even if we were in a hardened DOD facility from an inside the base perspective, it's that flow of electric power, that resilient flow of electric power that we need to be able to ensure so that in turn we can live up to our commitments to the American people to execute the responsibilities assigned to us. We need to not only do better inside the Department of Defense, we need to reach out in partnership with our industry partners.

DoD progress in mission assurance – the Secretary of Defense has now defined a department-wide strategy

We've gone a couple of directions in order to fix these problems. I'd like to say a few words about that now. First of all, for the first time ever, in the last week the Secretary of Defense adopted a mission assurance strategy that for the first time provides for department wide algorithms and risk assessment methodologies so risk assessments can be done the same way by the marine corp., as by the United States air force, toward solving that problem of consistency for vetting these algorithms […]

We are providing basis then, based on these common risk assessments to enable the Secretary of Defense to decide where each additional dollar should be invested to build resilience in a way that's most cost effective in this time of extremely scarce defense resources. Anybody who would like a copy of this, it hasn't really been released but it's unclassified, I'd be happy to share with all industry and international partners here today. Casey Groves, my colleague in the background, Casey would you stand up please? If you'd just give him your email address I'll be delighted to ensure you get an electronic copy of this new mission assurance strategy.

Depending on partnering with industry for mission assurance:

DoD cannot perform its mission without the cooperation of industry, and has new mechanisms for sharing information

It's the partnership with industry that's most important and I'm very aware we're making special progress with Gerry Cauley, I'm so grateful to you, all of our industry partners. Thanks to the leadership of the Department of Energy, Department of Homeland Security, and our industry partners, we've now stood up something called the Energy Surety Public-Private Partnership.

For the first time now we have a FOIA and FACA protected working group where we're going to be able to share sensitive information with industry that they need and they're in turn going to be able to provide us with information

that in some cases might be considered sensitive or proprietary, and within this relationship of trust this new opportunity for two-way flow of information that respects the bottom line orientation that industry must have in terms of cost recovery and everything else; we're going to be able to partner together in new ways.

Assuring the flow of electric power to critical national security functions:

The power industry needs to expand its resilience into a new hazard environment – Beginning with the national capital region

Let me give you an example. I hope that this will be one of the very first opportunities for progress. We're going to build a collaborative approach to look at the national capital region, going back to your question, to think about what more could we do to partner with industry to provide industry with a design basis that they need in order to strengthen the surety of the flow of electric power to critical national security functions.

The electric grid is extremely resilient. It's terrifically resilient against *traditional* threats and hazards.

But now we have a new hazard environment, don't we. We need to be able to share in this trusted environment with industry the design factors, we need to enable industry to have the design basis that's going to be essential as investment in the future grid goes forward. We're going to try that out, first of all in the national capital region. Then leverage that for the nation as a whole.

Prioritizing power restoration for national security

Secondly, we're going to discuss further how there could be prioritized restoration of power. Not all national security facilities in the national capital region are equally important from this functional analysis perspective that goes well beyond the Department of Defense. We need to be able to tell industry instead of just restoring power on the basis of which substation is connected to which substation, help them ensure that when power gets turned back on, as power gets restored, it will be done in a way that strengthens national security.

Those are just a couple of the little projects that we're going to work on using the national capital region to prove out these new opportunities for collaboration in which industry is going to lead and the Department of Defense is going to remain extremely grateful to the Department of Energy and the Department of Homeland Security for their leadership in helping build the grid of the future.

Thanks to all of you. I have plenty of time for questions and comments because I'm here to learn, not just give speeches. Who would like to go first?

Audience

(Joel Mowbray):

: Thank you, the question is if you look at the telephone industry, their partnership with cooperation of the government went fairly smoothly but maybe it was because the telecom industry as it developed in the wireless field already had essentially -- you had players already in the government perspective, government essentially said, okay we need to do X, Y, and Z and industry said okay. And there was back and forth on that. If you looked at that as a model and what do you see the DOD's role is as far as this hodgepodge of different agencies, DHS, DOD, FERC, NERC, other ERCs I probably don't even know about; how do you see the DOD's role in that in terms of working with industry to get to a common standard; figure out how to go forward at least protecting the most critical centers of infrastructure?

Honorable

Dr. Paul Stockton: My personal view is that the Department of Defense is a customer for all the goodness that everybody else in this building is producing. I'm so grateful to FERC for what you do, NERC provides the industry interface for reliability. We've got DOD, we've got DHS. The players are there. What we need to do again is take care of this inside the Department of Defense to understand what our priority needs are and then turn to our lead partners because they'll always be in the lead, so that from our humble perspective as one of the nation's largest energy customers we can have some attention to our requirements so that we in turn can serve the people of the nation.

We're looking at the telecom model. I think it's great and we'll want to look at other models that are out there. Let me emphasize that although we've been talking about mission assurance, I'm very mindful that I'm responsible on behalf of the Secretary of Defense for response to New Madrid when, not if it happens.

We have a new initiative that the Secretary of Defense has asked us to pursue to prepare for what we call complex catastrophes, catastrophes much worse than hurricane Katrina, not only in geographic scope and level of devastation but where we'd have these cascading failures of critical infrastructure that would create unprecedented threats to public health and safety. We need to be ready for complex catastrophes and so that's another realm on which we need to partner together, everybody that's here from the United States, and share what we're learning with our international partners who may also face catastrophic natural hazards.

Session 3, Panel 1

Panel 1: Understanding the Impact: Severe Space Weather and EMP Projections

John Kappenman:***Understanding the impact on power grids***

Thank you very much. My job this afternoon is to again address the issue of understanding the impact on the electric grids. Obviously this is a big topic area. There's lots of areas that can be impacted, so we're just going to peel the onion a couple of layers here, so to speak in addressing this.

Equipment damage

Equipment damage perhaps is one of the hinge issues that we need to talk about and it's certainly going to be a complex topic. This ultimately has to be something that is driven by effective public policies. We need to assure public safety.

Modern understandings of e-Threats have shown us that grounding designs for the power grid are flawed

Power grid design, I would say the premise of power grid design, grounding power grids is inherently a flawed premise or flawed design. The ground connections of course provide enormous economic benefits to society. There's no question about that, but during times of geomagnetic storm, or EMP events, ground becomes a source of danger to the grid. That's not so good from a public policy standpoint.

There has never before been a design code for e-threat withstand

No design code has ever imagined this threat and appropriately taken it into account. Arguably this is somewhat analogous to seismic withstands. We've had the ability to learn from pretty unfortunate circumstances that we need a seismic code where that is appropriate.

New public policy is needed for grid protection against these threats

Realistically this public policy needs to counter the potential for widespread damage and reduce the concerns of lengthy restoration. In my talk here today I'm just going to talk a bit about transformers, and give you a framework and appreciation for this complex topic. It's only reviewing a bit of what needs to be understood.

I'm going to show you a very simple cartoon sort of illustration of a transformer. Essentially a transformer, under normal conditions is a very efficient device. We have a piece of core steel, that core steel couples the high-voltage and low-voltage winding and because of that magnetic coupling a transformer is a very efficient device under normal conditions, better than ninety-nine percent efficiency. It takes a very small amount of electric energy to do that transformation of voltage.

How does GIC cause transformer damage?

When we have a geomagnetic induced current flowing in that transformer, this GIC flow begins to affect the operation of that transformer, [driving it] into a highly abnormal and destructive behavior to that transformer itself. Let's look at some of the dimensions of this.

What is "core saturation," and how does it cause damage?

GIC saturates that core steel. What that means is the magnetic field now is no longer contained by the core steel and begins to increase in intensity and expand outside of the confines of the core steel. Where you have large amounts of magnetic flux concentrating it can cause intense localized heating in those areas.

In addition to that, saturation also produces a large amount of current flowing in the transformer. In other words, it converts a transformer from normal efficient operation into a gigantic magnetic amplifier that is producing all sorts of distortion currents, [with] part of those distortion currents of course flowing in the transformers themselves. Part of them go out into the power grid and cause other problems in the power grid. Of course [within] the transformers themselves, this is another mechanism that can produce intense localized heating in that transformer.

What is the problem with localized heating in transformers? How bad can it get?

If you look at intense localized heating it can activate to the point where essentially it could be a bomb waiting to go off. You've got a huge amount of electric energy available as the ignition source. You've got 10,000 gallons of transformer oil that becomes the equivalent of a large fuel air bomb. If that is a very destructive event it has potential to do collateral damage to sensitive facilities like nuclear plants for example could be involved in that collateral damage.

In those cases where we have design codes, can they dependably forecast localized heating problems?

What is the design basis that we have for transformers out there? That's a big important question. We know that in some cases the models -- we don't have a great deal of confidence that they actually are showing all of the failure modes that can occur. I've never seen a model that has actually validated

some of the field test measurements that have been done on some of the transformers.

Can new transformer design specs fully solve this problem? Manufacturers typically cannot test their designs to the required specs.

Some of the infrastructure owners are out there buying new transformers with a certain amount of GIC withstands. Some of these GIC withstands are so large that the transformer manufacturers really don't have the ability to test those transformers up to those levels. It takes an enormous amount of electric energy because of big reactive demands and so forth to test these 765 KV transformers to these levels. So the manufacturers are only able to give model-only results.

The biggest problem is with the existing, aging transformer fleet, which was not built to any GIC withstand spec.

The bigger problem of course with transformers is we have many existing transformers already in power grid, 5,000 or more transformers in the U.S. alone that have never been built or specified with any sort of known GIC withstand, so how can we determine the performance envelope on all those transformers that will be there for many years?

Of course because there are existing transformers age and condition issues complicate that effort as well. It's a lot like saying if you've got ten meter tsunami walls as the transformer gets older they shrink down to five meter tsunami walls. We don't want that sort of public problem to creep in as well.

Existing transformer withstand capabilities can be estimated using related guidelines provided by transformer manufacturers

Using transformer standards, guidelines have been provided by transformer manufacturers, this is how to estimate what the GIC withstand is for a typical existing transformer that's out there. What we are now doing is providing a performance envelope for that transformer, at various levels of GIC for various time durations of GIC.

You'll see that for high levels of GIC, you can tolerate that but for relatively short durations. In fact the shortest duration defined by the standards that exist are ten seconds. Those are U.S. standards. International standards are actually five seconds of duration.

Also for the long duration events, things that run up to about a hundred minutes of duration or so are much lower levels of GIC withstand there. We think this is what was contributing to the failures in places like South Africa. We have long duration storms that can last for days, much more than a hundred minutes.

Unfortunately, the newest, high efficiency transformer designs appear to be moving in the wrong direction for GIC withstand, with up to ten times the vulnerability of older, less efficient transformers.

In contrast to the NERC report that identified old transformers as being particularly vulnerable, I would like to point out perhaps a new risk vector that has crept into the power grid design and that is the more modern, very high efficiency transformers using the modern core steels. If we plot their capability as shown in red, they have a ten-times lower GIC withstand according to these standards. As you can see, for long duration events, very low GIC withstand according to the standards.

In the single known case of a peer-reviewed transformer withstand value, a severe space weather event could exceed this limit by a factor of 20, or 2000%.

There's only been one peer reviewed publication that I'm aware of where transformer manufacturers have identified a withstand of a particular style of transformers. That was for the Salem transformer. If you look at what they have published here, this is the withstand that that Salem transformer can tolerate if the transformer is completely unloaded, 30 amps per phase is what it boils down to. If you have some load on that transformer, then it's much less.

In general while this is defining the envelope here and we can see it goes up in the case of some of the transformers as much as about 60 amps per phase the reality is a severe geomagnetic storm as we know from the simulations done from collected data making intelligent extrapolations from that collected data, we know that there will be transformers which have for some of the most severe and extreme events that we're aware of much higher GIC levels than 50 amps per phase, maybe in some cases approaching nearly 1,000 amps per phase. We begin to remove some doubt about what may happen to these design transformers.

Average U.S. EHV transformers are typically now approaching end of normal life, when failure rates increase by factors of about five

Now let's talk about age and condition. This is from another publication that's showing you the installation here of EHV transformers in the U.S. and you can see here the average age of the U.S. transformer fleet is really beginning to approach its end of normal life. And we know in the last quartile of the transformer's life, its failure rate statistically increases by a factor of five or so.

So that leads us to some concern in all of the estimates myself and others who've worked with me have done in trying to look at the number of transformer failures or transformers at risk that could be occurring in the North American grid, we did not have age and condition information on specific transformers available to us to make these sort of estimates.

One of my fears is that we perhaps are still understating the severity of the risk that is posed to the public.

Recommendation: It is time to move beyond industry self-assessment, much as society mandates for other critical industries

What are the things we need to do as we go forward? I think we need to step beyond industry self assessment to begin understanding this problem.

There needs to be an effective public policy framework that allows for a management of these complex risks. We have that model in many cases already. Airline regulation is a good example of that model that already exists. Flying aircraft is very complex, designing aircraft is very complex. But we have a set of regulations that require certification of the aircraft. It requires defining the performance envelope of the aircraft. It defines training air crews to operate that aircraft within that performance envelope. It requires black box recorders. It requires collection of data. It requires reporting of failures and incidents. It requires independent investigation teams of these events.

It helps us to understand the risks posed by this. It helps us to develop trend lines and estimate what the severe events could be. It helps us to jointly develop and review mitigation and remedial fixes. It helps us also to identify useful pilot projects and demonstration of hardware and hardening. Again I'll join the rest for any questions.

Session 3, Panel 2

Panel 2: Role of the Insurance Sector: Space Weather and Long-Term Blackouts

Buddy Dobbins: ***Introduction***

Thank you Mr. Chairman, and thanks to the EISS for allowing me to come share with you today. My name is Buddy Dobbins. I'm the Technical Director for Zurich Machinery Breakdown in North America. And I'm the team leader for our Machinery Breakdown Global Technical Center.

As you sit through a conference like this, or as I sit through a conference like this, many things go through my mind. I'm going to go off my speech for just a minute. I was curious; has anybody here ever been through a hurricane? The last one I went through was Hurricane Hugo in 1989. I was out of power for seven days. No electricity, seven days, I wanted my electricity back in two days. We had people that were out of power for over two weeks, three weeks, sometimes four.

I could so sympathize with those folks down in New Orleans and Louisiana, and Alabama after Katrina because so many of them were out of power for so long. I cannot even imagine what would happen in this kind of scenario we're talking about here today, so I'm really happy and thankful that you'd allow us to be a part of this.

Review, analysis and classification of losses at Zurich Insurance

Zurich insures equipment throughout the world used in every industry today. One of the responsibilities of my role in Zurich is to review, analyze, and classify losses related to the machinery and equipment used by these businesses. The analytical study of this equipment loss is a result of the accumulation of a large amount of data over time. We use this data to help forecast where, and what types of losses might occur in the future.

Such forecasts lead to risk an equipment advice that we use to help our customers reduce the risk of loss with whatever types of equipment they're using. It was this type of analysis that began to shed some light on potential effects of solar storms to some of our customers' insured equipment.

My colleague Mr. Ashutosh Riswadkar, who had already been involved with our Emerging Risk Group in 2008 and 2009 investigated the impact of solar storm threat when he approached me in late 2009 about the issue. He had some interesting things to tell me about the possible effects of solar storm, which up until that time had not been on my to-do list.

He had some interesting things to tell me about maybe some of the effects on large transformers. That's right in my ballpark. That got my

attention. Most of you attending these summits are aware of the cumulative damage that can be caused to the large transformers by the geomagnetically induced currents or GIC, brought about by coronal mass ejections. We've all heard that. We're aware of it.

Statistical analysis of transformer failures is part of my job

This study opened up a new book for us. I looked at thousands of claims. I look at thousands of claims daily. We have them in spreadsheets. That's part of my job. Every claim has a reason beside it, what caused it. None of those claims for transformers said coronal mass ejection, none of them say solar storm. They just say burned up. It's whatever the client calls in and says what it is; exploded. I've seen a picture of one that's a big fireball that somebody talked about earlier, when the oil explodes, it comes out the top. It's really pretty actually [*laughter – ed*.].

The results of Zurich's statistical survey: transformer failure rates in higher N. American latitudes "appear to follow an eleven-year cycle," and have "60% more failures than other regions."

Here are some of the areas we learned about during our research that convinced us to pay more attention to this phenomenon. Higher northern latitude areas of North America do appear to be more vulnerable to the effects of solar weather in the American continent. The average working lifetime of transformers are reported to be shorter in regions with greater geomagnetic storm activity.

I found that to be an interesting comparison. The northeastern region of the United States has the highest rates of detected geomagnetic activity. This area leads our country with sixty percent more failures in its transformers. This transformer failure rate appears to follow an eleven-year cycle. Obviously that's similar to the eleven-year solar cycle.

It may go without saying that the damages may also be due to cumulative effects of GIC on our aging electric grid infrastructure in North America. What's the problem then from a business interruption point of view; from an insurance point of view? Although utilities generally have access to spare transformers, large scale failures we know in the power grids will present serious challenges for the availability of replacement to damaged transformers, and other critical components. We've all heard that here today.

Collateral damage, and cascading failures

This may also lead to extensive collateral damage, and extended business interruption in ongoing operations in power-dependent industries, including medical, food, pharmaceuticals, healthcare, and many others. Can we say cascading failures?

Emergency power generators can help with shutdown – not with an extended power interruption

Offsite emergency power generators may help with a safe and orderly shutdown of critical operations that will be necessary for several industries but they will not be adequate for an extended interruption of power. Also I heard the term black power earlier, we talked to some of the operators in Quebec. I have people that go out and inspect this equipment. We talked to the operators. The operators in Quebec said black power, black power, that's the problem. Now they have it. When they went to be reinstalled it won't a problem if that situation occurs again.

That's only part of the picture. This is just the story of the transformers. There's more to tell here; damage to microelectronics, space, aviation, and telecommunications. We've all heard. It's a daunting list, however, with each category, with each tale of potential damage there's also a way to begin to mitigate the loss.

Zurich Insurance provides results of their analytic work to interested companies

That may be where the insurance company and risk engineer might be able to help. In fact, Zurich recently published industry-specific articles aimed at our customers that use this equipment, to provide them with some current information about the issues. We're spreading the word. Or we're trying to.

To illustrate a little further where the role of the insurance company might lie in this area, I want to conclude with a short story. It's not a story about electricity but I'll bring it back around to that. In the late 1800’s a young United States was finally getting back on its feet after a devastating inner conflict, the Civil War.

Rapidly evolving technology can bring new risks – a historical example

The states had finally started to reunite. To do that though the country needed new technology developed quickly, to help move its people and their products. Steam power became that technology. The age of steam was born and with it steam boilers, pressurized vessels. Although trains had been running with steam for some time before the war, a new era had arrived where even more powerful instruments pulled even more weight. Great steam ships moved gracefully up and down mighty rivers carrying good to and from growing cities, and farmlands gave way to manufacturing centers where large boilers supplied steam for production.

However, the new technology brought with it unintended consequences. Many lives were lost in unexpected and unanticipated explosions. In the late 1800’s a great steamship exploded on the Mississippi River, killing hundreds of soldiers and civilians alike. Sometime later in the early 1900’s, a shoe factory was completely demolished by its boiler in Massachusetts, killing dozens of women and children in the early morning hours.

Mitigation of new risks usually does take place – after multiple incidents, with serious loss of life and financial losses

The populous began to demand action. And at the same time, insurance companies that had insured these types of facilities and modes of transportation were beginning to study and learn why accidents were occurring. Two separate inspection groups began to form having common goals in mind. The main goal for both though was to stop the carnage.

In the early 1900s, the National Board of Boiler and Pressure Vessel Inspectors was formed, a group of government officials working together, dedicated to making these types of technologies safer. They reached out to the insurance companies that insured this equipment and mutual understanding was reached, that still exists.

How often do we hear about boiler explosions today? It's rare, mainly because of the message taken through education, loss prevention, and inspections that occur on a regular basis. In the case of boiler explosions, it took a number of high severity explosions and loss of life to see government and business begin to collaborate.

History seems to be repeating itself, as we wait for disaster to act

In the case of potential damages from severe solar storm, in the absence of a large number of expensive losses, we are again struggling with some inaction, possible inertia. However the threat is real. We see it. We hear of it, and it should not be ignored.

Insurance companies could be part of a proactive, public/private partnership to address this threat

The time starts evidently small steps but appear to be many. In my mind the story is one of the best examples I know where government and private enterprise worked together to solve what was a deadly problem, a problem that most people knew nothing about, which in this case is the best kind of problem. I believe a similar public/private partnership that includes insurance companies may be able to play a similar role with space weather issues discussed at this summit. Thank you very much.

Session 4, Panel 1

Panel 1: Building a Plan to e-Threat Security

Rt. Hon.

James Arbuthnot: ***U.K. Defence Committee e-Threat Report****: Recommendations*

Concurring with the Defence Secretary: *The UK recognizes EMP as so serious, it would be treated as a nuclear attack on the nation*

[…] I said yesterday that I would talk a little about the recommendations from the Defense Select Committee's report of February this year. Yesterday it was very good to hear that the Secretary of State for Defence considers that an electromagnetic pulse attack by the use of a high altitude explosion of a nuclear bomb would be considered in exactly the same way as any other nuclear attack, and would be responded to the same way.

Concurring with the Defence Secretary: *Defence spending balance now needs to shift to include e-threats*

It was also good to hear that he believes that we need to shift the balance of defence ***spending***, rather away from those pointy things that fly around shooting flames out of the back and missiles out of the front and rather more towards defending our infrastructure against the sort of attacks that as Paul Stockton said yesterday are the real threat now coming to our cyber and electronic infrastructure. That was good news.

Deterring an EMP strike is not enough

But I did disagree with his implication yesterday that deterrence was enough. Even in the short term deterrence is only a part of what we need to do. Because there are several reasons for this.

1. **Deterrence may not work.**

There are those who believe for religious reasons that they are better off dead than alive. Deterrence is not very successful against people like that.

2. **It may not work if those people also believe that we will not be able to tell where the attack came from.**

And the scenario was painted yesterday of a scud missile on a ship off the coast of Florida. I tend to think off the coast of the North Sea, but then, I would.

3. **If the consequences of deterrence failing are so catastrophic**;

We heard of the breakdown of water systems, no fuel, clogged roads, nuclear meltdown because of no water pressure to cool the reactors, no money, no communications. In fact a medieval world where there is not even the medieval infrastructure of horses, carts, and food distribution to cope with it. For us to fail to do enough to make ourselves a resilient as we could, then, it would seem almost to be a crime. It would be relatively cheap, now, to make ourselves more resilient.

4. **And in any event, there is one actor against who deterrence is bound to fail.**

That is the sun, dammit, because the sun seems to me to be impervious to our threats.

And so we need to build some form of resilience to act against the sun, even if we don't believe what many people including myself do believe, that there are malicious actors out there determined to do us harm.

We must build in resilience, and we need concurrence on how to do it

So we need to build resilience and we need therefore to agree precisely how we do it. We need to understand fully the pros and cons of hardening equipment and we need to understand fully the costs of doing that because if we just say to the government or to the private sector this is something you should do and it won't cost very much, that won't go very far. They will want specific details.

There hasn't yet, so far as I can tell, been any really good discussion of precisely how we establish those costs. It would be good to see a balanced discussion on the benefits and the disadvantages of hardening equipment. For example, does hardened equipment mean that there is a reduction in the performance of that equipment because it slows things down, and how do we persuade businesses that hardening is nevertheless worth doing because of the threats that are out there.

The different elements in the cost of hardening, the purchase of equipment, the installation of that equipment, the verification of how that hardening would work, how much it would cost, how easy it would be to operate and maintain that equipment; all of these things need to be discussed in public in order to persuade the public of what we need to do.

An integrated, national e-threat resilience plan is essential

As Jim Murphy has just said, we are only as strong as our weakest point. So is there any point in hardening bits of our infrastructure but leaving other bits that will themselves fail so make the hardened bits useless. We've got to work out precisely what it is that we do.

Here I'd like to pick up on Jim Murphy's point about cyber kitemarks, that was an interesting new line of discussion that we hadn't heard yesterday and I think that if we were able to develop similar standards across the developed world for the hardened equipment that I think we need to bring in, to do this at the beginning of this exercise would make it much easier and cheaper.

A call for increased international cooperation and coordination on e-threat protection

And talking of across the developed world, we need to get involved those countries who are not at the moment awake to these issues.

I would like to see France, for example, more involved in these discussions than they have so far been.

Actually, we need Russia and China also to be involved because they are well aware of the threats, they face similar threats.

This is an opportunity. We are in the beginning of something. Think how -- did any of you bring some of those electric plug converters to this country because of the irritating and idiosyncratic British plug system? Think how wonderful it would have been if we'd been able to get in at the beginning, across the developed world and suggested everybody have the same plug.

The Defence Committee Report concluded: the primary issue is resilience

This is really rather more serious. And it's much more vital to our wellbeing but the main point that I want to get across from the Defense Committee's report is first the issue of resilience.

Echoing the Israeli Chief Scientist's call for a Roadmap

We need, as Shlomo Wald yesterday said, we need to build a roadmap of how we move forward.

A coordinated plan is crucial – both within and between nations

Next, the issue of coherence and connectivity:

We need clear accountability and control between governments, between different departments within governments. We need to avoid people saying:

"That's not a problem of this department, that's a security issue."

The security department saying:

"That's not a problem for security, that's an electricity issue."

And everybody finally saying,

"It's somebody else's problem. We don't anyway have the money to deal with it."

Well if we don't deal with it, in my view, you soon won't have a department.

We must recognize the urgency of e-threats

But above all I think we need recognition of the urgency of the threat. We need recognition of the universal nature of the threat, the catastrophic seriousness of the threat, and then we need to build up, again as Jim Murphy was saying, a bit of awareness out in the country of quite what it is we face.

Public awareness is crucial to government action

Because my fear about government is that they tend not to act unless the public is demanding that they should act. And unless the public is aware of the sort of threats they face, they won't be going to their Member of Parliament in the surges that members of Parliament have on Friday or Saturday and saying we want you to spend less on our schools and hospitals and more on our electronic infrastructure.

Those present and represented at the summit must lead

We've got to make the public aware of these threats so that governments are forced to act. And in order to do that, we as a group here today in this room need to grasp this opportunity to lead the world in the direction that we know it needs to go.

Thank you very much.

Session 4, Panel 1

Panel 1: Building a Plan to e-Threat Security

Cong. Trent Franks: ***Introductory remarks***

Good morning to all of you. I can't tell you what it means to me to be able to continue to be with you. I have to say to you I'm a little intimidated always having to follow this man because he's got that British wit and I'm sort of a dry American. And I have to tell you though, with all my heart, I endorse every word that he spoke. I think he was right on, and I appreciate the courage that he has, given some of the political dynamics that seem apparent to me, and I just appreciate so much James, your courage.

There is growing hope for making progress in e-threat protection

I think every time that I have the opporunity to participate with a James Arbuthnot or my beloved friend Avi here, who I believe incidentally to be one of the greatest minds in America on this topic, I feel a little more encouraged that even in the face of all the political impasse that we often face, that there's some hope here of making progress.

It seems like in the political world oftentimes we get so caught up that we just don't really focus on the issues and say let's figure out what's right rather than who is right. And I'm hoping that we can somehow do that between our countries and our parties, and just the political world in general.

Infrastructure protection against EMP and blocking Iran's acquisition of nuclear weapons are my hightest national security priorities in Congress

As many of you know, I have made preparing and hardening the American infrastructure against the potentially catastrophic effects of an EMP event, and preventing Iran from gaining nuclear weapons with which they could precipitate an EMP event, my highest national security priorities in the United States Congress.

I know a lot has been said here about cyber threats. I know we've talked a lot about GMD, about geomagnetic disturbance, about the sun -- and I thought his [James Arbuthnot's] comments about the sun's politically charged proclivities and its stubbornness in the face of opposition were well taken.

There is a tendency to ignore the ultimate cyber and security threat: malcious EMP

But sometimes we, for some reason I'm not sure what it is, we have a tendency to try to eschew or avoid the whole nuclear burst that incidentally is the ultimate cyber security threat; not only does it threaten the systems themselves but it threatens the electricity with which they run. So

as we talk about cyber security we should never forget the ultimate cyber security threat is EMP itself.

My office has repeatedly found two roadblocks to getting anything done on this issue

Over the past several years during which my staff and I have been researching and advocating on this issue, we've repeatedly found essentially the same two roadblocks to getting anything done. I ask you all to grant me diplomatic immunity here in a few cases. Would you do that because I'm probably going to say some fairly straight things.

The 1st Roadblock: Lack of awareness – this is beginning to change

1. First we face the significant lack of awareness of even the existence of EMP not only among the general populous but also among the higher echelons of political class. Only a few years ago there were politicians in Washington who did not know what an EMP event even was, and fewer still took that threat seriously.

I'm encouraged that that has begun to change rather significantly and in large measure due to the efforts like Avi Schnurr and many others in this room.

Today a growing number of members of Congress are talking about EMP and several, including myself introduced legislation to help insulate our nation from the specter of an EMP event.

As Chairman of the Congressional EMP Caucus, I've hosted a number of events over the last few years to educate members of Congress and staff about the reality of EMP events. The media seems to be beginning at least to take the issue more seriously. I thought the article in *The Telegraph* was outstanding and it gives me a lot of hope because the people intrinsically get this. There's been an increasing amount of coverage in the past year or two related to both the threat of the naturally occurring and malicious EMP challenges that we face.

A wide array of government studies all concur: EMP and GMD represent catastrophic dangers and swift action is needed

At least seven national commissions and major independent U.S. studies have all independently concurred with the catastrophic danger represented by EMP [and GMD] and the necessity of taking swift measures to defend against both. Even NATO is taking notice, though surprisingly its EMP response report released in 2009 contained very few concrete proposals to defend against the threat, let alone any recommendations on preemptive measures that would be necessary to prevent an EMP attack from occurring.

The United Kingdom is beginning to take action on e-threat protection

But many nations, certainly Great Britain, are beginning to take action addressing this threat. They're beginning to talk about it and understand it.

Praise for the Defence Committee Report

And here in the House of Commons Defense Committee, under the leadership of Mr. Arbuthnot, a report was published earlier this year assessing the growing EMP threat. I applaud the committee and members and again particularly my friend James Arbuthnot for his courageous

leadership on this issue. I am confident you will all begin to aggressively pursue steps that are necessary to correct the most urgent vulnerability to EMP in your national infrastructure.

The Congressman expressed disappointment in the recent NERC GMD Report

I asked for diplomatic immunity. While I applaud the efforts of the vast majority of those responsible to consider problems like EMP, I feel honor bound to express some disappointment in a recent report by NERC in our own country that seem to appear to play down some of the challenges.

"Any effort to change our direction or our focus should be accompanied by solid, reliable, specific scientific citation, ostensibly unknown to the rest of the science community"

I know that may not have been the desire and I'm sure that's going to be addressed later today, but groups like that have a fiduciary and special responsibility to take this issue very seriously. And any efforts to change our direction or our focus should be accompanied by solid, reliable, specific scientific citation, ostensibly unknown to the rest of the science community, that would back up these assertions that seem to again play down the concern that a lot of us have. So I just have to say that and I hope that we begin to think about it together and work on that together.

The 2nd Roadblock: "An unwillingness to take our enemies at their word"

Let me go to the second roadblock that I've repeatedly encountered, it's been more challenging to overcome than a mere lack of awareness. It's the lack of willingness to take our enemies at their word.

In 1962 when both the Soviet Union and United States almost simultaneously discovered that the EMP phenomenon could be affected by detonating a nuclear warhead above the earth, there was no need to devise a completely new national strategy or security strategy to deal with a potential EMP attack. Because at that time we could still deal with our adversary through the lens of what we all know as mutual destruction deterrence.

Of course the theory of deterrence or mutual destruction not only doesn't work on some, Mr. Arbuthnot, it presupposes that our adversary is a rational actor. That process allowed us to maintain a high level of confidence that our enemy would not venture to attack if they were confident that they would endure equal or greater damage in retaliation.

As we learned on 9/11, Mutually Assured Destruction is not an effective deterrent against terrorists

9/11 is the stark reminder that Jihadist terrorists do not possess the rationality that is necessary for mutually assured destruction, for that strategy to be effective. Islamist terrorism's ideology and practice is to decapitate humanitarians with hacksaws on television while the victims scream for mercy; to cowardly hide behind women and children while launching rockets deliberately aimed and targeting innocent civilians; continually breaking treaties of peace and forcing children to blow themselves to pieces to affect the murder of other innocents. And we should not underestimate the intensity of their intent or conviction.

Terrorist ideology is epitomized by Iran's present leadership

This is a horrific ideology that's epitomized, in my opinion, in the leaders of Iran, the nation whose president today blatantly denies the Holocaust occurred and in the same breath threatens to make it happen again. All the while his nation is brazenly pursuing the means to do exactly that.

For radical terrorists, an EMP device would be an ideal, asymmetric weapon

To the radical Islamist terrorists, particularly those who believe that bringing about the downfall of American and Western powers would hasten an end-of-day scenario in which they usher in the return of this Twelfth Imam, to those individuals an EMP device would literally be their ideal asymmetric weapon.

In the words of one journalist, "An EMP weapon is one hundred percent Sharia compliant."

So consider for the moment the words of some of our enemies. President Ahmadinejad has said, "And you, for your part, if you would like to have good relations with the Iranian nation in the future, recognize the Iranian nation's greatness and bow down before the greatness of the Iranian nation, and surrender. If you do not accept to do this, the Iranian nation will later force you to surrender and bow down." The words of a lunatic or somebody who thinks he knows something the rest of us don't?

Sheik Hassan Nasrallah, the leader of Hezbollah said, "We have discovered how to get the Jews where they are most vulnerable. The Jews love life so that is what we will take from them. We will win because they love life and we love death."

These Jihadists are all such warm and happy human beings and it just touches your heart, [laughter – ed.] but the reality is we should not underestimate their hate for the West.

Iran and North Korea have already performed missile tests consistent with EMP scenarios, and are willing weapon proliferators

Moreover we must bear in mind that Iran and North Korea have all carried out tests involving high-altitude ballistic missile explosions, test modes consistent with an EMP attack. China and Russian already have both the knowledge and the wherewithal to carry out an EMP attack. All of these nations have shown themselves willing to proliferate weapons that could be used in this way in training nations that are unfriendly to the Western interests at best, and sworn enemies at worst.

North Korea has exported missile-related technology to countries such as Egypt, Iran, Libya, Pakistan, Syria, and Yemen and has secretly assisted Libya and Syria with their own nuclear programs, and continues to work with Syria, and North Korea continues to defy the Western world with its covert nuclear activities.

According to recent reports, North Korea is actively developing an EMP-enhanced nuclear bomb

There have been reports just in the last year or two that North Korea is actively developing what they say is an "EMP bomb".

Iran has become the world's primary terrorism exporter

Meanwhile, Iran itself is the world's chief exporter of terrorists, funding Jihadist terrorist groups like Hamas and Hezbollah, and sending troops, financial aid, weapons and ammunition into Iraq, Afghanistan and it's directly cost the lives of thousands of American soldiers.

"The purpose in this dialog: … the intent of our enemy is real." Iran and North Korea could become primary proliferators of EMP weapons and technology.

The purpose here in this dialog is to point out that the intent of our enemy is real and there are only two components to any threat, as far as from our enemies: their intent, and their capacity.

It should send a chill down our spines to consider that the same willingness that Iran and North Korea among others have demonstrated to proliferate missile and nuclear technology to unstable nations and to terrorist proxies would undoubtedly also become a willingness on their part to proliferate EMP weapons and technology to terrorists the world over.

Delay in hardening our infrastructure is an invitation to attack

The more we belabor about hardening our national infrastructure against an EMP attack, the more we invite Iran, North Korea, or one of the countless terrorist cells or networks they fund to exploit our vulnerability through developing and then orchestrating the use of EMP weapons to bring our civilization to its knees.

"The proglem is big enough to be seen, and small enough to be solved."

Fortunately we still live in that moment where the problem is big enough to be seen and small enough to be solved. I with all my heart believe that there's time and hope to prevent these apocalyptic scenarios that could be precipitated by a major EMP event. But that hope depends upon whether or not we take steps now to facilitate government and industry working together to harden our nation's military and our government and civilian electrical infrastructures.

Deterrence is not enough

I certainly believe that we have no alternative to hardening our grid. I would agree with Mr. Arbuthnot that deterrence is simply not enough. Our enemies know the potential of EMP and they are defiantly pursuing a means to weaponize it. While we might slow down that process through the use of counterintelligence and sanctions, we may not be able to stop the march of weapons proliferations being galvanized across the world by Islamic Jihad.

We can however make the use of an EMP weapon less appealing and much more potentially risky by mitigating the effect it would have upon our society.

The Shield Act – introduced by Congressman Franks, aimed at power grid protection against e-threats

To that end, in addition to the EMP caucus that we have in Congress, I've introduced the Shield Act in the United States Congress, which addresses our electric grid's vulnerabilities to an EMP event by establishing procedures intended to safely hibernate and insulate the grid from attack. More importantly, by providing hardware-based solutions to protect the grid.

Hardware-basedsolutions are an essential component of a solution

It's my belief that hardware-based solutions are absolutely critical as a component to any true solution.

Working together, ladies and gentlemen, we can implement policies like the Shield Act across the free world, and I would just look forward to the day in the not too distant future where we all

might gather to survey our progress in a group like this and conclude that conferences of this type and urgency on this subject are no longer necessary.

I thank you all for your commitment. Let us continue to work together. Thank you.

Session 4, Panel 1

Panel 1: Building a Plan to e-Threat Security

Avi Schnurr: ***Introductory remarks***

Thank you James.

Let me echo Congressman Franks' remarks with a slight addition. If Congressman Franks found it difficult to speak after James than I have to say I find it doubly difficult to speak after two such powerful speakers. Thank you very much for your remarks.

I want to talk this morning about ideas, toward building a path toward e-threat security, but I'd like to begin by thinking a bit about where we've been, before I talk about where I would recommend we go.

If you'll bear with me for a moment, I'd like to expand a bit on the discussions that have occurred on what has been done, what are the reports that have been published. Let me just take a couple of minutes to expand that list a bit, because I think it's appropriate.

I'm going to mention just government studies, not all of the studies.

- There of course was the **U.S. Congressional EMP Commission Report** and there were two of these reports.
- There was the **U.S. Congressional Strategic Posture Commission [Report]**.
- Currently we have an ongoing set of efforts by the White House Office of Science and Technology Policy [**Interagency] Working Group on GMD**.
- The Department of Energy working together with NERC published their **High-Impact Low Frequency** study a few years back.
- The U.S. Congressional Research Service published an **EMP and High-Power Microwave Threat Report.**
- **The U.S. Army Corp. of Engineers has an EMP Protection Report** that they have published that they work with.
- **The U.S. Department of Defense Science Board** published an **EMP and Nuclear Effects Study** rather recently, that addresses these issues in a military context.
- The **Oak Ridge National Laboratory** worked on a study that was sponsored and coordinated with **FERC, Department of Energy, Department of Homeland Security**.

- The **Department of Defense Strategic Command** has what I would call a full, ongoing library, a massive **library of studies** which they continue to build addressing a set of issues for EMP protection of installations, and other systems.
- Of course we have the **NASA / National Academy of Sciences Study**.
- We have the **Parliamentary Defense Committee Report and Study** that was discussed this morning from the Defense Committee here by James Arbuthnot.
- We have in the United Kingdom also the **National Risk of Civil Emergencies or National Risk Assessment Report**.
- We have the very recent **FERC GMD Staff Technical Conference**.

Given the remarkable, long list of studies, it is time to move on

I know this is a boring, annoying list, but this is remarkable, and I could have gone on. These are just recent government studies. There is a massive body of work. This is where we're coming from and I submit it is really time to make the decision that additional analysis, while appropriate and helpful, is not the only thing we should be doing at this point.

We all concur on one key point: In addition to more analysis, let's begin now to make progress on power grid protection

I think there's really no question, and I doubt that there's anyone in this room who would disagree with a simple key point; the time has come now to begin to look at all the previous body of work that has been done and begin in addition to additional analysis finding a way to make actual progress. So I think that's a key point and I recommend it be given some consideration.

Ordinary citizens cannot understand why protective work has not begun

Now when I go through this list with ordinary people who may not be so expert in this domain, I really don't get anywhere the end of the list. At some point they stop me and they say:

"Okay I get it, I understand. We're talking about a threat which sits somewhere between extremely bad and totally catastrophic, so obviously the government is dealing with this, right?"

Then they look at me with this kind of hopeful expression.

I had a conversation like this Saturday night, actually here in London, with someone who had no previous experience. We had about a three minute discussion, and that was where it went to.

Trying, and failing to explain government inaction against a catastrophic risk

I struggled to answer. How am I going to explain nothing's really happened here in the United Kingdom, in the United States and in any of the other twenty-one countries who are represented here today.

It's difficult. I can try to find a way but it is quite difficult to explain it's embedded in the political process and the fact that responsibility is diffused, as you have pointed out today, James.

The real challenge – a deficit of imagination. Government action to protect against a threat with no recent precedent is rare

But it's really difficult to understand. When I look at this and when I look at the scope of the devastating threat that we're talking about, what I have to say is that perhaps Reto Schneider yesterday, where are you Reto -- perhaps Reto you put it best when you spoke about a deficit of imagination.

We're very good in governments at looking at problems that have happened many times, usually one time is not enough, but three or four or five times with a devastating problem, that's usually enough to begin to recognize that action is necessary.

But to take action on a problem, even a problem as catastrophic as this one, which has never been experienced, is almost unprecedented in history. I don't know if a single example in history could be found.

That's the challenge. Because of all of the different kinds of catastrophic issues and problems that people talk about that we have experienced in all of our nations, this is completely unique.

Because if it is anywhere between very bad and completely catastrophic, experiencing it even a single time would be too much for us to deal with. We have to find a way to build our imagination, our ability to project and understand in advance what this threat is, and find simple ways to at least *begin* to deal with it.

It is unacceptable to put the continuity of our nations at risk

Let me put a period behind that point and let me say it this way.

In my view, it is intolerable, and it is unacceptable, to risk the health and the wellbeing of the United Kingdom, the United States, of any of the nations that are represented here, our other friends and allies.

It is intolerable to risk the continuity of our nations as we know them today for a threat which has been so well anchored that it took me about two or three minutes just to list the reports.

To-date, unfortunately, little has been done

If there were already actions moving forward, if we were already in a position to say there is a process going forward, let's just continue it, I don't think it would be necessary to make that point. But unfortunately we still haven't gotten to the point where there is movement actually in the governments of our various countries to get this done.

I think there are positive signs. I think many of the things I've heard at this summit suggest that maybe at last we're starting to move forward, and I think the commitment of many of the very senior people who are here reflect that. I am hopeful.

Recommendations on next steps

Let me finish with a few very brief comments on where I think we should go more specifically.

some no-regrets steps, and start moving forward to actually get this done.

- ***GMD Protection: Verifiable standards with teeth, driving specific changes***

In terms of GMD protection, clearly we need good standards. We need broad and meaningful standards, and standards that will drive both design and hardware. Depending on how we decide and how governments decide to set up those standards, I think there's a range of flexibility, but if the standards do not really identify verifiable and specific means to go forward and protect our infrastructure, then I think we will have taken a very valuable opportunity and potentially trampled on it.

I recommend that we don't do that. Let's take the opportunity and do it properly and if we do come up with standards, let's make sure they are solid, that they are verifiable, that they have adequate flexibility to deal with varying circumstances, but that they have the specificity and the teeth to actually accomplish what they need to accomplish.

Analysis vs action: Redressing the balance

There is always a question of balance. And I would like to portray very briefly a balance that I think deserves a bit of attention in this domain as well, and that's the balance between analysis and action, putting in place protective action and protective means.

Many people have talked about the fact that we need more data collection, we need more analysis, and I add to my voice to theirs; it is essential. It is critical.

Given the hundreds of different transformer designs in the U.S. fleet, trying to reach perfect understanding is an impossible – and unecesary - task

But when we look at the difficulty and complexity of the analysis and the difficulty and complexity of getting comprehensive data collection over the hundreds of different designs of transformers for example, we must ask ourselves: Is the balance set properly today between analysis and data gathering, and beginning to take actions which could protect some of our critical facilities.

Let's begin taking no-regrets actions

What I submit is that that balance needs to be redressed and in addition to additional analysis, in additional to additional data collection, we need to begin in parallel taking some, as Commissioner LaFleur said, some no-regrets actions, some no-regrets steps, and start moving forward to actually get this done.

- ***Malicious EMP Protection***

"Likelihood" is the wrong question

In terms of EMP, Congressman Franks spoke about that in some detail. I echo his remarks. I think what's important to say here is that when one looks at – as many people have talked about -- what should we do in regard to EMP, one of the questions that is frequently asked is what is the likelihood. I submit to you that in my view the question of likelihood is really the wrong question.

The real question is "vulneraiblty."

When it comes to a malicious act the question is vulnerability.

If you look in history – and I challenge the historians, and I know there are some historians in this august group -- if you look to history and looked for even a single case where an important vulnerability of a major nation in history was exposed .. and not exploited at some point by its enemies, I don't think you will find even a single case.

I would be happy to be proven wrong.

New vulnerabilities start at low likelihood. Then they grow, fast, to become primary strategies.

The likelihood today is low. Why is the likelihood low? Because this is a new vulnerability as our infrastructures have evolved. What one finds when one looks at major new vulnerabilities is they have a way of moving very quickly to center stage, and our enemies have a way of exploiting them.

If in fact the indications that we have heard this morning and certainly yesterday and in other forums, if the indications that there are solid and available means which are minimal in cost are in fact correct, and that it should be possible to begin protecting ourselves against both space weather issues and nuclear or non-nuclear EMP concerns, then I would recommend we get on with it.

If the costs are low, if the only issue is organizational, is the issue of finding ways to get past all the management challenges of the fact that there really is no electromagnetic threat protection department in any of our countries yet, then let's find a way to do that. Because I think the cost and the alternatives of not doing so will simply be unacceptable.

Some thoughts on reward and punishment

In closing let me say simply this.

I will make you a promise from my perspective, especially to the very senior leaders who are here and once again thank you so much for coming.

The reward

If you do everything that you can from your perspective and in your domain to begin working on this and addressing this problem, the reward will be that here in the United Kingdom the pubs will continue to be open, it will be possible to go to the Red Lion and have a pint three years, five years, fifteen years from now.

In the United States it will be possible twenty years from now to go and enjoy a baseball game. Thirty, fifty years from now your children and grandchildren will enjoy baseball. These will be the rewards.

I can also guarantee you, to quote Liam Fox, […] that even after you're dead, you will never be rewarded with public acclaim. That's not going to happen. But I think the reward that I just outlined is much greater.

The punishment

Let me also say the reverse. If we here today, and there is really -- as James said yesterday -- no one else to turn to. […]If we do not take the responsibility to get past all the procedural and structural and organizational differences and find ways to work together to make this happen internationally and within our countries, then someday everyone will know that there were opportunities, and this was one of them.

They will go back and they will see the results and what we accomplished here. And they will be able to identify [and say], as they go through the witch hunt,

"We have found some of the people we can blame."

In my view, that's not the right motivation. I don't think negative motivation is really very useful but I do think it has to be said.

The 2013 summit: April 8th and 9th, the Capital Building, Washington D.C.

I would go for the positive direction. I think today we have a tremendous opportunity.

And let me put something new on the table. About a year from now, […] on April 8th and 9th, Washington, D.C. we will have the 4th Electric Infrastructure Security Summit.

It will be bigger, it will be greater, and at that event I challenge all of you to bring very serious, very concrete progress that we can talk about and can congratulate ourselves about in this domain.

Thank you very much.

Session 4, Panel 2

Panel 2: The Role of Regulatory Policy

Gerry Cauley: Thank you Chairman Arbuthnot, and certainly very pleased to be here. This is my second version of this summit and I can see a lot of progress in the development of understanding of the risks and also of the understanding of actions going forward.

Focusing on specific actions

My purpose this morning would be to outline some specific actions I think we can take that are practical and cost effective with regard to addressing the GMD issue. First off I want to start by reminding everybody of who NERC is. In North America we have a unified power grid between Canada, the United States, and a small portion of the Baja of Mexico, so it was necessary to manage that reliability effectively, to have an international electric reliability organization. NERC is that organization. We were appointed within the United States by the Federal Energy Regulatory Commission with whom we work very closely as the ERO of the United States. We have similar relationships with each of the provinces in Canada.

One thing I gather from the two conferences, last year and this year, is a growing knowledge and understanding of the risks associated with solar magnetic disturbances. I think Avi listed some of the reports and some of them on EMP and some of them on GMD.

NERC did issue a report earlier this year and the purpose of the report was really to focus on the GMD issue as one that is know is an actual risk facing us now, that we know we've seen occurrences in the past. We know we'll see occurrences in the future, and to understand those risks.

One of the points I'd like to make about this, we have a lot of risks within the power grid operations and planning, and many of them have been around for many years. We understand them. We have storms; we have ice storms, snow storms, earthquakes, and tornadoes. Those fall into a category of risks that we experience frequently enough. We know how the system behaves and we know how to respond. We're just now beginning to understand some of the risks associated with EMP and with GMD, but I think our knowledge of those risks is growing.

The purpose of the NERC GMD Report

The purpose of the NERC report was to look at GMD in particular and our intent was to gather experts from industry, from the vendors, from government and internationally as well to try to get the best knowledge of what we think the response of the power grid would be to a significant solar magnetic disturbance. The result of that analysis I think aligns very closely with what we've seen in history; is that a GMD event is very chaotic. I think one of the presenters yesterday talked about instability and chaos. It's not a well-defined, well-constructed event.

GMD leads to voltage instabilities

It does create instabilities, both within the earth's magnetic fields, and then the currents we see in the power system, and it's a very complex phenomenon that we see. The result of our study showed that the system would see voltage impacts, absorption of reactive to the point where we would get into instability and a very strong likelihood of system collapse. This is consistent with

the event that we saw in March of 1989, and it's consistent with other events that have occurred in history.

GMD also leads to voltage equipment damage

That does not diminish the importance of considering equipment damage, particularly transformer damage, and our report highlights that. We do need to be concerned, particularly about certain equipment, that might be of an older vintage, and particular designs of equipment, that might be more susceptible. I think our report, collectively with the other historical reports, indicate sort of the range and diversity of the risk and nature of the risks, that it's complex. Our understanding is emerging.

NERC's Role includes understanding, as well as standards and compliannce

NERC's role is -- one of the tools we have is to do standards and to enforce compliance with this standards. But I look at our role as much broader than that. Our role really is to understand risks to catastrophic failures, instability of the grid and cascading failures of the grid. We look at really all hazards. Some of them I mentioned, some of the traditional ones, and also emerging ones such as cyber security.

Our role really is to characterize and shape these risks in a way that we understand them, and we can resolve a solution or approaches to go after those risks. A lot has been said at this conference about the risk of EMP, both a nuclear blast and hand-held or truck-mounted types of EMP as well as GMD. I think one thing that I hear consistently of all the speakers, this morning and yesterday with regard to nuclear blast-type EMP, is that the science and the technology and the understanding of that type of an event is known, and it's understood. It's demonstrable. We know it can be real.

The challenge for EMP of a nuclear-blast type is really how do we resolve that problem. I equate that to some extent to a nuclear attack on a nation. The question is whose decision is that? How do we deal with that? There are a of policy decisions way above my pay grade that could come into play. There are military options, there are deterrence options. A nuclear blast over a nation impacts not just the power grid but communications, banking, everything we know in society. It would really be a world game changer.

The question is where does that decision get made, where do those policies get made? To me that is an issue of national defense, and I think for that reason we have chosen at our working level to focus on the things that are in front of us that we know and understand and that have occurred in the past and we expect will occur again in the future. So we focus our energy on GMD at this point to -- as a problem that we believe that we can solve and have an impact.

I also think that some of the actions that I will outline specifically provide an opportunity with regard to potentially hardening of some equipment, or other procedural type improvements that will have a benefit both for GMD and EMP type events.

How do we proceed forward? First of all a framework. Several mentions have been made of standards or regulatory approaches. I firmly believe that the best approach is to have a partnership between government and industry to understand the problem. If it was a well-defined mature problem and a mature risk set then I think we might be in a different position where a more directive approach might be appropriate. But I think we're looking at really exploring and moving forward at the same time; learning and moving forward at the same time.

A partnership approach to look at a roadmap, with timelines

I would propose within the United States they approach that I would suggest would be a partnership between the Department of Energy, the Federal Energy Regulatory Commission, and NERC working with industry to put forth a very specific detailed roadmap with deliverables and timelines for those, and measuring of progress. I think that's what the public who we serve would be interested in seeing; government and industry working together to provide safe, and reliable electricity that -- and we've dealt with some of these threats and risks.

A 15 point plan

My fifteen-point plan, to my chagrin -- it's awful when you come up with fifteen, but I think some of them are related so I think if somebody spent some more time with it this could probably be collapsed to ten. I'm looking at things we can do in the next year, things we could do over the next two to three years, and things we can do in the next five years. So very specific actions I would suggest that we take on, and hopefully we'll be able to come back to the summit next year and report the progress on these.

First of all we should initially identify the facilities in the power grid that are most at risk from a GMD event. I would suggest that this model is effective not just in the United States and Canada but could be internationally adopted as well.

First of all, where are our weakest vulnerability points in terms of equipment? What near-term mitigations that we need to take which would include potentially modification, upgrades, operational procedures, but do we know where the problems are, the weak spots and what would we do about that.

Second, we should conduct interconnection wide, system wide studies of the behavior of the GMD currents and voltage response, what kind of reactor power loss would we see, and essentially do some wide-area interconnection studies.

Third we should do an assessment of our current inventory of spare equipment and this would have to be done with recognition of the need for confidentiality because of the secure nature of the information about the spares and where they are, and the usefulness that bad guys might find with that information. But I think we could build off of the industry's current spare equipment program and figure out how many there are, where are they, what are their capabilities, and also leverage off of NERC's database.

Fourth would be to work with vendors in the near term to enhance the GMD withstand requirements of transformers and other equipment, and include within that specification additional instrumentation that we need to measure the impacts of GMD events on equipment.

Fifth, I would continue to enhance the training of system operators and planners to know that they under different conditions and levels of alert they would know what actions they should be taking.

Sixth, we should work between industry and government and I think an enlightenment I had yesterday was working with the insurance industry as well. We should work to identify what are the design basis events that we're looking for. We've heard talk of 100 year storms, 200 year storms, the fact is this physical phenomena is statistical. It's not a clean definition of what a hundred year storm is. It's different geographically but I think we could enhance our

understanding by determining what are the design basis storms to which we should work. We could work with NASA and the Canadian Space Agency.

Seventh, we should begin comprehensive testing and forensics of transformers to understand what aspect of the transformer breakdown and aging is related to GMD and electromagnetic disturbances, versus simple aging of insulation and breakdown and aging of transformer. I think I would complement that one by saying this should be an opportunity to work with vendors to do some perhaps destructive testing of transformer equipment to understand the withstand capability and what the behaviors are under extreme conditions.

Eighth, I think we've heard this multiple times; we need to increase the number of ground-induced current monitors, looking at the current in the earth, but I would add to that the ability to monitor concurrently the flows of current and impacts on the equipment so that we can see the correlation between earth currents and equipment currents, and not just in DC/AC or harmonics and other impacts in terms of the behavior of a system relative to the earth. And that will take data and data concentrators where we can pull the data together into a common base or location where we can have access to do study. I would propose either through confidentiality or anonymity of the source of the data, that this data could actually be made publicly available to research institutes and universalities to help us understand the behavior of the earth and the power grid.

Ninth, we need to get in the hands of power system planners and operators tools they need to make this an everyday part of their system planning and design, so that they can treat this just as another part of building and operating a system.

Tenth, outside of NERC's responsibility out but an important one is the continued development and improvement of space weather forecasting. We're a big fan of the support of NASA and others who provide us the data for alerts, but it needs to be developed to another level.

Eleventh, I think in the longer term we would look at developing solar magnetic disturbance withstand and capability as a regular part of the planning aspect of system planning and operations. I think at some point eventually once we better understand the characteristics of system response, characteristics of the equipment, and we have the measurements to support that, it would be appropriate at some point to include GMD capabilities within NERC's operating and planning standards.

Twelfth, I mentioned earlier spare equipment assessment, like what do we have and where are they in capabilities. But I would add the twelfth as really what is our spare equipment strategy? I've heard some great ideas at the conference and previously about taking aged equipment that's going to be retiring and repurposing it for spares or being creative about developing a more robust set of spares. I think the recovery transformer that has been researched and developed by ABB in collaboration with industry is an important project to continue developing.

Thirteenth, develop longer term equipment standards with the IEEE and the IEC in terms of the design and provision of equipment.

Fourteenth, we need to look at expanding our reactive resources and making sure we have sufficient reactive resources and equipment on the system.

Fifteenth, is a catch-all, very broad area of strategy which looks at Commissioner LaFleur's comment yesterday about how much would be invested in infrastructure in the coming decades, that we need to have a purposeful strategy of building in cyber security and GMD and withstand capability within the system from the beginning.

This list is not the end-all list, but it provides some practical measures

I would close there. I think those are not the end-all list but a list of practical things that I view sort of straddling between industry and government as practical measures that are consistent with Commissioner LaFleur's no-regrets and do-no-harm approach, but show progress. I hope to come back in a future year and be able to discuss some of the progress we've made on this. Thank you.

Session 4, Panel 2

Panel 2: The Role of Regulatory Policy

Miles Keogh: Folks thanks for having me here. It is a great and slightly intimidating pleasure to speak to you from up here. I'm Miles Keogh. I advise the state public utility commissions of the fifty United States and the District of Columbia in the U.S. It's a little-known discrepancy between how the United States organizes its electrical system and how the rest of the world does, wherein we have federal authority that's well represented by Commissioner LaFleur, and Joe and our colleagues from the FERC, but also in each of the states the rates, terms and conditions of things like retail rates, infrastructure siting, and other kinds of long-term planning activities are actually accomplished state-by-state among the state governments, the State Public Utility Commission is who I advise.

Unfortunately Commissioner Lib Fleming with her lovely southern accent and extreme gravitas was not able to make it so I'm going to try and compress her thoughts and my thoughts into a great ball of a presentation. I know that you guys are all really wondering what's this guy doing up here, you're all waiting to see Gerry and Joe duke it out and I'm sort of the person in the middle holding up the rounds card here. Why are we letting me up here?

The role of state regulators

It's the old song about the bank robber who's asked why he robs banks; because that's where the money is. Setting the rates, terms and conditions at the state commissions is a function of if the improvements that we want to see done are to be successful, the case has to be made to the state regulators in the United States, that the investments are prudent.

So I'm not up here trying to tell you guys we're going to say you can't have your money. I'm simply identifying that this is an audience that you're going to need to work with and to engage in this process.

A new NARUC e-threat exercise is planned for this summer

We've been trying to engage in this process to different degrees. I participate as a member of NERC's Severe Impact Resiliency Task Force on the writing team. We've had several activities and educational things on EMP and GMD for our regulators. On July 22nd we're going to be doing a fishbowl game, similar to a tabletop exercise, but we're going to be engaging several of the people here, including Avi and Chris Beck and some other folks to engage with that.

Most state utility commissions are now beginning to get questions on EMP and GMD risks.

No rate cases have been requested

On a state-by-state basis I did a little informal poll while we had about thirty-five states respond to me on this, we have several states who came back and said they've been hearing, in public hearings and in interactions with rate payers, questions and concerns on EMP and GMD, and several states came back saying that they have staffers who monitor space weather conditions and who have actively sought education in this arena.

None of the states came back saying that they had any interaction with any of the companies and a specific filing case docket or proceeding regarding anything to do with EMP or GMD. Which makes me think either that the investments that are being made in this and the exploration that's being made in this is being done as part of the standard operations and maintenance spending done by the utilities or it's not. It's not coming out through commissions. That's simply a piece of "anecdata" for you, hopefully useful.

Recommendations

As far as what we should do, I think one of the great things about going near the end is that several folks have provided some great recommendations.

[…] But let me just throw out a couple of ideas about what actual progress could potentially look like.

One of the questions that came up yesterday was,

"Do we not spend more on actual discussion of this, commissions of investigation, and exploration, than we do on actually implementing solutions?"

I don't want to say that that's misguided, but I think it's extremely important to identify a strategy and a course, at least incrementally before taking action overwhelmingly. We can't allow a poor early action to undermine effective long-term action.

The state commissions can be part of the dialogue

I really offer myself and my members to participate in the development of a strategic direction forward. That doesn't mean we shouldn't act, I think Commissioner LaFleur spoke very well yesterday identifying that incremental actions as we find out what the right things to do are, we should, with all due haste take those actions.

Investing a very small piece of an estimated $Trillion power grid investment in the coming decades

I think we can time it well with existing investments and planned investments. My friends on Wall Street tell me we're looking at 1.85 trillion dollars spent just in the United States on electric system capitalization between now and 2030, of which about 800 billion of it is going to be on distribution and transmission system investments.

Surely in that, if we can find places where a nickel of prevention is going to supersede a dollar of retrofit, then I think that asking those questions about how we can harmonize those investments now fits well within the scope of prudence.

As we're trying to devise a strategy for moving forward, I think a collaborative model is emerging more and more in the electric sector in the United States. We used to talk about how we had dispatchable resources and forecastable load but now load or demand wants to be a demand resource and wants to get dispatched, and now a lot of the dispatchable resources are nondispatchable. The more and more areas we're finding that the bright line of jurisdiction that was guided by that forecastable load and dispatchable resources is blurring.

I think in a lot of ways we've come to a place where, confronted with problems that can't be solved without collaborative decision making, [… there are a number of] strategies that we

put together where we've partnered up with other federal and state colleagues in order to explore difficult issues, develop strategies for moving forward, and then start implementing them.

I think those are good models, and I think we should absolutely really harness those and drive them with great fury towards an improvement of our posture in this area.

Taking clear vulnerabilities off the table with cost effective investment

I will say this; a few years ago, three years ago or thereabouts, when I started talking about this with our commissioners, trying to help them understand is EMP and GMD […] a real thing or is this not a real thing. […] I don't think it's imprudent to take clear vulnerabilities off the table if it can be done in a cost-effective way.

Just to give some context; what sounds extremely expensive in a context outside of the electric grid improvements may not actually be as expensive in the context of electric grid improvements.

Between 2010 and 2012 the electric utilities were spending ten billion dollars a year in new transmission. The states collectively pay about 700 million dollars a year into a nuclear waste fund for which we get nothing. These are serious numbers that we're talking about in terms of what we need to spend to improve our posture here, but in the context of the electric system, especially if intelligently and prudently done, I think they may not be as big as they sound in the context that we're looking at.

A call for a growing, ongoing education process

Let me just conclude by saying one of the key pieces of success here is going to be the ongoing engagement and let's call it education of decision makers who matter. The average tenure of a State Public Service Commissioner is two and a half years. That's pretty short. The staff tend to stay on for a long time, but there's an ongoing requirement for new education for the folks who are going to decide if the utilities will get their money for these investments or not, and I think that generally speaking the political tenure of decision makers like state governors, state legislators, and even FERC commissioners, there's enough turnover there where intelligent and careful education of those decision makers is really going to be a worthwhile investment, as you engage them in these collaborative processes.

Again, the worst thing we can do is make bad decisions, ill informed decisions at the outset that undermine effective action over the long term.

With that, I'd really like to thank Avi, Congressman, Member of Parliament and all of you for your time, allowing me to participate and again on behalf of Lib Fleming, her apologies for not being able to join us today. Thank you.