Vulnerability to Space Weather, Manmade EMP & Cyber Attack

Summary

Solar super storms

It is predicted by NASA and by the NOAA that the Sun may be entering a particularly energetic period (*similar to that in which the most powerful solar storm ever recorded occurred*), with very energetic solar storms happening every couple of months instead of years, with activity peeking around 2013-2014. Scientists are already talking about the likelihood of solar "black swan event" in 2012. The risks posed by space weather are known and significant, a severe event could potentially have serious impacts upon infrastructure and society. The UK National Security Strategy identifies space weather as a Tier 1 risk, the highest of identified "priority risks." Under the worse case scenario, large areas of the Earth could be without electricity for long periods, possibly several months, with high loss of life. Countries, and areas, with "fragile" grid infrastructures are likely to be affected most - smart grid electronics may introduce additional vulnerabilities to exposed grids. The use of Smart Meters instead of analogue meters may also increase risk, as they are more likely to be damaged by solar events.

Practicality, Security, War, Terrorist or Cyber-Attack

It is recognised that if countries fail to implement suitable measures to protect themselves against electronic attack they leave themselves open to extreme danger.

Manmade EMP Events

High-Altitude Electromagnetic Pulse (HEMP)

The term HEMP is often used for EM signals created from a nuclear detonation interacting with the Earth's upper atmosphere. There are already nations possessing the capability to use HEMP devices to cause catastrophic results to critical infrastructures over wide geographical areas. Smart grid components are more prone to damage from HEMP than the parts of the system they replace. HEMP may seriously damage solid-state Smart Meters. The US National Security Working Group notes *"… vintage type electronic systems are much more robust and tolerant to EMP effects. The bad news is that these systems are growing old and … will be replaced with modern versions that are inherently more vulnerable to EMP."*

Non-Nuclear EMP (NNEMP) / Intentional Electromagnetic Interference (IEMI)

Extremely powerful portable radio transmitters (which may be mobile and coordinated) can be built to create NNEMP. Its effects are similar to solar threats and HEMP but are usually more localised. As noted by Radasky, "*… the IEMI threat to Smart Meters, distribution electronics, substation electronics, substation communications, control rooms and power generating facilities (including wind and solar facilities) is the same as for … HEMP.*" This vulnerability needs to be urgently addressed. There is presently no protection for Smart Meters against EMP. Even simple EMP devices such as a coil of wire and a battery at close range can disable them.

Preventing Natural and Manmade EMP Catastrophes

Smart grids create more potential points of failure from EMP than traditional grids. Ideally, protective no cost / low cost measures should be considered early in the brief and applied before rollout. Action is required sooner rather than later and could create numerous beneficial opportunities. As noted by Arbuthnot et al., "*The technology to protect critical infrastructures from natural or malicious electromagnetic threats now exists. Implementation costs are estimated at less than 0.01% of GNP."*

Cyber Security

The UK National Security Council recognises cyber-attacks as a Tier One threat. It has already been claimed that hackers from foreign countries have reconnoitered the US electricity grid possibly seeking to discover exploitable systemic vulnerabilities such as those found in present Smart Meter systems. Smart Meters can create substantial new cyber-vulnerabilities. As noted by Anderson & Fuloria, one of the gravest of these is that of "*a 'cyber-nuke'* [through the Smart Meters] *that would reduce* … [a country's] *population to destitution. Recovery from such an attack would be painful* [loss of life may also be high – present author's comment]*."* This risk does not exist with analogue meters.

Conclusion – the design of power grids, meter systems and electrical appliances needs to be rapidly rethought to deal with the real life issues that have been raised.

Vulnerability to Space Weather, Manmade EMP & Cyber Attack

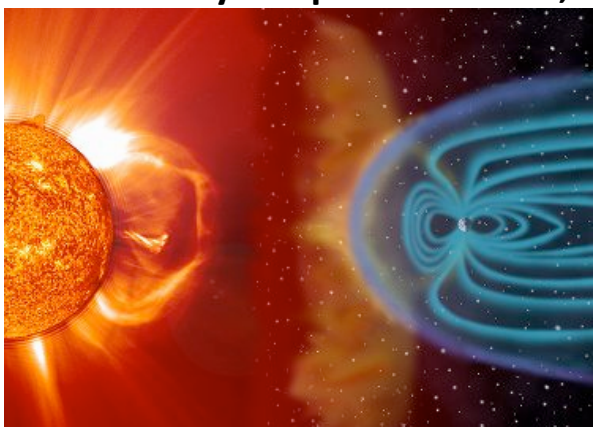


Image source: Courtesy US National Oceanic and Atmospheric Administration (NOAA).

Present Risk from Space Weather

"*The risks posed by space weather are known and significant, … a severe event could potentially have serious impacts upon … infrastructure and society more widely. It is essential that this hazard is sufficiently recognised and addressed by the Government and relevant civil bodies*" … The UK National Security Strategy (NSS) identifies space weather as a Tier 1 risk, the highest of identified "priority risks" (UK House of Commons Defence Committee 2012).

"*Smart Grid electronics may introduce additional vulnerabilities if the grid is exposed to [electromagnetic pulse (EMP)] threats … "* (Radasky 2011). The electromagnetic pulses created by solar storms – and manmade EMP events - can greatly compromise the integrity of electrical grids and damage electrical equipment and satellites. Smart Meters, as they are currently designed, are more vulnerable to such threats than the analogue meters they replace and will, at present, introduce further potential points of failure into the system.

In the USA, Dr Peter Vincent Pry, former Director of the US Nuclear Strategy Forum and President of EMPact America, states "*… given our current state of unpreparedness, within 12 months of an EMP event, about two-thirds of the U.S. total population… would perish from starvation, disease and societal collapse*" (Pry 2011). US Center for Security Policy President Frank Gaffney Jr. (former US Deputy Assistant Secretary of Defense for Nuclear Forces and Arms Control Policy), says such an event could cause 9 out of 10 deaths within a year from such factors (Gaffney Jr. 2011). No figures on potential losses appear available for the UK, Europe, or other areas of the planet.

Space Weather

"*Modern society depends on high-tech systems such as smart power grids, GPS, and satellite communications - all of which are vulnerable to solar storms*" (NASA 2011). "*It is … vitally important that the work of hardening … infrastructure is begun now and carried out as a matter of urgency*" (UK House of Commons Defence Committee 2012). This will require a major rethink on how Smart Grids and their components are designed and deployed. It is imperative that Smart Meters (and smart appliances) do not further increase such vulnerability.

Solar Super Storms

It is predicted by some scientists that the Sun's 11-year cycle will hit its maximum in late 2013 or early 2014. According to NASA and the US National Oceanic and Atmospheric Administration (NOAA), the Sun may be entering a particularly vicious solar maximum in 2013, similar to that in which the Solar Super Storm of 1859 (*the most powerful solar storm ever recorded*) occurred (Moskowitz 2011, NASA 2010, US NRC 2008). Phillip Chamberlin of NASA's Solar Dynamics Observatory said that there could be very energetic solar storms "*every couple of months instead of years*" during that time (Mosher 2011). According Riley (2012), there is an approximate 1 in 8 chance that a solar storm of equal magnitude to the 1859 event could cause devastating disruption to electric power transmission networks within the next decade. Such an occurrence could also result in significant (and preventable) loss of life (Pry 2011, Gaffney Jr. 2011).

Scientists are already talking about the likelihood of "*a black swan event*" in 2012 due to increased solar activity (Telegraph 2012). According to Dr Richard Fischer (Hough 2010), director of NASA's Heliophysics Division, the next solar storm of such a magnitude hitting Earth "*will disrupt communication devices such as satellites* [including those used for some smart grid communications – present author's comment] *and car navigations, air travel, the banking system, our computers, everything that is electronic. It will cause major problems for the world."* Such storms are already a major threat to less vulnerable (non 'smart') grid systems (Birnbach 2011). The risk of such events and their potentially detrimental effects on society, is far higher than other matters normally taken into account in risk planning.

John Kappenman (NRC 2008) modeled the potential effect of exposure to a storm of similar magnitude to the great solar storm of May 1921 on the modern US power grid and calculated that over 300 large EHV transformers would be at risk of permanent damage. Marusek (2007) claims that a solar super storm aimed earthwards could cause long-term blackouts in the USA, Canada, Europe and elsewhere. The UK's National Grid recognise that in the event of a severe solar storm, long-term blackouts of at least two months could arise for individual damaged transformers being restored or replaced. The probability of a disconnection event under such circumstances is presently foreseen as being 62% for England and Wales and 91% for Great Britain as a whole (UK House of Commons Defence Committee 2012). The possibility of multiple solar EMP events happening over an extended period of time that might damage repaired/replaced transformers does not appear to have been taken into consideration, nor does the additional time / labour force that could be required to replace Smart Meters damaged by the solar EMPs.

Avi Schnurr, Chair and CEO of the US Electronic Infrastructure Security Council, suggests that shorter individual power transmission lines (as found in the UK) may be at greatest risk of solar EMP. To back his case, he mentioned that detailed modeling in the US has indicated that densely concentrated sectors of the (US) grid were more at risk from solar EMP, and that for European power grids (of similar design to those in the UK), very large geomagnetically induced currents (GICs) had been noted for comparatively minor storm events. Whilst this is at odds with evidence presented by the UK's National Grid (UK House of Commons Defence Committee 2012), Schnurr's comments appear worth taking into consideration as the stakes are so high.

Satellites and spacecraft such as ACE, GOES, SOHO and the STEREO craft provide the main information required for forecasting solar storms. There is a risk that at least some of these may fail. Apparently, scientists are "*keeping their fingers crossed*" that the elderly Advanced Composition Explorer (ACE) and Solar & Heliospheric Observatory (SOHO) satellites are able to keep transmitting data on solar storms. "*ACE is particularly important as it sits at the L1 point, a million miles from Earth, and is able to detect the polarity of incoming Coronal Mass Ejections (CMEs). ACE was launched in 1997 for an operational mission of three years. … Crucially, it is a single point of failure in our ability to forecast Space Weather*" (UK House of Commons Defence Committee 2012).

According to Michael Hesse, Director of the Modeling Center at the Goddard Space Flight Center, as quoted by Kerr (2009), these satellites "*can fail any time, no one knows."* It was further noted by Kerr (2009) that "*One-third of major [solar] storms arrive unheralded and almost one-quarter of the warnings turn out to be false alarms…*" It was additionally noted in written evidence from the UK National Grid that "*CMEs can take from 18 hours to three days to reach Earth. Forecasting models are used to decide on their trajectory and timing. NASA issue forecasts of arrival time giving a six hour window. However these forecasts are frequently inaccurate, with the actual arrival being many hours early or over a day late.*" Present UK protective measures are "*based to a large extent on pre-emptive action, such as shutting down equipment as a precaution*, …" (UK House of Commons Defence Committee 2012). As this is the case, it appears that forecasts may fail to provide adequate warnings.

It is predicted that upcoming solar flares could greatly endanger National Security and may take down key services such as electricity grids, electronics and communications for prolonged periods. It appears imperative that countries protect their power grids to the best degree possible against such events. At best, such an event could cause individuals to be without electricity for hours or days. Under the worse case scenario, large areas of the Earth would be without electricity for longer periods, possibly several

months. Countries, and areas, with "*fragile*" grid infrastructures are likely to be affected most. The UK House of Commons Defence Committee (2012) state that it is "*vital that the … electrical grid is as resilient as possible to potential threats such as these. … Government departments … must work with National Grid to ensure that its backup procedures and equipment are sufficient to meet the reasonable worst-case scenario for a severe space weather event*. "

The present author contends that backup plans should also take into account the possibility that it may be necessary to deal with several severe space weather events over an extended high-risk period and that additional components that are sensitive to EMP should be avoided where possible. The present design of many high-tech devices (including Smart Meters) makes them more vulnerable to EMP effects than the units and technologies they replace. Transformer designs could also be improved (Birnbach 2011, EMPrimus 2011). There is also a need to ensure that generic civil contingency plans that "*address blackouts and temporary loss of electronic infrastructure caused by a range of events*" are improved, as at present they are inadequate (UK House of Commons Defence Committee 2012).

The estimated worldwide economic cost in the first year alone after such an extreme event is $1 trillion to $2 trillion. "*Even a recurrence of the lesser super-storm of May 1921 could lead to blackouts affecting 130 million Americans and half of North America*" Kerr (2009). Russia and China have already been hardening their grids against such risk (Pierobon 2011).

According to Connor (2011), the US and UK are planning to undertake "controlled" power cuts to their national electricity supplies to protect them against potential damage from large solar storms that might otherwise take months or even years to repair. However, such "controlled" power cuts can only take place if warnings are given in time and, as noted above, this is not always possible. The 1859 event, the most powerful solar storm ever recorded *(which is considered to be 10 times greater in magnitude than anything observed in the last 50 years)*, caused shorting in the telegraph systems in North America and Europe, creating electric shocks and numerous fires (Odenwald 2000). Nowadays the effects would be far more damaging and widespread due to the increased use of electricity and more complex technology and components, including Smart Meters, that are more easily damaged by EMP.

With a possible lack of accurate forecasting, and overstretched staff, there is the real chance that there will be insufficient warning time for effective mitigative actions to be taken on some occasions when solar storms present danger, thereby further increasing grid vulnerability. As an example of the possible suddenness of events that might occur, during the huge solar storm of 1989 in Canada operating conditions in Quebec went from normal *"to complete Provence wide blackout in an elapsed time of 92 seconds*" (Horizon 2012). For the space weather warnings that do come through before the event, it is noted in the report by the UK House of Commons Defence Committee (2012), that for some events there may be two or three days warning and with others there may be only eight minutes notification.

The effects that the electromagnetic pulses (EMP) of solar super storms would have on Smart Meters, smart grids and smart technologies have yet to be fully assessed. The International Electrotechnical Commission (IEC) does not yet have immunity tests covering the effects of solar storms on Smart Meters (Radasky 2011). It is known however that they are less robust to EMP threats than analogue meters, and that the wireless telecommunications systems that many of them operate through could be damaged by the late-time (E3) portion of High-altitude Electromagnetic Pulses (HEMP) from nuclear detonations, which exhibit strong similarities (in terms of spatial distribution and time variation) to the GIC of extreme solar storm events (Radasky et al. 2001).

Solar Storm of 1989

The geomagnetically induced currents (GICs) that the solar storm of 1989 created caused the overloading of circuits, tripping of breakers, and (in severe cases) even melted the windings on heavy-duty transformers (NASA 2010). Transformers were damaged in the USA, Canada and the UK. Satellites were also damaged – this latter fact is mentioned as some smart grids use satellites for communication which might get damaged (and even potentially fall out of orbit) as a result of future solar storms. Microwave relays too (as used in smart grid communications) are also vulnerable to damage, as are the control chips of smart technologies.

Generator step-up transformer damaged by March 1989 solar storm.
Images: Kappenman (2011). Images originally provided courtesy of Public Service Electric and Gas and Peter Balma.

The March 1989 event was of considerably lesser strength than the 1859 event (a disturbance storm time (Dst) value of -589 nT was registered in 1989 compared to a Dst of -1760 nT for the 1859 event (Lakhina et al. 2005). [The Dst index is a measure of geomagnetic activity used to assess the severity of magnetic storms. It is expressed in nanoteslas and based on the average value of the horizontal component of the Earth's magnetic field measured hourly at four near-equatorial geomagnetic observatories. *A negative value is shown when the Earth's magnetic field is weakened*].

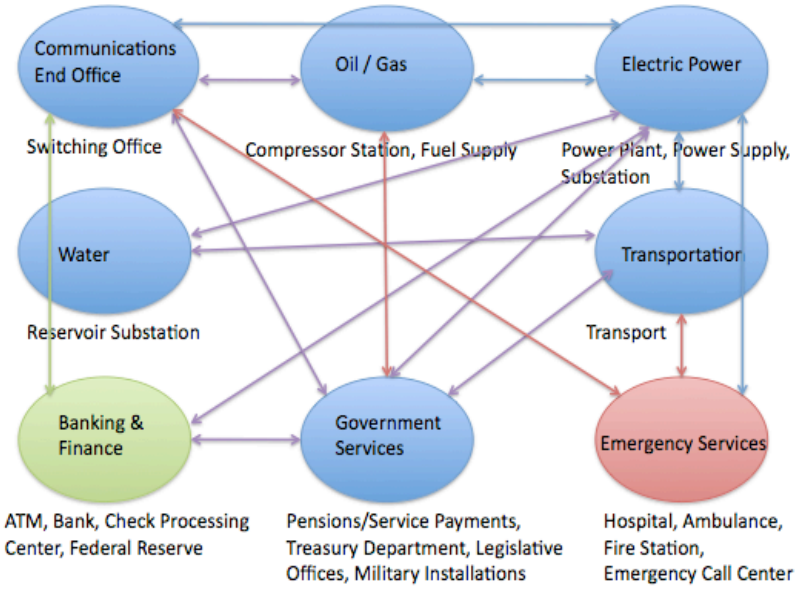
Fortuitously, that solar storm hit in the middle of the night: if it had hit during peak load conditions, grid closure may have cascaded into the USA (Riswadkar & Dobbins 2010). It caused over 200 power anomalies in North America. These included (as previously mentioned) the blackout of the province of Québec in Canada due to a voltage depression that could not be mitigated by automated compensation equipment); melting of power transformers in New Jersey (including the failure of a transformer at a Nuclear Power Plant); voltage swings at major substations; and generators tripping and going out of service (US NRC 2008).

A utility firm placing a top priority order for the replacement of a damaged generator step-up transformer as a result of the 1989 event was told it would take almost 2 years to fulfill [at present there is a 3-year lead time for orders to be fulfilled (which could be greatly extended in future) if orders for replacements were high – *comment by present author*]. Luckily, a spare was available which was installed within 6 weeks (Marusek 2007). Within 25 months of the March 1989 storm, 12 Nuclear Plants had transformer incidents that were suspected as being delayed failures caused by that storm (Kappenman 2011). The direct cost of the March 1989 solar storm was over $2 billion [£1.245 billion]. The cost of protecting key areas of the US grid against EMP would be $150 million [£94 million] (Riswadkar & Dobbins 2010). The costs could be substantially greater for smart grids as a result of their additional electronics introducing increased potential EMP vulnerabilities into grid systems (Radasky 2011). Measures to reduce risk are already being put in place by governments to secure their "*critical electric infrastructures*" (EIS 2011, 2010).

Solar storms of equal, or greater, magnitude to that of the 1989 solar storm have occurred in 1859, 1872, 1882, 1903, 1909, 1921, 1928, 1938, 1958, 1989 (Gonzalez et al. 2011). Other solar flares of similar or greater magnitude to that experienced in the March 1989 solar storm have occurred in 2001, 2003, 2005, 2011 and 2012 (NASA 2012, 2012a, 2012b).

It appears more cost-effective to create robust EMP protected smart grids and electrical equipment now than to have to do so in retrospect. Solar events are not particularly rare (and the risk from manmade EMP, as discussed later in this document, is rising). Research now indicates that large GICs are also possible at low-latitudes as well as at high latitudes (Kappenman 2011). It appears that utility grids will need to be protected against both solar EMP and manmade EMP to comply with the International Infrastructure Security Roadmap. It is proposed that such matters should be urgently addressed.

Sensitivity to Geomagnetic Storms



The economy is sensitive to geomagnetic storms due to a network of interdependencies. [Adapted from original graphic by US Department of Homeland Security].

The US National Research Council (NRC 2008) states, "*Because of the interconnectedness of critical infrastructures in modern society, the impacts of severe space weather events can go beyond disruption of existing technical systems and lead to short-term as well as to long-term collateral socioeconomic disruptions*." As noted by Arbuthnot et al., (2010), "*There is limited time to upgrade national electric grids to avoid solar flare-induced, global scale burn out*." Unfortunately such time is quickly running out with much still remaining to be done. The consequences of such an event, or series of events, should they occur, could be dire as the effects could cascade through other systems dependent, either directly or indirectly on electricity. It is therefore vital that utility grids and meters are as robust as possible to try to withstand such potential threats.

Distribution of drinkable water could be greatly compromised by a severe solar storm, as could cooking and food refrigeration facilities, fuel supply, heating, lighting, Internet and telephone communications, sewage disposal and transport (fuel pumps require electricity to work). Banking, government, medical treatments and emergency services could also be affected to various degrees. "*The longer the outage, the more problematic, and uncertainty-fraught the recovery will be*" (Foster Jr. et al. 2004). The effects of a solar super storm(s), as predicted for 2012/2013/2014, could take many years to correct and severely damage national economies. There is no room for complacency.

UK Government Expert Opinion

The UK Government is aware of the threat of solar storms and has already taken various contingency measures, including allowing some transformers to be switched off if necessary (Connor 2011). The UK Government's chief scientific adviser, when speaking at the annual meeting of the American Association for the Advancement of Science (AAAS) in Washington DC in 2011, further noted that solar storms could cause catastrophic damage to the world's economy. "*The potential vulnerability of our systems [to space weather] has increased dramatically. Whether it's the smart grid in our electricity systems or the ubiquitous use of GPS*." Professor Sir John Beddington (Brewster 2011).

Similar concerns were raised by The Right Honourable Liam Fox MP, when he was UK Defence Secretary, when he warned that with our heavier reliance on technology our way of life is now more at threat from such solar events than ever before (EIS 2010). To help address this matter an assessment of space weather was carried out for The UK's National Risk Register of Civil Emergencies (UK House of Commons Defence Committee 2012), this noted that the relative likelihood of severe space weather within the next 5 years was between 1 in 2 and 1 in 20 (UK Cabinet Office 2012).

Whilst severe solar storms occur infrequently, they have the potential to create catastrophic long duration impacts on electricity supply and end users (US NRC 2008). Less severe storms can also cause significant damage. As Smart Meters are more vulnerable to stray high-energy electrical fields than the units they replace, and it appears that they may be more vulnerable to severe space weather, retaining (and reinstalling) analogue meters might be worth considering for these reasons alone.

"*Severe space weather can cause disruption to a range of technologies and infrastructure, including communications systems, electronic circuits and power grids*" (UK Cabinet Office 2012). Erinmez et al., (2002) noted that whilst the power transmission systems of UK's National Grid are "*generally designed to operate reliably under challenges mainly related to terrestrial weather conditions … the measures* [used to increase their] *robustness have also made transmission systems more vulnerable to the risk of space weather through geomagnetic storm activity*."

US Expert Opinion

In similar vein to Professor Beddington, Jane Lubchenco, Head of the National Oceanic and Atmospheric Administration (NOAA), is on record as having said at the American Association for the Advancement of Science (AAAS) 2011 meeting that the US also needs to be better prepared than at present to avoid loss of electrical power and communications as a result of solar flares. She stated that "*This is not a matter of if, it's simply a matter of when and how big. We have every reason to expect we're going to be seeing more* [potentially harmful] *space weather in the coming years, and it behooves us to be smart and to be prepared*."

"*Many things we take for granted today are so much more prone to the effects of space weather than was the case during the last maximum*," Lubchenco declared (Moskowitz 2011a). The challenge faced may increase as the World is likely to become more 'technologically dependent' as it edges towards 2013 and other periods of solar maxima – *it appears wise to start 'future proofing' technology now and industry needs help from governments to do so*. As noted by Tom Bogdan, Director of the US Space Weather Prediction Center, "*What's at stake are the advanced technologies that underlie virtually every aspect of our lives*." He also mentioned that forthcoming individual solar events could be particularly powerful (Lovett 2011).

These comments echo the earlier thoughts of John Kappenman at the 2008 US National Research Council workshop on the societal and economic impacts of severe space weather events (US NRC, 2008). He additionally noted that lack of preparedness could result in "*significant societal impacts and with economic costs that could be measurable in the several-trillion-dollars-per-year range*."

Seven months after that meeting, NASA found a giant breach in the Earth's protective shield (Phillips 2008) that will dramatically increase the impact of solar storms discussed in the report above – *comment by present author*.

Need for Robust Power Grid Solutions to Space Weather

Since 1989, development of open access on transmission systems has encouraged the transport of large amounts of energy across grid infrastructures to benefit economic returns by delivering less expensive energy to areas on demand. That rationalisation, however, taken alongside the increased likelihood of multiple equipment failures from solar events (and manmade EMP events) has increased the risk of collateral damage – *sophisticated items, such as Smart Meters (and satellites used for smart grids), are more likely to be damaged by such events than the equipment they replace*. *Smart appliances too may be more easily damaged than their conventional counterparts.*

The vulnerabilities of electric grids to EMP events are now being addressed in the USA by the US National Security Working Group (NSWG 2011). Also in February 2011, US Congressman Trent Franks proposed for federal legislation the H.R. 668 SHIELD Act (Secure High-voltage Infrastructure for Electricity from Lethal Damage Act), "*to amend the Federal Power Act to protect the bulk-power system and electric infrastructure … against natural and manmade electromagnetic pulse (`EMP') threats and vulnerabilities,"* (Franks 2011). Further support for increasing the robustness of smart grid systems worldwide – as related to EMP risk – beyond what is already being achieved might prove appropriate?

Riswadkar & Dobbins (2010) propose the hardening of system and critical assets through installing circuits or passive devices to prevent, or reduce, geomagnetically induced currents (GICs) flowing into electrical grids. Both aging transformers & grid infrastructure and smart grids create mitigation challenges. The risk of solar flares to the low orbiting satellites that can be used for smart grid data transference also has to be taken into consideration, these too should be hardened, as X-class flares, which are on the increase till 2013 (Moskowitz 2011a), can cause their orbital decay.

Some locations where it is presently proposed that Smart Meters will be installed are more vulnerable than others. In particular, electrical grids are at greater risk from the effects of geomagnetic activity in areas where igneous rock (such as granite) is present (Odenwald 2009). [The high resistance of such rock encourages geomagnetically induced currents (GICs) to course through power lines situated above them raising risk of damage].

Shielding just 10% of critical infrastructure could reduce anticipated damage from EMP events considerably (The Sage Policy Group, 2007). The author of this present document suggests that, as it is possible that more than one solar super storm may inflict damage during this period, ideally protection levels should be 'As High As Reasonably Achievable' (AHARA). Uncharted territory is being entered into where the intensity of a severe space weather event might even exceed that of the 1859 Carrington Event and lesser severe space weather events (in comparison) may also arise that may cause considerable damage and loss of life.

As noted by Professor Sir John Beddington, the UK Government's chief scientific adviser, "*The risk we face from solar events] is slightly scary, and I think properly so. … We've got to be scared by these events otherwise we will not take them seriously*" (Moskowitz 2011a).

Many of the precautions taken to protect smart grids and technology from natural EMP events will also help protect them / reduce the potential impact from manmade EMP events by rogue nations and terrorists.

References

Birnbach, C. (2011), Understanding the problem: Nuclear and Non-Nuclear EMP. Presentation given at The 2nd Annual World Summit on Infrastructure Security, Washington D.C.

Brewster, T. (2011), Professor Sir John Beddington says governments need to get ready for some serious solar storms. ITPro News, http://www.itpro.co.uk/631306/government-advisor-warns-of-solar-storm-disaster

Connor, S. (2011), 'Controlled' power cuts likely as Sun storm threatens national grid. The Independent, 13 June 2011, http://www.independent.co.uk/news/science/controlled-power-cuts-likely-as-sun-storm-threatens-national-grid-2296748.html

EIS (2011), EIS Summit: International Infrastructure Security Roadmap, Electric Infrastructure Security Summit - The Capitol Building, US Congress, Washington D.C., 11 April 2011.

EIS (2010), EIS Summit Summary Report, Report: The First World Infrastructure Security Summit, Electric Infrastructure Security Summit - London, 20 September 2010, Westminster Hall, Parliament, UK.

EMPrimus (2011), Grid and transformer protection, http://www.emprimus.com

Erinmez, I.A. et al. (2002), "Management of the Geomagnetically Induced Current Risks on the National Grid Company's Electric Power Transmission System", Journal of Atmospheric and Solar Terrestrial Physics, 64, pp. 743–756. Special Addition for NATO Space Weather Hazards Conference, 2000.

Foster Jr., J.S. et al., (2004), Commission to Assess the Threat to the United States from Electromagnetic Pulse Attack, Volume 1: Executive Report, 59 pp.

Franks, T. (2011), Secure High-voltage Infrastructure for Electricity from Lethal Damage Act' or the SHIELD Act', H.R. 668, http://www.empactamerica.org/HR668_SHIELD_Act.pdf

Gonzalez, W.D. et al. (2011), Extreme geomagnetic storms, recent Gleissberg cycles and space era-superintense storms, Journal of Atmospheric and Solar-Terrestrial Physics, 73, pp. 1447-1453.

Horizon (2012), Solar Storms - The Threat to Planet Earth. Television program first broadcast on BBC HD, 6th March 2012, British Broadcasting Corporation, UK).

Hough, A. (2010), NASA warns solar flares from 'huge space storm' will cause devastation, The

Telegraph, 14 June 2010, http://www.telegraph.co.uk/science/space/7819201/Nasa-warns-solar-flares-from-huge-space-storm-will-cause-devastation.html
Kappenman, J.G. (2011), Severe Solar Activity/Space Weather and the Global Threat to Electric Grids. Presentation given at The 2nd Annual World Summit on Infrastructure Security, Washington D.C.
Kerr, R.A. (2009), Space Weather Forecasting Are We Ready for the Next Solar Maximum? No Way, Say Scientists, Science, 324, pp. 1640-1641.
Lakhina, G.S. et al. (2005), Research on Historical Records of Geomagnetic Storms. In: Proceedings IAU Symposium No. 226, International Astronomical Union, Dere, K.P. et al. (Eds).
Lovett, R.A. (2011), What If the Biggest Solar Storm on Record Happened Today?: Repeat of 1859 Carrington Event would devastate modern world, experts say. National Geographic News, 2 March 2011, http://news.nationalgeographic.com/news/2011/03/110302-solar-flares-sun-storms-earth-danger-carrington-event-science/
Marusek, J.A. (2007) Solar Storm Threat Analysis, Impact. 29pp.
Mosher, D. (2011), Solar Flare Sparks Biggest Eruption Ever Seen on Sun: Enormous ejection of particles into space shocks scientists. Daily News, National Geographic, 8 June 2011, http://news.nationalgeographic.com/news/2011/06/110608-solar-flare-sun-science-space/
Moskowitz, C. (2011), Sun erupts with mightiest solar flare in 4 years: Explosion hurls massive wave of charged particles into space, toward Earth, http://www.msnbc.msn.com/id/41604785/ns/technology_and_science-space/t/sun-erupts-mightiest-solar-flare-years/
Moskowitz, C. (2011a), U.S. Must Take Space Storm Threat Seriously, Experts Warn, http://www.sott.net/articles/show/224561-U-S-Must-Take-Space-Storm-Threat-Seriously-Experts-Warn
NASA (2012) , Hotshot, Biggest Solar X-Ray Flare on Record, http://sohowww.nascom.nasa.gov/hotshots/X17/
NASA (2012a), Hotshot x 17.2 and 10.2 flares!, http://sohowww.nascom.nasa.gov/hotshots/2003_10_28/
NASA (2012b), Second Biggest Flare of the Solar Cycle, http://www.nasa.gov/mission_pages/sunearth/news/News030712-X5-4.html
NASA (2011), Getting Ready for the Next Big Solar Storm, http://science.nasa.gov/science-news/science-at-nasa/2011/22jun_swef2011/
NASA (2010), Solar Shield – Protecting the North American Power Grid, http://science.nasa.gov/science-news/science-at-nasa/2010/26oct_solarshield/
NASA (2009), New Solar Cycle Prediction, Science News, NASA Science, http://science.nasa.gov/science-news/science-at-nasa/2009/29may_noaaprediction/
NOAA/SEC (1999), NOAA/SEC Satellite Working Group, April 1999,
http://www.swpc.noaa.gov/sww/sww99/WGReports.html
NRC (2008), Severe Space Weather Events - Understanding Societal and Economic Impacts: A Workshop Report, National Research Council of the National Academies, The National Academies Press, 141 pp.
NRR (2010), National Risk Register 2010, http://interim.cabinetoffice.gov.uk/media/349003/nrr2010-chapter2.pdf
NSWG (2011), National Security Working Group, Weekly National Security Working Group Update, Republican Study Committee
http://rsc.jordan.house.gov/UploadedFiles/NSGW_041311_Update.pdf
Odenwald, S. (2000), The 23rd Cycle: Learning to live with a stormy star, Columbia University Press, http://www.solarstorms.org/S23rdCycle.html
Odenwald, S. (2009), The Day the Sun Brought Darkness. NASA News & Features, http://www.nasa.gov/topics/earth/features/sun_darkness.html
Phillips, T. (2008), Giant breach in Earth's magnetic field discovered, NASA Science, Science News, http://science.nasa.gov/science-news/science-at-nasa/2008/16dec_giantbreach/
Pierobon, J. (2011), Smart Grids may make U.S. more vulnerable to electromagnetic pulses from solar flares or a terrorist attack, http://theenergyfix.com/2011/08/15/smart-grids-may-make-u-s-more-vulnerable-to-electromagnetic-pulses-from-solar-flares-or-a-terrorist-attack/
Radasky, W. & Savage, E. (2010), Intentional Electromagnetic Interference (IEMI) and Its Impact on the U.S. Power Grid. Report prepared by Metatech Corporation for Oak Ridge National Laboratory. 53 pp.
Radasky, W.A. et al. (2001), Nuclear and Space Weather Effects on the Electric Power Infrastructure, NBC Report Fall/Winter 2001, pp. 37-42.

Riley, P. (2012), On the probability of occurrence of extreme space weather events, Space Weather: The International Journal of Research and Applications, 10, S02012, 12 pp.

Riswadkar, A.V. & Dobbins B. (2010), Solar Storms: Protecting your operations against the Sun's 'dark side', Zurich Services Corporation, 12 pp.

Telegraph (2012), Solar flares could cause "as much devastation as a tsunami", The Telegraph, http://www.telegraph.co.uk/earth/earthnews/9131396/Solar-flares-could-cause-as-much-devastation-as-a-tsunami.html

The Sage Policy Group (2007), Initial Economic Assessment of Electromagnetic Pulse (EMP) Impact upon the Baltimore-Washington-Richmond Region, The Sage Policy Group, http://www.pti.org/docs-safety/EMPecon_9-07.pdf

UK Cabinet Office (2012), National Risk Register, Cabinet Office, 58 pp. http://www.cabinetoffice.gov.uk/resource-library/national-risk-register

UK House of Commons Defence Committee (2012), Developing Threats: Electro-Magnetic Pulses (EMP), Tenth Report of Session 2010–12. Report, together with formal minutes, oral and written evidence. HC 1552, The Stationery Office Limited, London.

US NRC (2008), Severe Space Weather Events - Understanding Societal and Economic Impacts, http://books.nap.edu/catalog.php?record_id=12507

Practicality, Security, War, Terrorist or Cyber-Attack

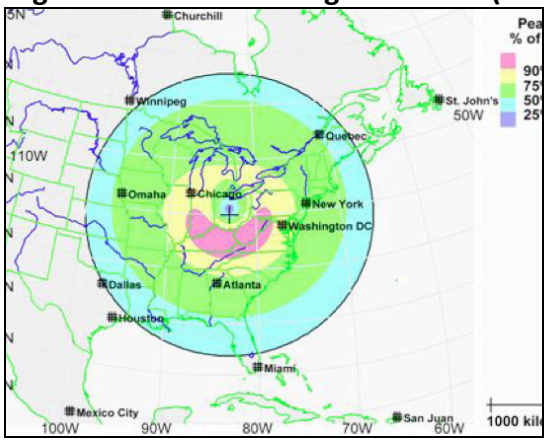
"*If the world's industrial countries fail to devise effective ways to defend themselves against dangerous electronic assaults then they will disintegrate within a few years*" UK House of Commons Defence Committee (2012).

If EMP vulnerabilities remain unaddressed they will present increased invitations for attack (Graham et al. 2011). It appears prudent to reduce such risks wherever practical rather than adding to them by inappropriate design, component and/or operation specification. Sleep walking into the future could rapidly lead to nightmare scenarios.

As noted by William R. Graham, Chairman of the US Commission to Assess the Threat to the United States from Electromagnetic Pulse Attack, "*A serious national commitment to address the threat of an EMP … can lead to a national posture that would significantly reduce the payoff for such an attack …*"

Manmade EMP Events

High-Altitude Electromagnetic Pulse (HEMP)



Source: Kappenman (2011).

"*Several potential adversaries have or can acquire the capability to attack the United States with a high-altitude nuclear weapon-generated electromagnetic pulse (EMP). A determined adversary can achieve an EMP attack capability without having a high level of sophistication. EMP is one of a small number of threats that can hold our society at risk of catastrophic consequences. EMP will cover the wide geographic region within line of sight to the nuclear weapon. It has the capability to produce significant damage to critical infrastructures and thus to the very fabric of US society, as well as to the ability of the United States and Western nations to project influence and military power*." Commission to Assess the Threat to the United States from Electromagnetic Pulse Attack (Foster Jr. et al. 2004).

The term HEMP is often used for EM signals created from a nuclear detonation interacting with the Earth's upper atmosphere. EMP can cause "temporary upset and even catastrophic failure to modern electronics and electrical systems over considerable geographic areas of the Earth" (NATO 2011).

HEMP Components

HEMP Type	Intensity	Time to reach intensity
E1	50,000 V/m	≤ 10 ns
E2	100 V/m	1 microsecond - 1 second
E3	40 V/km	1 - several hundred seconds

Source: Radasky (2011).

E1 and E3 HEMP are indicated as being the greatest threat to power systems. As noted by Radasky (2011), "*as more Smart Grid electronics are placed in substations, these E1 HEMP fields become a significant concern to their performance. Also the placement of new Smart Grid communication antennas and electronics in substations should consider the threat of E1 HEMP. … E1 HEMP will also*

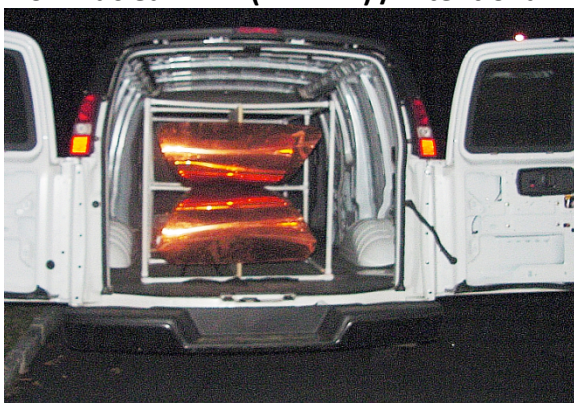
couple efficiently to aboveground medium and low voltage power lines that are typical for the distribution grid and also to the low voltage drop lines to homes or businesses." Burial of distribution line reduces EMP risk – and can also provide additional health benefits (comment by present author).

Radasky (2011), also notes that for "*the shorter drop lines to homes, levels on the order of several hundred kV are possible that could seriously damage solid-state Smart Meters*." Additionally, it is often seen as impracticable to protect wireless systems (such as used in Smart Meter systems – *present author's comment*) against EMP attack. The US National Security Working Group (NSWG 2011), notes "*… vintage type electronic systems are much more robust and tolerant to EMP effects. The bad news is that these systems are growing old and must be replaced, and they will be replaced with modern versions that are inherently more vulnerable to EMP."*

Source Region Electromagnetic Pulse (SREMP)

These are caused as a result of nuclear detonation, such as can be created by an air-burst EMP cruise missile, interacting with the Earth's and its adjacent atmosphere. A single SREMP event could cause irreparable damage to most electronics within a 30 km (18.6 mile) area (Powerwatch 2010). Power supplies for large areas of a smart grid could be easily disabled by such devices unless suitable precautions are taken - *as a matter of best practice Smart Meters should be designed to fail in a "supply on" mode.* The vulnerability of electronic Smart Meters to such events appears far greater than that of the electromechanical rotating-disk meters they are designed to replace which are unlikely to be damaged by such events.

Non-Nuclear EMP (NNEMP) / Intentional Electromagnetic Interference (IEMI)



NNEMP Level EMP Source. Source: Kappenman (2011).

Non-Nuclear EMP (NNEMP) is also known as Intentional Electromagnetic Interference (IEMI) and is labeled as the "*Intentional malicious generation of electromagnetic energy introducing noise or signals into electric and electronic systems, … disrupting, confusing or damaging these systems for terrorist or criminal purposes*," (IEC 2005).

Extremely powerful portable radio transmitters (*which can be mobile and coordinated*) can be built to create NNEMP. Its effects are similar to solar threats and HEMP but are usually more localised, unless a coordinated attack is undertaken (where they could create effects far larger than those achievable by large nuclear EMP pulses). The additional electronics used to create smart grids and related smart technologies, including Smart Meters, may increase system vulnerability. As noted by Radasky (2011), "*… the IEMI threat to Smart Meters, distribution electronics, substation electronics, substation communications, control rooms and power generating facilities (including wind and solar facilities) is the same as for the E1 HEMP.*" This matter needs to be urgently addressed.

NNEMP/IEMI present a comparable risk scenario likelihood to that of Cyber Attack (Kappenman 2011). They pose a serious threat to medium and high voltage transformers and smart grids. Technical solutions are being created to address such threats (Birnbach 2011, Radasky & Savage 2010), but do not yet appear to have been applied to Smart Meters.

Close Range EMP

"*There is no protection on a smart meter against a EMP (Electro Magnetic Pulse) which could be as simple as a coil of wire and a battery at close range. It could blow the electronics in the meter or simply change memory bits which might change the rate figures or readings. It could also trigger the electric cut off circuit and allow burglars to cut your power even if your breaker box is locked*" (Electron 2011).

Power Surges

A recent sustained power surge in California appears to further indicate the increased susceptibility of Smart Meters to such events compared to the conventional analogue meters they replace (Dremann 2011). In that incident 80 PG&E SmartMeters caught fire and burned out after the power surge, causing some residents and utilities officials to question their safety. The surge, which lasted 80 minutes, affected 200 homes and businesses. None of the analogue meters were affected.

"*The idea with SmartMeters is to make the customers' and the utility's life better, but this is a good example of how sometimes the old way is the good way,*" Debbie Katz, spokesperson for Palo Alto utilities. Katz further commented that the advantage of the analogue meter over its intended 'smart' replacement is that it does not have internal electronics which can be shut down or disrupted by power surges (Dremann 2011). At that time Paolo Alto city officials were seeking to undertake additional research and investigative work to ensure Smart Meter shortfalls and glitches were resolved before investing further in them. On 21st February 2012 Palo Alto Municipal Utility District decided to reject Smart Meter deployment at the present time. It is the 50th Californian local government body to do so (OTLB 2012).

Measures should be taken to ensure that Smart Meters, if deployed, are robust enough to withstand the technical challenges documented above – *present author's comment*.

References

Anderson, R. & Fuloria, S. (2010), On the security economics of electricity metering, 9th Workshop on the Economics of Information Security, Harvard University, George Mason University in Arlington, VA, June 2010, 18 pp.

Birnbach, C. (2011), Understanding the problem: Nuclear and Non-Nuclear EMP. Presentation given at The 2nd Annual World Summit on Infrastructure Security, Washington D.C.

Dremann, S. (2011), Power surge raises questions about SmartMeters: East Palo Alto electricity surge burnt out digital meters, Palo Alto Online News, http://www.paloaltoonline.com/news/show_story.php?id=22378

EIS (2010), EIS Summit Summary Report, Electric Infrastructure Security Summit, 20 September 2010, Westminster Hall, Parliament, UK.

Electron (2011), Could Hackers Break into Your Electric Meter? Scientific American Article, TechLuck - Green Energy Forum, http://techluck.com/cgi-bin/YaBB.pl?action=print;num=1316581337

Foster Jr., J.S. et al., (2004), Commission to Assess the Threat to the United States from Electromagnetic Pulse Attack, Volume 1: Executive Report, 59 pp.

Gaffney Jr., F.J. (2011), Gaffney: EMP Attack on US Means 9 Out of 10 Dead Within 12 Months, http://mrctv.org/videos/gaffney-emp-attack-us-means-9-out-10-dead-within-12-months

Graham, W.R. et al. (2011), Commission to Assess the Threat from High Altitude Electromagnetic Pulse (EMP): Overview. Presentation given at The 2nd Annual World Summit on Infrastructure Security, Washington D.C.

IEC (2005), International Standard IEC 61000-2-13 ed1.0, Electromagnetic compatibility (EMC) - Part 2-13: Environment - High Power Electromagnetic (HPEM) Environments - Radiated and Conducted, International Electrotechnical Commission, Switzerland. Quoted by Koepke (2010).

Kappenman, J.G. (2011), An Overview of ElectroMagnetic Threats to Electric Grids – Space Weather, EMP & IEMI. Round Table presentation given at The 2nd Annual World Summit on Infrastructure Security, Washington D.C.

Koepke, G. (2010), Highlights of Connectivity Week 2010: EMC and Smart Grid, http://www.emcs.org/acstrial/newsletters/summer10/EMCStandards.html

NATO (2011), Electrical and Electromagnetic Environmental Conditions: AECTP-250 Edition 2, Allied Environmental Conditions and Test Publication, NATO International Staff, Defence Investment

Division.
NSWG (2011), National Security Working Group, Weekly National Security Working Group Update, Republican Study Committee, http://rsc.jordan.house.gov/UploadedFiles/NSGW_041311_Update.pdf
OTLB (2012), Palo Alto Municipal Utility District Rejects Smart Meters — Now Fifty Local Governments in California Say No http://stopsmartmeters.org/2012/02/22/palo-alto-municipal-utility-district-rejects-smart-meters-now-fifty-local-governments-in-california-say-no/
Powerwatch (2010), Smart Meters - smart idea - not so smart implementation http://www.powerwatch.org.uk/news/20101018_smart_meter.asp
Pry, P.V. (2011), Dr. Peter Vincent Pry President, EMPact America Statement Before The Congressional Caucus On EMP The Capitol Room HVC 200 February 15, 2011, http://www.empactamerica.org/pry-statement-to-emp-caucus.pdf
Radasky, W. & Savage, E. (2010), Intentional Electromagnetic Interference (IEMI) and Its Impact on the U.S. Power Grid. Report prepared by Metatech Corporation for Oak Ridge National Laboratory. 53 pp.
UK House of Commons Defence Committee (2012), Developing Threats: Electro-Magnetic Pulses (EMP), Tenth Report of Session 2010–12. Report, together with formal minutes, oral and written evidence. HC 1552, The Stationery Office Limited, London.

Preventing Natural and Manmade EMP Catastrophes

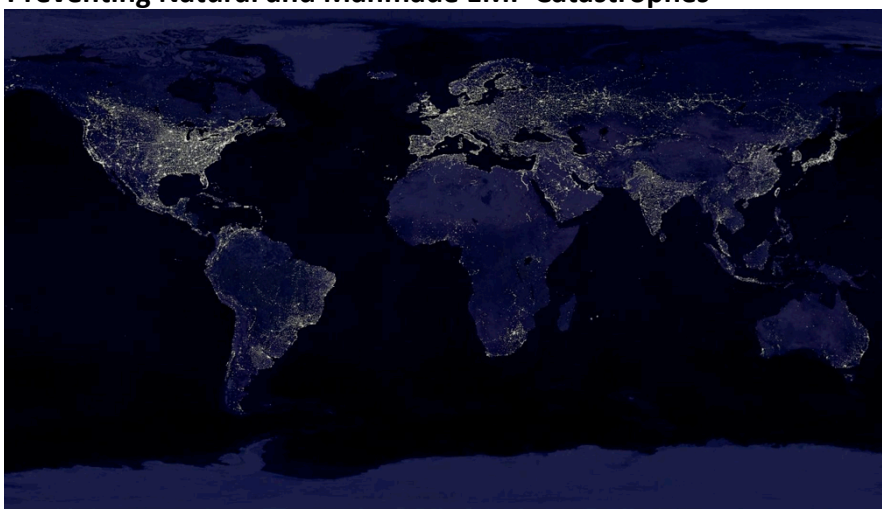


Image source: NASA

Smart grids create more potential points of failure from EMP than traditional grids. Ideally, protective measures should be considered early in the brief and applied before rollout. Cost effectiveness is essential (EMPrimus 2011, Koepke 2010). It is possible through robust planning to prevent EMP catastrophes. Action is required sooner rather than later for protecting smart grids, Smart Meters and smart appliances, and could create numerous opportunities for investment and the development of new sustainable technologies.

At present there are no procedures to "perform *"black start" [restoring a power station to operation without requiring use of using the external power grid] under severe damage scenario,"* as these require energy and telecom transport that are power dependent (Graham et al. 2011). It is recognised that if substantial numbers of transformers fail the restart of the grid will be more complicated (UK House of Commons Defence Committee 2012). Problems will be further exacerbated if meters also fail due to inappropriate non-EMP resilient design.

Power grids, meter systems and related technologies should be designed where practical to prevent / reduce likely adverse effects from EMP.

Recommendations *(partial listing as related to EMP – various authors)*
• Adhere to the Electric Infrastructure Security Council (EIS) International Infrastructure Security Roadmap (EIS 2011).
• Determine grid and network level vulnerabilities & prioritise actions.
• Improve forecasting ability for EMP events.
• Protect important infrastructures and "high value" assets through appropriate design measures - including hardening.* "High value" assets include essential government operations and those of other national institutions.
• Grid-level protection systems should be installed to protect against EMP threats to transformers.
• Harden smart grid infrastructures and related technologies against EMP risk.*
• Delay rollout of additional Smart Meters till after main period of solar risk if unhardened. Ideally also harden against risk of manmade EMP attacks and allow retention of analogue meters.
• Develop regional and national smart grid restoration plans and survival plans for populations.
• Provide Government endorsement & tax incentives for required work.
• Undertake "controlled" power cuts when necessary to protect grid.
• Identify & address regulatory gaps that preclude effective mitigation.
• Manufacture robust essential components for infrastructure, such as large transformers, within own country – this may greatly help shorten recovery periods and create extra jobs.

*If budget does not stretch to automatically protecting Smart Meters in this way, individuals should be allowed to retain or have analogue meters reinstalled.

"*The technology to protect critical infrastructures from natural or malicious electromagnetic threats now exists. Implementation costs are estimated at less than 0.01% of GNP. For example, costs for protection of the U.K. electric grid are estimated at approximately £ 0.1B. The corresponding estimate for the U.S. would be approximately $1B*," EIS (2010). … "*Since much of this cost would in any case be incurred for normal periodic upgrade and modernization, the net costs are even lower*," Arbuthnot et al. (2010).

Recovery periods are shortened as level of grid protection increases (Birnbach 2011). Significant, affordable improvements can be made to prevent, prepare, protect and recover from EMP events (Graham et al. 2011). It is anticipated that the costs of EMP protection may in part be compensated by reduced insurance costs (Birnbach 2011).

"*If addressed, our reduced vulnerability helps deter attack, enhances infrastructure resilience and confers added protection against cyber threats and damaging geosolar storms*." Commission to Assess the Threat from High Altitude EMP (Graham et al., 2011).

Certain measures, such as a widespread changeover to fibre-optic data and signal cabling, may greatly increase system robustness to EMP threats (Cikotas & Kappenman 2011) and also open up other streams of revenue (Fehrenbacher 2009) – the hardening of such systems will further increase their attractiveness to investors.

References

Arbuthnot, J. et al. (2010), EIS Summit: Electric Infrastructure Security Summit. The First World Infrastructure Security Summit, - London, 20 September 2010, Westminster Hall, Parliament, UK.

Birnbach, C. (2011), Understanding the problem: Nuclear and Non-Nuclear EMP. Presentation given at The 2nd Annual World Summit on Infrastructure Security, Washington D.C.

Cikotas, B. & Kappenman, J. (2011), Options for Protection: Protecting National Electric Grids and Critical Infrastructures. Presentation given at The 2nd Annual World Summit on Infrastructure Security, Washington D.C.

Connor, S. (2011), 'Controlled' power cuts likely as Sun storm threatens national grid. The Independent, 13 June 2011, http://www.independent.co.uk/news/science/controlled-power-cuts-likely-as-sun-storm-threatens-national-grid-2296748.html

EIS (2011), EIS Summit: International Infrastructure Security Roadmap, Electric Infrastructure Security Summit - The Capitol Building, US Congress, Washington D.C., 11 April 2011.

EMPrimus 2011, Grid and transformer protection, http://www.emprimus.com

Fehrenbacher, K. (2009), Fiber Have a Role in the Smart Grid? A Tennessee Utility Thinks Sohttp://gigaom.com/cleantech/does-fiber-have-a-role-in-the-smart-grid-a-tennessee-utility

Foster, J.S. Jr. et al. (2008), Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack: Critical National Infrastructures.

Graham, W.R. et al. (2011), Commission to Assess the Threat from High Altitude Electromagnetic Pulse (EMP): Overview. Presentation given at The 2nd Annual World Summit on Infrastructure Security, Washington D.C.

HMG (2010), A Strong Britain in an Age of Uncertainty: The National Security Strategy, HM Government, Presented to Parliament by the Prime Minister by Command of Her Majesty October 2010, The Stationery Office Limited.

Koepke, G. (2010), Highlights of Connectivity Week 2010: EMC and Smart Grid, http://www.emcs.org/acstrial/newsletters/summer10/EMCStandards.html

McClelland, J.H. (2011), Protecting our Critical Infrastructures. Presentation given at The 2nd Annual World Summit on Infrastructure Security, Washington DC

UK House of Commons Defence Committee (2012), Developing Threats: Electro-Magnetic Pulses (EMP), Tenth Report of Session 2010–12. Report, together with formal minutes, oral and written evidence. HC 1552, The Stationery Office Limited, London.

US Homeland Security (2009), Securing the Modern Electric Grid from Physical and Cyber Attacks. Hearing before the Subcommittee on Emerging Threats,. First Session 21 July 2009, Serial No. 111-30, 147pp.

Cyber Security

"… it is quite possible that a nation state might launch … [a cyber-attack targeting Smart Meters to switch off a country's electricity supply] during a time of international tension. A second possibility is a terrorist organisation. A third possibility could be environmental activists; … A further possibility is a criminal, who switches off a number of an energy company's meters and threatens widespread havoc unless a ransom is paid. … Yet another angle is the possibility of criminal energy theft …" The introduction of Smart meters create significant new cyber-vulnerabilities, (Anderson & Fuloria 2010).

The UK National Security Council now recognises cyber-attacks as a Tier One threat – the highest priority for UK national security (HMG 2010, AEPN 2010).

Experts at the IEEE Smart Grid Comm 2010 conference warned that consumers and utilities' infrastructures are becoming more vulnerable to cyber-attack due to the increased security vulnerabilities and the two-way communication of smart grids as compared to existing systems. They predict that the smart grid will present up to 440 million possible points to be hacked by 2015 (Schwartz 2010). The US Department of Energy also recognise shortfalls in the cyber security plans (US DOE 2012).

It is recognised by the US Government Accountability Office (US GAO) and the US Department of Energy (US DOE) that the transition to smart grids is opening electric grids open to increased cybersecurity weaknesses that risk damaging their efficient operation (US DOE 2012, US GAO 2011, Mills & LaMonica 2010). It has already been claimed that hackers from a major foreign country have reconnoitered the US electricity grid possibly seeking to discover exploitable systemic vulnerabilities such as those presented in present Smart Meter systems (Anderson & Fuloria 2011).

In 2009 cyber security analyst Morgan Wright, when leading the Global Public Safety and Homeland Security Program at CISCO Systems, claimed that having the US electric grid standardised on a single platform, instead of a more distributed layered model, had caused a lot of cyber vulnerabilities and that its operating system had been hacked into by foreign state sponsored spies. He further claimed that when they gained access they scoped out vulnerabilities and control systems and may have left backdoors in place, remote control devices, or things they could activate at a later date to carry out set tasks such as shutting down or redistributing the nation's power (Wright 2009).

Built In Security

The US GAO states that "*increasing the use of new system and network technologies can introduce new, unknown vulnerabilities. … our experts stated that smart grid home area networks … do not have adequate security built in, thus increasing their vulnerability to attack.*" To counter such risks, over $30 million *(£18.62 million*) has been awarded to address these cyber-security and reliability issues (Schwartz 2010). Even with such massive funding, some experts still express grave concerns (Mills & LaMonica 2010) and it is recognized that cyber security plans can often be incomplete or lack sufficient detail (US DOE 2012). Smart Meters being hacked could result in local and widespread disruptions, sensitive facilities being 'taken out', loss of data privacy (*including information on the types of equipment individuals own, building occupancy patterns and identity theft*). Loss of data privacy may also arise from data collected by Smart Meters through non-intrusive appliance load monitoring being sold by utilities to third parties unless appropriate safeguards are put in place (Quinn 2009).

Manipulation of Smart Grid Data

Electricity theft is a cause of great concern to utility companies, and already there are devices existing that allow Smart Meters to be altered remotely to register less energy consumption than actually used (Wisniewski 2012, Mills & LaMonica 2010). Assistant Professor Le Xie of Texas A&M University notes that it is likely that some attackers could be virtual traders seeking to benefit financially through intercepting and manipulating smart grid data to place safe bets on energy demands (Schwartz 2010).

Smart Meter Data

Every electrical appliance has its own energy fingerprint readable by Smart Meters. Those accessing such information have indications of the appliances individuals have and how often they use them.

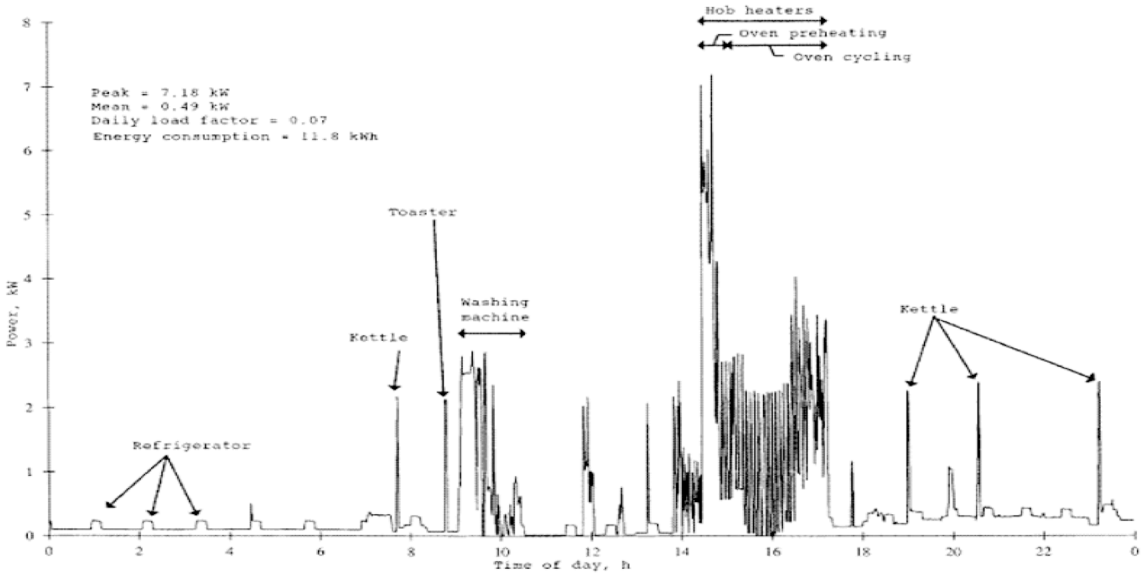


Image source: Newborough & Augood (1999).

Parties wishing Smart Meter data?	Potential use (partial listing)
Utilities	Efficiency analysis, monitoring of electricity usage & load for forecasting & bills
Electricity usage advisory companies	To promote energy conservation & awareness measures
Insurance companies	Determining health care premiums based on unusual behaviours (such as sleep problems*), that might indicate illness
Marketers	Profiling for targeted advertisements
Law enforcers	Identifying suspicious or illegal activities
Civil litigators	Determining when home occupied, by how many parties & activities undertaken
Landlords	To verify lease compliance
Private investigators	Monitoring for specific events
The Press	Information on famous individuals' movements & lifestyle
Creditors	Determination of behaviour that might indicate creditworthiness
Criminals	To identify the best times for burglary or to identify high-priced appliances to steal

Original source: SGIP (2010)

*Emissions from some wireless Smart Meters have been reported to be linked to health and sleep problems (EMF SN 2011) – *present author's comment*.

Data Provision & Privacy/Security Issues

"*Digital information and communication technology offers the possibility of a new world of freedom. It also offers possibilities of surveillance and control which dictatorships of the past could only struggle to establish. The battle to decide between these possibilities is being fought now*," Stallman (2010).*

**Refer also to Appendix 7 of main document*.

"We … have the technology to record … (energy consumption) every minute, second, microsecond, more or less live... From that we can infer how many people are in the house, what they do, whether they're upstairs, downstairs, do you have a dog, when do you habitually get up, when did you get up this morning, when do you have a shower: masses of private data. … We think the regulator needs to send a strong signal to say that the data belongs to consumers and consumers alone. We believe that's a blocker to people adopting the technology," Martin Pollock of Siemens Energy, quoted by Wynn (2010).

Unlike conventional meters that measure total energy use through day and night tariffs (and are normally read four times every year), Smart Meters allow energy use to be read with far finer granularity (typically every half-hour). There is much debate as to what level of information should be provided by Smart Meters and to whom it should be provided. "… *high resolution electricity usage information can be used to reconstruct many intimate details of a consumer's daily life … [there are many ways], that information could be used in ways potentially invasive of an individual's privacy*." Quinn (2009).

As an example of the level of privacy invasion that is possible, it was recently shown by Dario Carluccio and Stephan Brinkhaus (at the 28th Chaos Computing Congress (28c3) hacker conference in Germany) that hacking into a Smart Meter could in, addition to identifying activity patterns in homes (including whether they were occupied) and the types of equipment being used, even allow identification of the movies being played by occupants. Prior to concluding that the security encountered was poor and the data resolution the meters provided was too high, they were also able to demonstrate how easy it was to alter apparent energy usage (Wisniewski 2012).

A court in the Netherlands (Cuipers & Koops 2008) has already determined that the mandatory collection of non-essential fine-grained Smart Meter data is against Article 8(1) of the European Convention of Human Rights (which the UK is signed up to). That ruling has led to mandatory Smart Meter installation being halted in the Netherlands (metering.com 2009). It is important to address such potential legal issues as early as possible and ensure that necessary safeguards are put in place.

"it [is] imperative that proper consideration is given to individuals' fundamental rights to privacy," EC (2011). Under EU Data Protection Law, consumers' rights to privacy "*may not be overridden*", as it is their degree of positive acceptance, support and involvement with Smart Meters and related technology that will determine the level of success smart metering achieves.

"*Data protection issues play a very important and even decisive role in the successful implementation of smart metering*," Knyrim & Trieb (2011).

As noted by Berliri & Maxwell (2010):
- 'Privacy by Design' creates opportunities rather than threats for smart grids – *it instills consumer confidence.*
- Consumers concepts of privacy are altering; soon statutory provisions may be inadequate. Privacy should be embedded into the technology.
- There may be competitive advantages for those able to offer the highest levels of privacy protection.

Robust privacy measures and policies are required to cover data usage and distribution if consumers are to be brought onboard and potential security shortfalls addressed.

Smart grid privacy measures			
Privacy threat		Service required	Existing protection mechanisms
Network threats	Shallow packet inspection	Anonymity	Anonymity networks
	Deep packet inspection	Confidentiality	Encryption
Data usage threats	Unauthorised usage/access	Access control	Policies, legislation, secure storage
	Customer privacy	Customer control of customer data	

Source: Sooriyabandara & Kalogridis (2011).

Undertaking robust measures to anonymise Smart Metering data and remove recognisable appliance load signatures can help to address privacy concerns (Efthymiou & Kalogridis 2010, Kalogridis et al. 2010). Such measures may include: Privacy Enhanced Home Energy Management using Elec Privacy algorithms (*to disguise the signatures of electronic equipment*) and Escrow: Data Anonymisation.

Privacy Initiatives

Ontario, Canada

The province of Ontario in Canada is a world leader in embedded privacy protections for smart grids (PBD 2010). Adopting its guidelines may help prevent many claims on Human Rights privacy issues that might otherwise stall or halt rollouts.

1. Proactive not Reactive; Preventative not Remedial "*Smart Grid systems should feature privacy principles in their overall project governance framework and proactively embed privacy requirements into their designs …*"
2. Privacy as the Default "*Smart Grid systems must ensure that privacy is the default — the "no action required" mode of protecting one's privacy — its presence is ensured*."
3. Privacy Embedded into Design "*Smart Grid systems must make privacy a core functionality in the design and architecture of Smart Grid systems and practices — an essential design feature*."
4. Full Functionality — Positive-Sum, not Zero-Sum "*Smart Grid systems must avoid any unnecessary trade-offs between privacy and legitimate objectives of Smart Grid projects*."
5. End-to-End Lifecycle Protection "*Smart Grid systems must build in privacy end-to-end, throughout the entire life cycle of any personal information collected*."
6. Visibility and Transparency *"Smart Grid systems must be visible and transparent to consumers - engaging in accountable business practices - to ensure that new Smart Grid systems operate according to stated objectives."*
7. Respect for User Privacy *"Smart Grid systems must be designed with respect for consumer privacy, as a core foundational requirement*."

That document states that the above principles should be applied to: accountable business practices; Information Technology (IT) systems; and physical design and networked infrastructure for smart grids (PBD 2010).

"… if the data protection rights of consumers are not sufficiently taken into account, then their acceptance of the new technology will be lacking, which could lead to its unsuccessful implementation," Knyrim & Trieb (2011).

Another concern related to 'Privacy by Design' is that present smart grid systems have a life expectancy of 10-20 years, during which time any in-built security they may have risks becoming compromised or outdated.

United Kingdom

The UK is adopting an approach to privacy drawn on international best practice measures and the advice of privacy experts (DECC 2011). In September 2011, it was announced that the UK Government has established a central data and communications company to administer access to smart grid data to help allay consumer privacy concerns over Smart Metering. The UK Government will also oversee its security (smartmeters 2011).

California, USA

In July 2011, California voted to adopt it's own comprehensive set of privacy and security rules for the three utility companies that provide the majority of Californians with electricity (King 2011). If consumers wish, they will be able to allow third parties to receive their backhauled Smart Meter data directly from the utilities, as opposed to directly from the Smart Meters in order to support services

including demand response, energy advice and energy efficiency. It is important to note that the CPUC declared that "*The utilities … will bear no new liability for the actions of third parties which acquire information via this [mechanism]*."

The CPUC also stated that they will not exercise jurisdiction over third parties who directly receive energy usage data from installed devices that receive data via the HAN interface (King 2011). It is likely that the Californian and UK initiatives will be a success if they fully take into account Human Rights' privacy issues and the need to anonymise electrical metering data to gain public trust.

Texas, USA

In Texas all meter data on electricity shall belong to the customer (BSM (2011). Texas Utilities Code 39.107(b) states: "*All meter data, including all data generated, provided, or otherwise made available, by advanced meters and meter information networks, shall belong to a customer, including data used to calculate charges for service, historical load data, and any other proprietary customer information*. …"

Blackout Attacks

One of the gravest scenarios is that of "*a 'cyber-nuke'* [through the Smart Meters] *that would reduce* … [a country's] *population to destitution. Recovery from such an attack would be painful* [loss of life may also be high – present author's comment]*. As a matter of national survival, the government would probably authorise any electrician or other competent person to short-circuit dead meters. Utility contractors might need to spend a year or more visiting every house to rekey or replace them*" (Anderson & Fuloria 2011). This risk does not exist with analogue meters.

Network security experts state that once a hacker gains access to the smart grid he/she may gain control "*of thousands, even millions, of [smart] meters and shut them off simultaneously*." Individual hackers may also be able to substantially raise or lower power demand, disturbing the local power grid's load balance and creating a blackout. They also state that such outages would "*cascade to other parts of the grid, expanding the blackout,*" with no one being able to predict the possible scale of such damage (Meserve 2009).

There is a high cost to blackouts, the Northeast Blackout of 2003 in North America cost $3 billion (£1.86 billion). A coordinated attack on the grid "*could lead to even more significant economic damages*" (ICFC 2003). The cost of precautionary and protective measures are far less. "*As the nature of our technology becomes more complex, so the threat becomes more widespread. … However advanced we become, the chain of our security is only as strong as its weakest link*", the Rt. Hon. Dr. Liam Fox MP when UK Defence Secretary (Fox 2010).

The development of appropriate solutions to realistic threats to security of supply should be carried out before further large-scale smart grid rollouts are undertaken. "*Without securely designed smart grid systems, utilities will be at risk of not having the capacity to detect and analyze attacks, which increases the risk that attacks will succeed and utilities will be unable to prevent them from recurring*," (US GAO 2011).

Unnecessary National Security risks should be avoided/reduced wherever possible. The present installation of remote off-switches for Smart Meters further increases risk of blackouts - *ideally Smart Meters should be designed to fail in the 'on' mode to reduce this risk*. This safety measure would also be in accord with Human Rights laws in Europe which stop defaulters simply being disconnected (Anderson & Fuloria 2010a).

References

AEPN (2010), Cyber Terrorism Escalated To Tier One Risk In The UK, AEP Networks, http://www.prosecurityzone.com/News/It_security/Network_security__routers_and_data_centres/Cyber_terrorism_escalated_to_tier_one_risk_in_the_uk_15519.asp#axzz1QjuniAJI

Anderson, R. & Fuloria, S. S. (2011), Smart meter security: a survey, 7pp. (draft),

http://www.cl.cam.ac.uk/~rja14/Papers/JSAC-draft.pdf
Anderson, R. & Fuloria, S. S. (2010), Who controls the off switch? In IEEE conference on Smart Grid Communications, NIST, Maryland, USA, October 2010, http://www.cl.cam.ac.uk/~rja14/Papers/meters-offswitch.pdf
Anderson, R. & Fuloria, S. (2010a), On the security economics of electricity metering, 9th Workshop on the Economics of Information Security, Harvard University, George Mason University in Arlington, VA, June 2010, 18 pp.
Berliri, M. & Maxwell, W. (2010) Smart metering, smart grid and privacy by design, Project E-Cube, 21 September 2010.
BSM (2011), Smart Meter Data Belongs to the Customer, http://www.bansmartmeters.com/blog/2011/03/smart-meter-data-belongs-to-the-customer/
Cuipers, C. & Koops, B.J. (2008), Het wetsvoorstel 'slimme meters': een privacytoets op basis van art. 8 EVRM, Universiteit van Tilburg.
DECC (2011), Smart Metering Implementation Programme: Response to Prospectus Consultatiion. Supporting Document 1 of 5 Data Access and Privacy. Department of Energy and Climate Change and the Office of Gas and Electricity Markets, 56 pp.
EC (2011), Article 29, Data Protection Working Party Opinion 12/2011 on smart metering Adopted on 4 April 2011, 00671/11/EN WP 183, The Working Party on the Protection of Individuals with Regard to the Processing of Personal Data, http://ec.europa.eu/justice/policies/privacy/index_en.htm
Efthymiou C. & Kalogridis, G. (2010), Smart Grid Privacy via Anonymization of Smart Metering Data, First IEEE Int. Conference on Smart Grid Communications, Oct. 2010
Fox, L. (2010), Keynote presentation at The First World Infrastructure Security Summit, Electric Infrastructure Security Summit, Westminster Hall, Parliament, UK, 2010.
HMG (2010), A Strong Britain in an Age of Uncertainty: The National Security Strategy, HM Government, Presented to Parliament by the Prime Minister by Command of Her Majesty October 2010, The Stationery Office Limited.
ICFC (2003), The Economic Cost of the Blackout An issue paper on the Northeastern Blackout, August 14, 2003, ICF Consulting, 3pp.
Kalogridis, G. et al. (2010), Privacy for Smart Meters: Towards Undetectable Appliance Load Signatures, First IEEE Int. Conference on Smart Grid Communications, Oct. 2010.
King, C. (2011), California PUC adopts consumer data access and privacy rules for smart meters. Smart Grid Watch, eMeter, http://www.emeter.com/smart-grid-watch/2011/california-puc-adopts-consumer-data-access-and-privacy-rules-for-smart-meters/
Knyrim, R. & Trieb, G. (2011), Smart metering under EU Data Protection Law, International Data Privacy Law, 1(2), pp. 121-128.
Meserve, J. (2009), 'Smart Grid' may be vulnerable to hackers. CNN.com, http://edition.cnn.com/2009/TECH/03/20/smartgrid.vulnerability/#cnnSTCText)
Mills, E. & LaMonica, M. (2010), Money trumps security in smart-meter rollouts, experts say. InSecurity Complex, cnet NEWS, http://news.cnet.com/8301-27080_3-20007672-245.html?tag=mncol;txt
Newborough, M. & Augood, P. (1999), Demand-side management opportunities for the UK domestic sector, IEE Proceedings of Generation Transmission and Distribution 146(3), pp. 283–293.
PBD (2010), Privacy by Design: Achieving the Gold Standard in Data Protection for the Smart Grid. Information and Privacy Commissioner, Ontario, Canada, Hydro One Inc. and Toronto Hydro Electric. 37 pp.
http://www.ipc.on.ca/images/Resources/achieve-goldstnd.pdf
Powerwatch (2010), Smart Meters - smart idea - not so smart implementation,
http://www.powerwatch.org.uk/news/20101018_smart_meter.asp
Quinn, E.L. (2009), Privacy and the New Energy Infrastructure, Social Science Research Network, 09, pp. 1995-2008.
Radasky, R.A. (2011), High Power Electromagnetic (HPEM) Threats to the Smart Grid, EMC Interference Technology, Directory & Design Guide 2011, pp 46-55.
Schwartz, M.J. (2010), Smart Grids Offer Cyber Attack Opportunities Hackers are likely to exploit the 440 million potential targets researchers predict smart grids will offer by 2015. InformationWeek, http://www.informationweek.com/news/security/vulnerabilities/showArticle.jhtml?articleID=227701134
SGIP (2010) NISTIR 7628, Guidelines for Smart Grid Cyber Security: Vol. 2, Privacy and the Smart Grid, The Smart Grid Interoperability Panel - Cyber Security Working Group, National Institute of Standards

and Technology, Vol. 2, pp. 30–32, http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol2.pdf, pp. 30-32.
Smartmeters (2011), Britain Remains Smart Grid leader. smartmeters, http://www.smartmeters.com/the-news/2584-britain-remains-smart-grid-leader-.html
Sooriyabandara, M. & Kalogridis, G. (2011), Smart Grid Privacy by Design, ETSI 6th Security Workshop, Sophia Antipolis, France, 19th Jan 2011, PowerPoint presentation, http://docbox.etsi.org/Workshop/2011/201101_SECURITYWORKSHOP/S5_SECURITYinSMARTGRIDS/SOORIYABANDARA_TOSHIBA_SmartGridsPrivacybyDesign.pdf
Stallman, R. (2010), Is digital inclusion a good thing? How can we make sure it is?, IEEE Communications Magazine, 48, pp. 112-118.
TUC (2011), [Texas] Utilities Code, Title 2. Public Utility Regulatory Act, Subtitle B. Electric Utilities, Chapter 39. Restructuring of Electric Utility Industry, Subchapter A. General Provisions, http://www.statutes.legis.state.tx.us/Docs/UT/htm/UT.39.htm
US DOE (2012), Audit Report: The Department's Management of the Smart Grid Investment Grant Program, OAS-RA-12-04, 21pp, http://energy.gov/sites/prod/files/OAS-RA-12-04.pdf
US GAO (2011), Electricity Grid Modernization: progress being made on Cybersecurity Guidelines, but key challenges remain to be addressed. United States Government Accountability Office, Report to Congressional Requesters.
Quinn, E.L. (2009), Smart Metering & Privacy: Existing Law and Competing Policies. A Report for the Colorado Public Utilities Commission, 62 pp. http://www.dora.state.co.us/puc/docketsdecisions/DocketFilings/09I-593EG/09I-593EG_Spring2009Report-SmartGridPrivacy.pdf
Wisniewski, C. (2012), Smart meter hacking can disclose which TV shows and movies you watch, nakedsecurity, http://nakedsecurity.sophos.com/2012/01/08/28c3-smart-meter-hacking-can-disclose-which-tv-shows-and-movies-you-watch/
Wright, M. (2009), Discussion on America's Newsroom,
http://www.youtube.com/watch?v=k5iNNp3qwbk&feature=related
Wynn, G. (2010), Privacy concerns challenge smart grid rollout, http://www.reuters.com/article/2010/06/25/us-energy-smart-idUSTRE65O1RQ20100625

Conclusion – the design of power grids, meter systems and electrical appliances needs to be rapidly rethought to deal with the real life issues that have been raised.