VOL 1 ISSUE 4 **December 2015**

IR3 Feature Articles

Editorial Corner

Dr. Robyn Fiori

About the Editor

Dr. Robyn Fiori is a research scientist for the Canadian Hazards Information Service of Natural Resources Canada specializing in space weather. Her research is applied to the development and improvement of space weather tools and forecasts to be used by operators of critical infrastructures and technologies in Canada. As well, it has been published in numerous peer reviewed scientific journals, including the Journal of Geophysical Research, the Journal of Atmospheric and Solar-Terrestrial Physics, and Space Weather. Dr. Fiori received her B.Sc., M.Sc., and Ph.D. from the University of Saskatchewan, Department of Physics and Engineering Physics while studying in the Institute of Space and Atmospheric Studies.

This Issue

The fourth issue of IR^3 highlights the interdependency of critical infrastructure and describes some of the strategies and organizations developed to mitigate risk and improve the resilience and security of these systems.

Communication is key in any disaster scenario, regardless of the cause. Benoît Robert, Justine Arnoux, and Luciano Morabito describe the interconnectivity of telecommunications systems and the importance of inter-organizational cooperation to ensure the smooth operation and resilience of the systems, both in general and in an emergency situation. They review different kinds of Canadian telecommunications, their interdependencies, and the challenges and opportunities involved in information sharing.

Power systems form a critical layer of infrastructure on which many others depend. Damage to such systems is accompanied by severe impacts to the economy, safety, and security. Kenneth Friedman and Tiffany Choi examine the risks to large power transformers, the challenges involved in the replacement of one or more failed transformers, and discuss risk mitigation strategies. Focusing on impacts to the electrical power grid, Christopher Balch discusses the role of the NOAA Space Weather Predictions Center in mitigating impacts through the real-time monitoring and forecasting of geomagnetic activity on a variety of time scales.

The RCMP's National Critical Infrastructure Intelligence team works to protect all Canadian infrastructures. They write an article describing modernization of the RCMP's suspicious incident reporting system which collects information on suspicious incidents to review in a broader context with the goal of identifying potential threats.

Connie Delisle and Felix Kwamena point out the interdependency of critical infrastructure and the importance of training to properly understand the challenges involved in developing critical incident response action plans and to strengthen response efforts. They describe scenario-based learning techniques applied by the infrastructure resilience researchers and Carleton University at a recent workshop.

Next Issue

For Issue 5 we invite authors working in academia or industry to contribute articles relating to their experience in the field of infrastructure resilience describing potential sources of compromise and lessons learned. Draft articles of 3000-4000 words are requested by early April. You may not have much time or experience in writing 'academic' articles, but IR^3's editorial board can provide guidance and help. Your experience is valuable and IR^3 provides an ideal environment for sharing it.

Understanding the Impediments to Inter-Organizational Information Sharing: Application to the Telecommunications Sector

Benoît Robert, Ph.D.
Département de mathématiques et de génie industriel
École Polytechnique Montréal
Email: benoit.robert@polymtl.ca

Justine Arnoux, M.Sc.A.
Département de mathématiques et de génie industriel
École Polytechnique Montréal
Email: justine.arnoux@polymtl.ca

Luciano Morabito, Eng.
Département de mathématiques et de génie industriel
École Polytechnique Montréal
Email: luciano.morabito@polymtl.ca

Abstract

Telecommunication networks are considered critical infrastructure because these networks provide a vital resource which society needs to properly operate. These networks are also highly interconnected systems. Enhancing the resilience of telecommunication networks is therefore essential and has to be supported by inter-organizational cooperation. Important challenges remain in the sharing of information between telecommunication operators regarding their interdependencies. This article presents the various types of Canadian telecommunication operators, categories of interdependencies between them, as well as challenges and opportunities linked to information sharing. A framework for exchanging and sharing information is then proposed. This article is the outcome of research done by the Centre risque & performance at Polytechnique Montréal, within the framework of a project financed by Defence Research and Development Canada, with the cooperation of Industry Canada and the Centre de services partagés du Québec (Arnoux, 2015).

I. Wide Variety of Actors to be Involved to Ensure System Resilience

Telecommunication systems correspond to one of the ten classes of critical infrastructure defined in the Government of Canada's *National Strategy for Critical Infrastructure* (Government of Canada, 2009). Telecommunication systems are vital for the smooth functioning of society as a whole, and represent a particularly heavily used category of critical infrastructure. These systems are not only at the heart of all socioeconomic activities and the ongoing management of organizations, they also play a key role during emergencies to allow, among other things, the coordination of first responders. Importantly, all other critical infrastructures depend on telecommunication systems. For example, water and power utilities use telecommunications for their SCADA (supervisory control and data acquisition) systems, which enables them to operate their facilities remotely (Rinaldi et al., 2001). This massive use of telecommunications is far from reaching an end; consider, for example, the concepts of the digital society, the Internet of Things and Smart Cities, which are in the news these days.

It is clear that telecommunication systems must be protected. In particular, their resilience must be safeguarded. Resilience is defined as "the capacity of a system, community or society potentially exposed to hazards to adapt, by resisting or changing in order to reach and maintain an acceptable level of functioning and structure" (Government of Canada, 2009, p. 4). According to the *National Strategy for Critical Infrastructure*, "responsibilities for critical infrastructure in Canada are shared by federal,

provincial and territorial governments, local authorities and critical infrastructure owners and operators – who bear the primary responsibility for protecting their assets and services" (Government of Canada, 2009, p. 2).

In the case of telecommunication systems, a brief overview of the sector will emphasize the diversity of the owners of telecommunication systems, or Telecommunications Service Providers (TSPs), which inevitably have a role to play in ensuring the resilience of telecommunication systems.

As in other countries, such as the United States and France, the word "monopoly" no longer characterizes the telecommunications sector in Canada (Schiller, 2003). In the past, this sector was structured essentially in the form of large regional monopolies, most of which were held by Bell Canada, and regulated by the *Railway Act*; however, it has evolved considerably since the 1970s (CRTC, 2005). Influenced by the wave of deregulation under way in the U.S. telecommunications sector at the time and the emergence of new technologies that made it possible to provide ever more diversified services, the telecommunications sector has acquired a more competitive functional structure (CRTC, 2005).

Thus, in 2013, the Canadian Radio-television and Telecommunications Commission (CRTC) listed more than 800 TSPs in Canada (CRTC, 2014).

The Canadian government classifies these suppliers in different categories as shown in figure 1.

<table>
<tr><td rowspan="6">TSPs*</td><td rowspan="2">Incumbent TSPs</td><td>Large incumbent TSPs</td><td colspan="2"></td></tr>
<tr><td>Small incumbent TSPs</td><td colspan="2"></td></tr>
<tr><td rowspan="4">Alternative TSPs</td><td rowspan="3">Facilities-based alternative TSPs</td><td>Incumbent TSPs – out of territory</td><td></td></tr>
<tr><td rowspan="3">Non-incumbent TSPs</td><td>Cable BDUs**</td></tr>
<tr><td>Utility telcos</td></tr>
<tr><td>Other carrier</td></tr>
<tr><td colspan="2">Non-facilities-based alternative TSPs (Resellers)</td><td colspan="2"></td></tr>
</table>

Figure 1: Categories of Telecommunications Service Providers (TSPs)

*Telecommunications Service Providers

** Broadcast distribution undertakings

The descriptions of the different categories of TSPs come essentially from the CRTC's *Communications Monitoring Report 2013*.

The two major categories of TSPs are:

1. incumbent TSPs, and
2. alternative TSPs.

The first category, incumbent TSPs, includes the companies that used to provide telecommunications services on a monopolistic basis before the sector was liberalized and competition was introduced. In the literature, these companies are also called "historical operators" or "incumbent local exchange carriers (ILECs)." Incumbent TSPs are divided into two subgroups: large incumbent TSPs, and small incumbent TSPs.

Large incumbent TSPs are those that serve relatively large areas, usually including both rural and urban populations, and provide a range of services: wireline voice, Internet, data transmission, dedicated lines and wireless. The three large incumbent TSPs in Quebec are Bell Canada; Telus for Quebec City and the Gaspésie region; and Télébec, a subsidiary of Bell Aliant that serves the remote regions of Quebec.

Small incumbent TSPs are companies that serve relatively small areas (usually municipalities located in

low population density regions). Because of the small size of the regions they serve, these companies generally do not offer long-distance telephone services with their own facilities. However, they do offer wireline telephone services, Internet, data transmission services, dedicated lines and wireless services. Sogetel Inc. (Quebec) and Lansdowne Rural Telephone Company Ltd. (Ontario) are examples of small incumbent TSPs.

The second major category, alternative TSPs, includes companies that did not have a monopoly before the markets were liberalized, such as Rogers and Vidéotron, and incumbent TSPs that operate outside their own territories, such as Telus in regions of Quebec where it is not the incumbent TSP (e.g., Pontiac region). In the literature, these companies are also called "alternative operators" or "competitive local exchange carriers (CLECs)." Alternative TSPs are also divided into two subcategories:

1. facilities-based alternative TSPs, and
2. non-facilities-based alternative TSPs.

Facilities-based alternative TSPs are those that own and operate telecommunication systems. This group is subdivided into incumbent facilities-based TSPs operating out of territory (Telus in Quebec) and non-incumbent facilities-based TSPs. Non-incumbent facilities-based TSPs are divided into three further subcategories:

1. Cable broadcast distribution undertakings (BDUs), which are the former monopolistic cable companies that also provide telecommunications services. Bragg, Cogeco, Rogers, Shaw and Vidéotron are a few examples.
2. Utility telcos, which are TSPs whose entry into the telecommunications services market was due to the activities of the company or one of the companies in the group in a utility sector, such as electricity, gas, etc. The Port of Montreal is an example of this kind of TSP.
3. Other carriers that own their own transmission facilities (e.g., long-distance, urban or local transmission facilities).

Non-facilities-based alternative TSPs do not own any telecommunication infrastructures and do not operate any telecommunication system. They are generally called resellers, since they purchase telecommunications services from other TSPs and resell them or create their own system that enables them to serve their customers. Thus, resellers are companies that lease high-volume capacity from operators and offer services to potential customers. Resellers constitute the largest group of TSPs in Canada, accounting for 68% of TSPs (CRTC, 2014). Koodo and Distributel are examples in Quebec.

This brief description of the various TSPs in Canada reveals that telecommunication system resilience is an issue affecting numerous actors.

II. Collaborating to Ensure Telecommunication System Resilience

Another factor to be remembered when discussing TSPs in Canada is that the various TSPs are interdependent on each other, regardless of which TSP category they belong to.

The first form of interdependence among TSPs is inevitable since it relates to the interconnection of the different TSPs' systems so that customers of one TSP can communicate with customers of another TSP. Telephone exchanges, for example, tend to be locations for interconnections. However, there are other situations in which one TSP needs to use another TSP's system to provide its own service. For example, roaming agreement contracts may be entered into by two TSPs so that customers of one TSP can use their cell phones in another TSP's area if the TSP serving them does not have a mobile telephone system on a particular segment of the territory. Both interconnectivity among TSPs and roaming contracts give rise to functional interdependencies among TSPs since a resource (here, a physical portion of the system) is "exchanged" between two TSPs so they can provide their telecommunications services (Peerenboom et al., 2002; Rinaldi et al., 2001; Robert and Morabito, 2008).

A second kind of interdependency among TSPs corresponds to so-called geographic

interdependencies, which describe situations in which telecommunication equipment belonging to different TSPs are co-located. In telephone exchanges that are affected by functional interdependencies, as described above, there can also be geographic interdependencies since the exchanges house equipment belonging to different TSPs. In the telecommunications sector, another kind of co-location, and thus geographic interdependency, appears when different TSPs, each with its own optical fibres, share a single conduit, bridge or utility pole to carry their fibres.

With regard to the resilience of telecommunication systems, these functional and geographic interdependencies among TSPs mean that the question cannot be addressed by working in silos. On the contrary, given their interdependency points, TSPs must work together to enhance the overall resilience of telecommunication systems.

This idea of collaboration among the owners of critical infrastructures, including telecommunication systems, is not a new one. As early as 2009, the Government of Canada's *National Strategy for Critical Infrastructure* specified that one of the objectives proposed to improve the resilience of critical infrastructures was to "advance the timely sharing and protection of information among partners" (Government of Canada, 2009, p. 3).

In the case of telecommunication systems, this exchange of information could consist, on one hand, in sharing best practices among TSPs regarding the measures put in place within each organization to improve system resilience. On the other hand, a more specific exchange of information about the TSPs' interdependency points on the systems could also help increase the resilience of these systems.

On this topic, in 2013 the Quebec Regional Emergency Telecommunications Committee (RETC) recommended that "companies that own joint infrastructures initiate discussions on the identification of common sites and of the impacts and domino effects of the partial or total destruction of these sites" (CRTU, 2013, our translation). The objective of the sharing of information about interdependencies among TSPs, as recommended by the RETC, is a dual one: first, to be able to identify the geographic sites where physical infrastructure is shared by TSPs and identify which TSPs are located on these sites. This identification process will make it possible, as the second step, to find the most critical locations where the interdependencies are strongest and a failure could have major consequences in terms of the number of systems affected, the geographic extent of the zones affected by disruptions, and the impacts on the organizations (telecommunication systems, other critical infrastructures, etc.) and people present in these zones.

Achieving this goal of sharing information among TSPs concerning their interdependency points could make it possible to increase the resilience of telecommunication systems in several ways.

Working together on the TSPs' interdependency points could make it easier to identify points where protective or mitigating measures would be desirable to increase robustness. Indeed, identifying the most critical interdependency points could induce the TSPs to choose to implement adapted protective or mitigating measures and thus be better able to resist disruptions at the interdependency points.

A multi-organizational study of interdependencies among TSPs could enhance system resilience by making it easier to identify the TSPs that should be alerted in case of a disruption. During a disruption, a proactive attitude can then be adopted, meaning that TSPs will generally have time to prepare and make decisions. Thus, if a disruption becomes a threat for an interdependency point among TSPs, the prior identification of the TSPs involved would enable them to be warned of a potential failure of their systems at the interdependency point. These TSPs could then take the necessary steps to optimally manage the disruption and be more resilient in that regard.

Finally, in the event of disruptions on a telecommunication system, it would be possible to establish other communication channels or create temporary physical linkages via the systems' control centres. If TSPs cooperated, they would know which ones were present at the interdependency points in the zone that could potentially be affected by a disruption.

Thus, possibilities for looping could be identified more easily. Thanks to such looping, the TSPs might be able to maintain an acceptable level of functionality and thus remain resilient in the event of a disruption. In the longer term, regarding the most critical interdependency points, the various TSPs involved might even consider redundancy measures; there again, the objective would be to improve the overall resilience of the telecommunication systems.

II. CHALLENGES TO BE MET REGARDING INFORMATION SHARING AMONG TSPS

Despite the potential value of collaboration among TSPs to improve the resilience of telecommunication systems, the sharing of information concerning their interdependencies remains problematic.

In partnership with Industry Canada and the Centre des services partagés du Québec, the *Centre risque & performance* has identified a series of impediments to information sharing. These impediments can be classified in the following four categories:

1. difficulty of accessing information;
2. sensitivity of information;
3. complexity of information; and
4. ignorance of information.

3.1. Difficulty of accessing information

Information can be difficult to access for six main reasons.

1. In the current state of affairs, no organization in the telecommunications sector, whether governmental, public, parapublic, or private has the mandate to carry out an overall analysis of interdependencies (functional and geographic) among TSPs. It is true that there are initiatives at the operational, tactical or strategic level with various committees, such as the RETC in Quebec, the Canadian Telecommunications Emergency Preparedness Association (CTEPA), the Canadian Telecom Cyber Protection (CTCP) Working Group and the Canadian Security Telecommunications Advisory Committee (CSTAC), but none of these initiatives has the specific mandate of analyzing interdependencies among TSPs from a general perspective. The question of mandate is a legitimate one. As explained in part 1 of this article, historical developments in the telecommunications sector have meant that it changed from a monopolistic structure to a context of deregulation, where there are currently hundreds of different TSPs in Canada. As the number of TSPs increased, the problem of interdependencies among them arose. Today, there is a clear need for a mandate to work on this problem. The absence of a clearly established mandate makes it difficult to access the information needed to study interdependencies, since it raises the question of who should do such a study.
2. It is difficult to access information because of the dispersion of the information needed for an overall study of interdependencies among TSPs. Such an analysis requires one to seek out information from different organizations. These organizations are becoming increasingly large and are divided into numerous departments or subsidiaries-- each of which has a kind of functional independence and occupies a specific market segment. Consequently, information may be distributed among the various departments or subsidiaries. There is not necessarily a single location where information is stored. The fact that information is not always clearly indexed (who holds the information?) or even systematically indexed (no document management system) in the different organizations or their departments and/or subsidiaries can make it even more complicated to access information. The fact that information is dispersed, reinforced by the fact that it is not always clearly or systematically indexed, makes it hard to acquire information since it takes more time, and consequently more resources (human, material and financial), to gather it.
3. The problem of access to information as a result of its dispersion would be mitigated if communication among different departments

and/or subsidiaries within organizations occurred naturally. In other words, if organizations' various departments/subsidiaries were in the habit of exchanging information, the time needed to collect it would be reduced. However, the culture of organizations is characterized by a silo mentality, meaning that some departments or subsidiaries of an organization are reluctant to exchange information with the other departments or subsidiaries of the same organization. The silo mentality in organizational culture reinforces the dispersion of information within organizations; the result is that information gathering is difficult. A substantial investment in resources (human, material, financial) is therefore needed to collect information, as indicated above.

4. Resources dedicated to risk management and emergency measures within organizations (resources that would be able to provide information on interdependencies) are often limited and already very busy managing outages or incidents that might affect the system. When one also considers that breakdowns related to interdependencies are not very common, it is easy to explain why an organization would not invest more resources in this problem. There is therefore a real problem of resources in accessing information.
5. Information may be held by one or more people who have left the organization or changed departments (retirement, resignation, promotion, new job, etc.). This raises the issue of tacit knowledge management, organizational memory and knowledge transfer. Information can "get lost" when an employee leaves an organization.
6. Organizational or technological changes can also make it hard to access information. Organizational changes can lead to new projects or new guidelines, and employees may then lose interest in a specific issue, such as interdependencies among TSPs. Similarly, in the case of technological change, employees may start using new tools, in which case training is likely to emphasize the new tool to the detriment of existing ones. The preservation of information may then be in danger in the sense that fewer and fewer people will need to use it regularly.

3.2. Sensitivity of information

Information sensitivity is another major impediment to the sharing among TSPs of information regarding their interdependencies.

More specifically, some information is considered to be confidential within an organization. Confidentiality may be justified, but it always means that it is difficult for an organization to share information with others.

There are three main reasons why some information is confidential:

1. Service contracts between a TSP and certain customers (e.g., banks, hospitals, etc.) may prohibit the TSP from disclosing information concerning its system to other parties (e.g., other TSPs).
2. Organizations may wish to protect certain information by means of confidentiality agreements due to the competitive environment characterizing the telecommunications sector. Organizations distrust each other, and it is considered unprofessional for an organization to share information with its competitors. The fear of losing a competitive advantage or market share or seeing a strategic orientation disclosed is ever present and may deter TSPs from sharing information about their interdependencies.
3. In today's security context, certain information is confidential due to the risks inherent in disclosing it (Robert and Morabito, 2010). The disclosure of information may represent an additional vulnerability for a system if this information is not suitably protected or if it is misused, especially if the information concerns the vulnerability of certain infrastructures. For example, knowing the precise location of a

telephone exchange that is particularly critical for a TSP may represent a real danger if the information is used to harm it. In addition, on the scale of a group of TSPs, a general analysis of their interdependencies involves pooling information from different organizations. The pooling of information that is not in itself confidential may lead to the creation of more general information that could become confidential because it is extremely critical and would therefore represent a real risk if it were disclosed.

3.3. Complexity of information

Another impediment to the sharing of information among TSPs about their interdependencies is related to the information's complexity.

Telecommunication systems are highly complex and automated. The system's reaction in certain situations may therefore be difficult to predict. For example, in response to the same triggering event, a given system may react differently depending on its configuration and use at that specific time, such that one cannot say what might be the consequences associated with a given hazard without performing a more in-depth analysis. In these circumstances, the misinterpretation of a single piece of technical data may lead to incorrect conclusions in analyses of interdependencies among TSPs. The TSPs involved could then be held liable, which is evidently not a desirable situation.

3.4. Ignorance of information

The last factor making the sharing of information on interdependencies among TSPs more difficult is ignorance of information.

Given customers' strong demand for increasingly inclusive, high-performance services, telecommunications is a sector marked by extremely fast technological change. Under these circumstances, most of the TSPs' energy is focused on improving their systems' performance and deployment. This situation means that the commissioning of new technologies, equipment, or even updates is not always preceded by a systematic study of the effects of these changes on how the system itself functions, let alone the functioning of neighbouring systems. The speed with which changes occur makes it difficult to keep track of them all. The result is a certain "loss of control" over information which, even though it is minimal at each stage, increases as the infrastructure changes, modernizes and becomes more complicated.

3.5. Summary of impediments to information sharing

Table 1 summarizes the impediments to information sharing identified above.

Difficulty of accessing information	Sensitivity of information	Complexity of information	Ignorance of information
Lack of mandate	Confidentiality under contractual agreements	Risk of misinterpreting technical data	Speedy technological development focused on system performance that does not make the study of interdependencies a priority
Dispersed information, not always clearly or systematically indexed	Distrust due to competitive environment		
Silo mentality in organizational culture	Risks related to today's security environment		
Unavailability of resources (human, material, etc.)			
Staff mobility			
Organizational and technological changes			

Table 1: Impediments to information sharing

IV. Toward a Framework For Exchanging and Sharing Information

In the context of reluctance to exchange information, it seems appropriate to work on a framework for exchanging and sharing information that is dedicated to TSPs. By framework for exchanging information, we mean a set of rules that define who should exchange information, what information should be exchanged, what form it should take, etc. Establishing a framework for information exchanges that takes into consideration the identified impediments to the sharing of information should make it easier for TSPs to collaborate in order to enhance the resilience of telecommunication systems.

Understanding the impediments to TSPs' sharing of information about their interdependencies is one of the first steps in defining the problem and building a good understanding of what conditions must be respected in defining such a framework. For example, it is recommended that a framework for exchanging information among TSPs stipulate that information related to the vulnerability of a specific telecommunication system should never be manipulated due to the competitive environment in the sector. The sensitivity of the information shared should therefore be reduced to the absolute minimum, given that sensitivity can be an impediment to information sharing. To facilitate access to information, which is another impediment to information sharing, it is also recommended that the information TSPs are asked to integrate into an exchange framework should always be targeted, minimized and justified.

A study by the *Centre risque & performance*, in partnership with Industry Canada and the Centre des services partagés du Québec, is currently working to define such a framework for information exchanges among TSPs. This project is expected to continue until May 2016. The next step will be to address the question of a mandate to manage such an information exchange framework.

References

Arnoux, J. (2015). Les défis du partage d'informations entre des fournisseurs de services de télécommunications interdépendants. (M.Sc.A. thesis, École Polytechnique de Montréal, Canada). Accessed at http://www.polymtl.ca/crp/recherche/memthese.php

CRTC. (2005). *Canadian Telecommunications Policy Review* (Discussion paper). Accessed at http://publications.gc.ca/collections/Collection/BC92-58-2005E.pdf

CRTC. (2013). *Communications Monitoring Report.* Accessed at http://www.crtc.gc.ca/eng/publications/reports/policymonitoring/2013/cmr2013.pdf

CRTC. (2014). *Communications Monitoring Report.* Accessed at http://www.crtc.gc.ca/eng/publications/reports/PolicyMonitoring/2014/cmr.pdf

CRTU (2013). Exercices de la série Simba-Nicky (SN1 à SN3), Rapport final : version pour approbation par le CRTU, Rapport confidentiel, Industrie Canada, 2013.

Government of Canada. (2009). *National Strategy for Critical Infrastructure.* Accessed at http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/srtg-crtcl-nfrstrctr-eng.pdf

Peerenboom, J.P., Fisher, R.E., Rinaldi, S.M., and Terrence, K.K. (2002). Studying the chain reaction. *Electric Perspectives, 27*(1), 22–35.

Rinaldi, S.M., Peerenboom, J.P., and Kelly, T.K. (2001). Identifying, understanding, and analyzing critical infrastructures interdependencies. *IEEE Control Systems Magazine, 21*(6), 11–25.

Robert, B., and Morabito, L. (2008). The operational tools for managing physical interdependencies among critical infrastructures. *International Journal of Critical Infrastructures, 4*(4), 353–367.

Robert, B., and Morabito, L. (2010). An approach to identifying geographic interdependencies among critical infrastructures. *International Journal of Critical Infrastructures, 6*(1), 17–30.

Schiller, D. (2003). Télécommunications, les échecs d'une révolution. *Le Monde diplomatique, 50*(592), 28–29. Accessed at http://www.monde-diplomatique.fr/2003/07/SCHILLER/10269

Biographies

Benoît ROBERT *is a civil engineer, professor and director of the Centre risque & performance, a research centre dedicated to the integration of risks in the evaluation of the performance of critical infrastructure (CI). The Center specializes in the study of cross-sector interdependencies and domino effects between CI, namely the energy, telecommunications, water and transportation sectors. Professor Robert has developed an expert system of interdependency modeling currently being applied by the civil security authorities of the City of Montréal in collaboration with the ministère de la Sécurité publique du Québec.*

He is also leading a research project in collaboration with Defense Research & Development Canada, Industry Canada and the Centre de services partagés du Québec. This project aims at developing a sharing information framework for the telecommunications sector in order to better understand and potentially model keys functional interdependencies between the main Canadian and regional stakeholders of this sector.

Professor Robert has also developed a resilience methodology for the critical systems of the Province of Québec with numerous governmental partners and organizational resilience indicators. In addition to his research activities, Professor Robert teaches technological risk management, emergency and business continuity planning and organizational resilience engineering.

Justine ARNOUX *holds a French industrial engineering degree (2015) and a Master degree in industrial engineering (2015) from Polytechnique Montréal. She was a student at the Centre risque & performance from January 2014 to August 2015 and worked on the challenges of information sharing between telecommunications service providers about their interdependencies. It was her Master thesis' topic.*

Justine is now looking for new challenges in risk management, business continuity and associated professional fields.

Luciano MORABITO *holds a Bachelor in electrical engineering with a speciality in telecommunications (2002) and a Master degree in industrial engineering and management of technological projects (2004) from Polytechnique Montréal. Since 2004, he works as a research associate at the Centre risque & performance where he is responsible for the development of new methodologies and operational tools for managing interdependencies and modeling domino effects among critical infrastructures.*

Risk Mitigation Strategies for Large Power Transformers

Kenneth Friedman, Ph.D.*
Senior Policy Advisor
Office of Electricity Delivery and Energy Reliability
U.S. Department of Energy

*Tiffany Choi***
Technical Specialist
ICF International

Abstract

Large Power Transformers (LPTs)[1] have long been a concern for the North American electricity industry because simultaneous failures of multiple LPTs could lead to extensive loss of load and considerable economic damage, including replacement and other collateral costs; yet a timely replacement of multiple, failed transformers presents industry with a great challenge because of the complex and lengthy process involving the procurement, design, manufacturing, and transportation of LPTs. The electric power grid is one of the critical life-line functions on which many other critical infrastructures depend, and the impairment of this infrastructure can have a significant economic and security impact. The electric power infrastructure faces a wide variety of possible threats, including natural hazards, cyber and physical security threats, and space weather. While the potential impact of these threats on the infrastructure is uncertain, public and private stakeholders in the energy industry are considering a variety of risk management strategies to mitigate the risk. In this paper, authors examine issues surrounding LPTs and assess various related risk mitigation strategies.

I. BACKGROUND

The North American electric grid faces various high-impact, low-frequency (HILF) risks, including a coordinated cyber and physical attack and a severe geomagnetic disturbance (GMD) or electromagnetic pulse (EMP) event that could damage a difficult-to-replace generating station and substation equipment causing a cascading effect on the system.[2] The electricity industry has long embraced resilience as part of continuity of operations planning, risk management, and has built reliability and redundancy into the system; however, the limited availability of spare LPTs could present a challenge in the event of multiple LPTs failing simultaneously. That is because multiple LPT failures could result in a long-term service interruption and considerable economic loss, yet the quick replacement of multiple, failed transformers can be difficult.

LPTs are custom-engineered equipment that entail a significant capital expenditure and long lead times due to an intricate design, procurement and manufacturing process. Although prices vary by manufacturer and by size, an LPT can cost millions of dollars and weigh hundreds of thousands of pounds. The engineering design, procurement and manufacturing of LPTs are complicated processes that include the prequalification of manufacturers, a competitive bidding process, and the purchase of raw materials (see figure 1). The result is the possibility of an extended lead time that could stretch beyond 20 months if the manufacturer has difficulty obtaining certain key parts or materials or if there are large number of orders in queue. High-voltage bushings are known to have long lead times and limited supplier sources. Two raw materials, copper and electrical steel, account for more than half of the total cost of

[1] Throughout this report, the term LPT is broadly used to describe a power transformer with a maximum nameplate rating of 100 megavolt-amperes (MVA) or higher unless otherwise noted. However, it should be noted that there is no single, absolute, industry definition or criteria for what constitutes an LPT and that additional specifications are often used to describe different classes of LPTs.

[2] "High-Impact, Low-Frequency Event Risk to the North American Bulk Power System," NERC, June 2010, http://www.nerc.com/pa/CI/Resources/Documents/HILF%20Report.pdf (accessed December 4, 2015).

materials of an LPT and are critical to the efficiency and performance of the equipment. However, there are a limited number of suppliers, and the price volatility of these two commodities in the global market can affect the manufacturing condition and procurement strategy for LPTs.

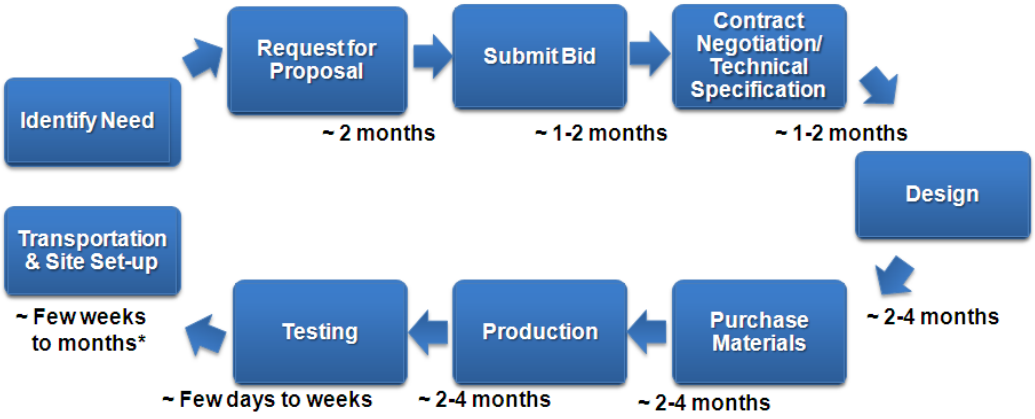

Figure 1. Large Power Transformer Procurement Process and Estimated Lead Time

Note: This figure illustrates an optimal flow of the procurement and manufacturing processes and estimated lead time, which can extend beyond the estimated time frame shown.

* Variable depending on distance and logistical issues.

Source: USITC and industry estimate

Transportation of an LPT also presents a challenge due to its large dimensions and heavy weight which pose unique requirements to ensure safe and efficient transportation. Current road, rail, and port conditions are such that transportation is taking more time and becoming more expensive.[3] Although rail transport is most common, long-distance LPT moves usually require multiple modes of transportation. Access to a railroad is becoming an issue in certain areas due to the closure, damage, or removal of rail lines. Damage to LPT's on the U.S. rail system can occur due to g-force impacts, and rail sidings can present a challenge. When an LPT is transported on the road, it requires special permits from each state on the route of the LPT being transported. Obtaining these special permits can require an inspection of various infrastructure (e.g., bridges), which can add delay. In addition, transporting LPTs on the road can require temporary road closures due to traffic issues, as well as a number of crew and police officers to coordinate logistics and redirect traffic.

Recognizing the limited availability and difficult transport logistics of LPTs as potential challenges for electric grid resilience, both the public and private sectors have been undertaking a variety of efforts to address this concern. This paper provides a high level summary of some of the key activities that are underway in the government and in the industry to mitigate the risk associated with losing multiple LPTs.

II. Transformer Transportation Working Group

In 2014, the electricity industry convened the Transformer Transportation Working Group (TTWG) in coordination with the Electric Subsector Coordinating Council and its Senior Executive Working Group to develop an industry action plan on

[3] Siemens, Transformer Lifecycle Management, http://www.energy.siemens.com/mx/pool/hq/services/power-transmission-distribution/transformer-lifecycle-management/TLM_EN_.pdf (accessed December 4, 2015).

the movement of LPTs.[4] The TTWG has been tasked with identifying essential government and private sector partners and their specific capabilities to help enhance and expedite the efficient and secure movement of LPTs.[5]

In 2015, the TTWG analyzed transportation stages by breaking down typical rail, road, and barge movements into specific sub-components and activities to highlight potential transportation bottlenecks and support missions. The TTWG identified the following high priority recommendation areas: streamline permitting and clearance process, prioritize access to transportation assets and infrastructure, conduct joint industry government exercises and drills, and ensure security needs are met.[6]

This utility industry group is further engaged in extensive outreach with the transportation industry, in particular Class I railroads, to address transformer transportation challenges. The utility industry is expanding information sharing between utilities and transportation entities, developing emergency playbooks and support guides, and performing exercises and drills. To date, the industry has received significant support and cooperation from the railroad industry in this effort, including evaluating the inventory and availability of, and priority access to, specialized rail equipment needed to transport transformers. Under emergency conditions, the utility and transportation industries would make every effort possible to expedite the movement of critical transformers.

III. U.S. National Strategies related to Large Power Transformers

In 2015, U.S. Administration recommended that the U.S. Department of Energy (DOE) "analyze the policies, technical specifications, and logistical and program structures needed to mitigate the risks associated with loss of transformers" in the *Quadrennial Energy Review (QER): Energy Transmission, Storage, and Distribution Infrastructure*. Specifically, the Administration has made it a priority to work toward "increasing the security and resilience of the electric grid, including the development of an integrated national plan to mitigate challenges pertaining to aging power transformers, the cyber and physical security of transformers, and the vulnerabilities of large power transformers."[7]

Per this recommendation, DOE has worked with energy sector partners to develop a national strategy to reduce risk associated with the loss of LPTs. The goal of this effort is to secure a critical element of the nation's electric power grid through a public-private partnership and in collaboration with the electricity and manufacturing industries in the United States and in Canada. This strategy aims to reduce risk to grid reliability posed by the loss of critical LPTs, with a focus on three main areas:

1. Understanding and mitigating current and future risks to LPTs through an analysis of threats, vulnerabilities, and consequences;
2. Enhancing protection of LPTs by sharing best practices, and improving protection and hardening technologies; and
3. Ensuring efficient mechanisms are available to replace damaged equipment by working with the electricity industry, transformer manufactures and transporters, as well as Canadian stakeholders.

Further, the QER specifically recommended DOE to consider the "development of one or more transformer reserves through a staged process."[8] DOE

[4] The working group consists of a functional cross-section of transmission engineering and operations, mutual assistance, spare equipment, logistics, and security executives along with subject matter experts from the major sectors and trade associations of the electric utility industry.
[5] EEI Transformer Transportation Working Group, 2015.
[6] Ibid.

[7] Quadrennial Energy Review: Energy Transmission, Storage, and Distribution Infrastructure, the White House, April 2015, http://energy.gov/sites/prod/files/2015/04/f22/QER-ALL%20FINAL_0.pdf (accessed December 4, 2015).
[8] Ibid.

is working to address this concept through the evaluation of a potential national strategic reserve of power transformers. Specifically, this analysis will include the following elements:[9]

- The appropriate number of spare LPTs and total capacity in MVA necessary to maintain the current level of reliability of the electric grid;
- The consideration of tradeoffs regarding the level of reliability and the number of spare transformers;
- An engineering analysis on the potential locations of spare transformers, taking into account current system operational parameters;
- A review of common substation designs and identifications of the types of transformers to be maintained in a strategic transformer reserve;
- An operational research analysis examining the logistics of transportation, installation, and energization of spare LPTs to enable greatest efficiency; and
- A comparison of alternative criteria for withdrawal of spare LPTs from the strategic transformer reserve to replace critically damaged LPTs, including the consideration of related existing industry programs.

IV. Industry Consortium-led Transformer Sharing Programs

Three key industry-wide transformer sharing programs exist in North America — Edison Electric Institute (EEI)'s Spare Transformer Equipment Program (STEP), SpareConnect, and the North American Electric Reliability Corporation (NERC)'s Spare Equipment Database (SED) Program, all of which are designed to provide ways in which utilities may identify and voluntarily share spare transformers and other related equipment across North America in the event of an emergency.[10]

In 2006, EEI, the main trade association for U.S. investor-owned electric utilities established the STEP to cost-effectively increase reliability, particularly in deliberate destruction of electrical transformers in a terrorist event.[11] Although a triggering event is limited to an act of terrorism as declared by the President, the STEP provides a ready mechanism for participating utilities to voluntarily share assets in the event of other catastrophic loss. The U.S. Federal Energy Regulatory Commission (FERC) granted blanket authorization for the transfer and cost recovery of transmission equipment under the STEP program in September 2006.[12] As of 2015, 56 transmission providers that represent about 70 percent of the transmission grid were participating in this program.[13]

In 2012, NERC initiated the SED program, which is a confidential web-based catalog of spare transformers rated at 100 kV or higher. Unlike EEI's STEP program, however, the SED program has not been granted pre-approval from FERC or state regulators for equipment transfers. Thus, the ability to transfer the ownership of transformers from one company to another may require additional approvals, even during an emergency. As of March 2015, 34 entities were participating in the SED Program, and together they held 165 transformers with a total of 33,700 MVA.[14]

---

[9] The consideration of national strategic transformer reserve is a part of DOE's grid modernization laboratory call. Task 6.5.4 - Strategic Transformer Research of the Department of Energy's Grid Modernization Laboratory Call, http://www.netl.doe.gov/File%20Library/Business/solicitations/2016GMLabCall.pdf (accessed December 4, 2015).

[10] For more information, see http://www.eei.org/issuesandpolicy/transmission/Pages/sparetransformers.aspx and http://www.nerc.com/pa/RAPA/sed/Pages/Spare-Equipment-Database-(SED).aspx (both accessed December 4, 2015).

[11] This program only goes into effect when the President of the United States declares an event to be a terrorist attack.

[12] Federal Energy Regulatory Commission, Order on Application for Blanket Authorization for Transfers of Jurisdictional Facilities and Petition for Declaratory Order, Docket Nos. EC06-14-000 and EL06-86-000, September 22, 2006.

[13] Spare Transformers, EEI, http://www.eei.org/issuesandpolicy/transmission/Pages/sparetransformers.aspx (accessed December 4, 2015).

[14] NERC Spare Equipment Working Group, 2015.

Launched in 2014, EEI's SpareConnect is another transformer sharing initiative, which complements the above-mentioned programs and voluntary mutual assistance programs.[15] SpareConnect provides decentralized access to points of contact at power companies to enable its participants to connect quickly with other members of the program, in the event of an emergency, for possible sharing of transmission and generation step-up transformers and related equipment, including bushings, fans and auxiliary components.[16] SpareConnect's membership represents U.S. investor-owned utilities, public power utilities, electric cooperatives, joint action agencies, federal power marketing agencies, merchant generators, and Canadian public and private electric utilities.

V. Proposed National Spare Transformer Program

In June 2015, eight electric utilities proposed to create a national stockpile of spare transformers and other essential grid equipment through a stand-alone company, Grid Assurance LLC.[17] As proposed, Grid Assurance would purchase large, mobile transformers and other equipment and maintain them at secured strategic locations in the United States. The stored equipment would be available to participants, who would pay a cost-based subscription fee.

Grid Assurance petitioned and FERC granted that utilities' participation in Grid Assurance would be a permissible resiliency element of a physical security plan for NERC's mandatory critical infrastructure protection (CIP) 014-1 standard.[18] FERC further established that FERC's prior authorization is not required for the purchase and sales of spare equipment from Grid Assurance that is not in service at the time it is transferred. However, FERC did not acknowledge the "cost-effectiveness" of the sparing service because FERC could not determine whether costs incurred under the sparing service would be just and reasonable.[19] Contingent on regulatory approvals, Grid Assurance is expected to launch sometime in 2016.[20]

VI. Individual Utility Emergency Spare Strategies[21]

Utilities have implemented various combinations of spare transformer strategies, including the stocking of interchangeable spare transformers, the ordering of conventional spares in advance, and the early retirement of conventional transformers for use as spares. This section provides several utility emergency spare approaches based on interviews with and surveys of a number of utilities and stakeholders of different sizes and geographic locations across North America.

Utilities stock conventional spares that are equivalent and interchangeable to their critical transformers. While they are typically used for reliability purposes, these transformers can also be used as emergency spares as needed. Under this approach, the spares are identical to those transformers

---

[15] About, SpareConnect, http://spareconnect.org/about/ (accessed December 4, 2015).

[16] "SpareConnect," September 10, 2014, http://www.nreca.coop/wp-content/uploads/2015/02/spareconnect_flyer_9_11_2014_draft.pdf (accessed December 4, 2015).

[17] For more information, see Grid Assurance at http://gridassurance.com/ (accessed December 4, 2015).

[18] "Petition for Declaratory Order and Request for Expedited Action," Grid Assurance filing at the FERC, June 9, 2015, http://gridassurance.com/lib/docs/20150609-5141(30632101).pdf (accessed December 4, 2015).

[19] "Sparing service" has a meaning as delineated in the following: http://www.energy.gov/sites/prod/files/2015/09/f26/Grid%20Assurance_Submission_RFI_Transformer%20Reserve.pdf (accessed December 4, 2015).

[20] "Order on Petition for Declaratory Order," FERC, August 7, 2015, http://www.ferc.gov/CalendarFiles/20150807160548-EL15-76-000.pdf (accessed December 4, 2015).

[21] This section provides a high level summary of emergency spare strategy provided in the following report: "Considerations for a Power Transformer Emergency Spare Strategy for the Electric Utility Industry," Prepared by the Electric Power Research Institute for the U.S. Department of Homeland Security, September 30, 2014, http://www.dhs.gov/sites/default/files/publications/RecX%20-%20Emergency%20Spare%20Transformer%20Strategy-508.pdf (accessed December 4, 2015).

to be replaced and often stored at the substation next to existing transformers. This allows for quick energization without the transformer being moved; however, due to the close proximity of such spares to the existing transformers, these spares are also exposed to potential HILF physical attacks.

Another approach is ordering conventional spares earlier than needed for critical substation nearing the end of their service lives. This way, utilities can secure in advance a spare that they will certainly need eventually. In this approach, utilities assess the health and the probability of failure of each transformer to project the remaining life of the transformer. Such assessment enables a cost analysis, as well as the estimation of return on investment. It should be noted, however, that spare transformers need a fair bit of maintenance.

In this last approach, some utilities retain retired transformers to repurpose them as emergency spares. These are transformers that have retired, but not failed, which would allow them to be used as temporary spares until a new transformer is manufactured and transported.

To complement these emergency spare strategies, some utilities have adopted internal programs to manufacture and store conventional spare power transformers for their power system or have entered into informal sharing arrangements with neighboring utilities.

VII. REGIONAL AUTHORITY-DIRECTED TRANSFORMER LOSS MITIGATION

The Independent System Operators (ISOs) or Regional Transmission Organizations have diverse views on their involvement in utility emergency transformer spare programs. While some indicated no involvement in the spare transformer strategy, at least one ISO indicated that it directs the purchase of spares by transmission owners in its operating territory based on probabilistic risk assessment.[22] This assessment incorporates the state or health of transformers, as well as the probability of natural disasters, such as hurricanes and tornados. Although further work is needed to include other HILF events, such as physical attacks, the inclusion of severe weather probabilities makes it an applicable strategy for emergency spares to some extent.[23] In addition to power transformers, equipment critical to the integrity of the grid known to have long lead times should be supported by a spare.[24]

The broad availability of emergency spare transformers, such as the national transformer reserve program suggested in the QER, could be an important complement to existing transformer sharing or emergency spare programs. However, some utilities expressed reservations with collaborative programs, including concerns about sharing assets that the utility fully financed, the practicality of transporting spares over long distances, impedance mismatching, and information confidentiality.[25]

VIII. NERC RELIABILITY STANDARDS

Three NERC Reliability Standards have been developed in the past few years and approved by FERC, in an effort to enhance the resilience of the grid. Specifically, a new Reliability Standard, EOP-010-1—Geomagnetic Disturbance Operations, became effective in April 1, 2015, requiring certain reliability coordinators and transmission operators to develop procedures to help mitigate the effects GMDs have on the grid.[26] The standard directs reliability coordinators to develop and implement operating procedures that

---

[22] "Spare Equipment Philosophy for Bulk System Network Facilities and Interfaces," Section IV of PJM Transmission and Substation Design Subcommittee Technical Requirements, PJM, 2002.

[23] "Considerations for a Power Transformer Emergency Spare Strategy for the Electric Utility Industry," Prepared by the Electric Power Research Institute for the U.S. Department of Homeland Security, September 30, 2014.

[24] PJM, 2002.

[25] "Considerations for a Power Transformer Emergency Spare Strategy for the Electric Utility Industry," Prepared by the Electric Power Research Institute for the U.S. Department of Homeland Security, September 30, 2014.

[26] Reliability Standard for Geomagnetic Disturbance Operations, FERC Order No. 797, June 19, 2014, http://www.ferc.gov/whats-new/comm-meet/2014/061914/E-18.pdf (accessed December 4, 2015).

can mitigate the effects of GMD events. The standard also directs reliability coordinators to distribute space weather information to enable coordination and consistent awareness throughout the area. Finally, the standard directs transmission operators to develop GMD operating procedures and processes that are tailored to each operator's respective system.[27]

Another NERC Reliability Standard, CIP-014-1—Physical Security, became effective October 1, 2015, to address the physical security threats to and vulnerabilities of the U.S. power grid.[28] This standard provides a structured framework that focuses on the most critical facilities and incorporates risk management planning to mitigate the threats and vulnerabilities related to each identified critical asset.

A third NERC Reliability Standard, TPL-001-4—Transmission System Planning Performance Requirements, was developed in an effort to enhance the resilience of the grid. This Reliability Standard requires Planning Coordinators and Transmission Planners to study the impact on system performance of a spare equipment strategy that could result in the unavailability of major transmission equipment that has a lead time of one year or more (such as a transformer). This requirement will become effective January 1, 2016.[29]

IX. Manufacturers' Research and Development Initiatives

Power transformer manufacturers have been continuously working to enhance their products and transformer designs for utmost reliability. As such, a number of manufacturers are exploring the research and development (R&D) of mitigation and hardening options, including the consideration of parts that are more resilient to potential threats, as well as protective devices.

Based on discussions with power transformer manufacturers, they are working to ensure that their products meet the needs of their customers today and in the anticipated future, and that transformers can operate under expected or normal operating conditions, as well as in emergency situations. Some of the R&D areas include: alternate materials and designs to improve resilience; physical hardening of transformers; on-line or remote monitoring devices for LPTs; explosion proof transformers; transportable or mobile transformers; transformers with armored panels to prevent ballistic damage; improving thermal performance; and using non-magnetic materials. At least one manufacturer has launched a transformer and grid resilience program, offering assessment, hardening, monitoring, and rapid response/replacement services.[30]

Some manufacturers are also engaged in the development of flexible spare transformers of various types, such as the Recovery Transformers (RecX). The U.S. Department of Homeland Security's (DHS), the Electric Power Research Institute, ABB, and CenterPoint Energy (CNP), developed RecX, a prototype EHV transformer that would drastically reduce the recovery time associated with EHV transformers. The RecX is lighter (approximately 125 tons), smaller, and easier to transport and quicker to

[27] "Project 2013-03 Geomagnetic Disturbance Mitigation," NERC, http://www.nerc.com/pa/Stand/Pages/Project-2013-03-Geomagnetic-Disturbance-Mitigation.aspx (accessed December 4, 2015).

[28] "Physical Security Reliability Standard (Final Rule)," Federal Register, November 25, 2014, https://www.federalregister.gov/articles/2014/11/25/2014-27908/physical-security-reliability-standard#p-4 (accessed December 4, 2015).

[29] Another new NERC Reliability Standard, TPL-007-1 — Transmission System Planned Performance for Geomagnetic Disturbance Events, has been filed at the FERC in May 2015. See http://www.ferc.gov/whats-new/comm-meet/2015/051415/E-1.pdf (accessed December 4, 2015).

[30] ABB, "Transformer and Grid Resiliency and Recovery," May 21, 2015, http://www04.abb.com/global/usabb/usabb045.nsf!OpenDatabase&db=/global/usabb/usabb049.nsf&v=1A6E&e=us&url=/global/seitp/seitp202.nsf/0/C91D04B865AD629885257E4C004FAABA!OpenDocument (accessed December 4, 2015).

install than a traditional EHV transformer. The RecX has been operating in CNP's grid since March 2012, after a successful exercise that included the transportation, installation, assembly, commissioning and energization of the transformer in less than one week. The RecX is a 345:138kV, 200 MVA per phase transformer (equivalent to 600 MVA) and was designed to be an applicable replacement for more than 90 percent of transformers in this voltage class, which is the largest voltage class of EHV transformers.[31]

Some utilities are working with manufacturers to establish agreements in advance to expedite the manufacturing of transformers if needed. Such an agreement may involve manufacturer's pre-ordering and stocking of parts with long lead times, having a master agreement or transformer design in advance, or negotiating reduced lead times in case of an emergency. However, it should be noted that an agreement that provides one utility higher priority delivery might increase the lead-time for another utility, due to finite production capability, therefore, this may not improve the overall response time to meeting all utilities' transformer orders.[32]

At least one company seeks to fill an industry's need for spare transformers by offering a transformer rental program in which spare transformers in a range of voltages are available for rent to utilities across the United States in exchange for fees.[33] In this transformer rental model, the company would maintain an inventory of spares at regional distribution centers close to covered assets, so that transformers could be rapidly transported and installed at utility sites as needed.

Other companies offer temporary mobile substations and portable spare transformer units that can be quickly deployed in case of an emergency, such as a natural disaster or a terrorist attack, as well as during routine maintenance or equipment failure. The use of mobile substations and transformers as spares offers certain beneficial features that normal spares may not offer, such as the off-site storage that may provide protection from physical attacks, the flexibility of adjustable configuration, as well as reduced time in deployment and installation.[34] Such mobile substations may be ideal for use in temporary power restoration for critical infrastructure and sites, such as hospitals, shelters, and water pump stations.

X. Concluding Remarks

The electric power grid is one of the critical life-line functions on which many other critical infrastructures depend, and the impairment of this infrastructure can have a significant economic and security impact. The electric power infrastructure faces a wide variety of possible threats, including natural hazards, cyber and physical security attacks, and space weather. Despite the numerous ongoing efforts to mitigate risks associated with losing multiple LPTs, public and private stakeholders in the energy industry continue to evaluate a variety of existing and possible risk management strategies to mitigate the potential impact of various HILF events.

Biographies

***Dr. Friedman** is a Senior Policy Advisor in the Office of Electricity Delivery and Energy Reliability, Infrastructure Security and Energy Restoration Division at the U.S. Department of Energy (DOE). He has over 35+ years of experience in energy policy and analysis, including efficiency, renewable energy, and climate change. Currently, he acts as the lead DOE point of contact in*

[31] For more information about RecX, see: http://www.dhs.gov/files/programs/st-snapshots-prototyping-replacement-ehv-transformers.shtm and http://www.nytimes.com/2012/03/15/business/energy-environment/electric-industry-runs-transformer-replacement-test.html?_r=1 (both accessed December 4, 2015).

[32] "Considerations for a Power Transformer Emergency Spare Strategy for the Electric Utility Industry," Prepared by the Electric Power Research Institute for the U.S. Department of Homeland Security, September 30, 2014.

[33] For more information, see Wattstock at http://www.wattstock.com/ (accessed December 4, 2015).

[34] For example, see Delta Star at http://www.deltastar.com/default.aspx (accessed December 4, 2015).

critical infrastructure protection in working with government and private sector partners in the implementation of the Presidential Policy Directive-21 Critical Infrastructure Security and Resilience, including the development of the Energy Sector Specific Plans. He works with sector partners including Canada in addressing new and emerging threats, such as space weather, HEMP and geomagnetic disturbances, and coordinated physical or cyberattacks. His other experiences include direct support to senior DOE management, including Assistant Secretaries and their Deputies, as well as serving as Director of the Energy Technology Policy Division at the International Energy Agency in Paris, France.

Dr. Friedman is the winner of the Eric Peterson Award from the Office of Energy Efficiency and Renewable Energy for analytical contributions to DOE and the winner of the 2006 Outstanding Performance Award in the Office of Electricity Reliability and Energy Delivery. He received his master's and Ph.D. from Michigan State University.

***Ms. Choi** is a Technical Specialist at ICF International, with more than 10 years of experience in the realm of energy infrastructure security and resilience. She has been instrumental in the development of the Energy Sector Specific Plans (2007, 2010, and 2015), the facilitation of energy sector public-private partnership, and the implementation of subsequent energy resilience policies and programs. She was one of the lead authors of key DOE publications relating to energy infrastructure issues, including Dams and Energy Sectors interdependency, insurance's role in energy infrastructure security and resilience, and large power transformers in the electric grid. She obtained her bachelor's degree from the University of Virginia.*

Space Weather Forecasting for the Electrical Power Grid

C. C. Balch
NOAA Space Weather Prediction Center
Email: christopher.balch@noaa.gov

I. INTRODUCTION

On March 13, 1989, one of the most severe geomagnetic storms of the modern era led to a large number of anomalies in the North American bulk power system, including a power outage of about nine hours duration in the Hydro-Quebec system, as well as severe damage to the Public Service Electric and Gas Salem Unit 1 generator step up transformers in Delaware Bay [see *North American Electrical Reliability Corporation (NERC)*, 1990 for a compilation of effects]. Section two of the NERC report reviews events leading to the Hydro-Quebec blackout and describes the difficulties in restoring power primarily due to equipment damage. Specific equipment affected included two generating step up transformers (due to overvoltage), surge arrestors, a shunt reactor, and static VAR compensators. The restoration of power was challenging and required assistance from external electrical power providers, as well as "voluntary reduction from certain industrial customers". Further descriptions may be found in *Czech et al.* [1989].

About a week after the storm, Public Service Electric and Gas discovered an "alarming increase in the total combustible gas content in the oil" in one of its generator step-up transformers at the Salem nuclear power plant. Subsequent visual inspection of the failed transformers showed 'severe damage', described in detail in section three of the NERC report. The report describes additional anomalies at this operating location, and uses measured reactive load during the storm to infer a geomagnetically induced current of about 224 Amps (~75 Amps per phase) [see also *Balma*, 1989].

The storm affected other parts of the bulk power system as well. Section five of the NERC report catalogues an extensive set of widespread anomalies, suggesting a very busy period for power system operators. Included in the list are negative sequence alarms, transformer noise, tripping of equipment, phase unbalance alarms, substantial swings in reactive load, and voltage control problems. Of the 211 events in the log, about 2/3 reference specific impacts on equipment. The regions reporting effects were diverse, including Quebec, Manitoba, British Columbia, Northeastern U.S., Virginia, Ohio, Wisconsin, Minnesota, North Dakota, Washington (state), and the WAPA operating area.

Although the March 1989 storm was certainly a 'wake-up call' for these kinds of effects, the phenomena of geomagnetically induced currents (GICs) had been discovered much earlier. The first published record promptly follows the deployment of the telegraph, effectively the first time nature was provided an artificial conducting pathway for the currents induced by geomagnetic storms [*Barlow*, 1849; *Prescott*, 1866]. Likewise, not too long after the deployment of long conductors for electrical power, GICs were noticed in the grid [*Davidson*, 1940]. A careful review of published reports back to 1847 by Boteler et al. shows that GICs have had an ongoing impact on human technologies that use long conductors since their inception [*Boteler et al.*, 1998].

Since March 1989, the bulk power grid has continued to grow steadily [*National Research Council*, 2008]. Today's grid, however, has not been exposed to a geomagnetic storm as large as March 1989, underscoring the importance of assessing how this critical infrastructure will respond to the inevitable

reoccurrence of a storm of at least this size, and to anticipate the response to the most severe conditions one might reasonably anticipate over a long interval of time, e.g. a one-in-one-hundred year event. Determining how large such an event might be is difficult due to the lack of an extended record of detailed geomagnetic field observations. The development of appropriate 'benchmark' space weather events was identified by a recent report, the U.S. National Space Weather Strategy [*National Science and Technology Council*, 2015], as a key goal, and highlights the need for further work to address this question.

Mitigation strategies tend to fall into two classes. The first of these is accomplished through system analysis, modeling and design. Systems planning engineers can apply a benchmark geo-electric field time series to their system model, calculate the GIC in the system, and use their model to identify vulnerable components where hardware modifications may be advisable. The second approach uses forecasts of geomagnetic activity together with real-time monitoring to strategically operate the system during geomagnetic storms. A general template of storm-time operating procedures was developed by the *North American Electrical Reliability Corporation (NERC)* [2013]. This document discusses some generally accepted practices, but also advises operators to carry out a GIC impact study on their specific system.

Forecasting geomagnetic activity poses a significant challenge to the agencies charged with this task. Science-based prediction techniques must consider the full series of cause-and-effect that ultimately leads to these disturbances. For each link in the chain, forecast accuracy is necessarily limited by available observations, as well as the state of knowledge and modeling of the physical processes involved. A succinct description of the space weather phenomena that leads to these storms was provided previously by Fiori et al. [2015]. In this paper we focus more specifically on the phenomena as they relate to geomagnetic forecasting in the context of current capability, to give the reader a sense of what is known and not known in the forecast analysis process.

II. Space Weather Forecasting – Cause and Effect

Geomagnetic storms occur when processes in the near-earth space environment produce magnetic variations on the ground that are superposed on Earth's natural background magnetic field (Figure 1). These rapid storm-time variations result from a complicated collection of current systems in the Earth's ionosphere and magnetosphere. The current systems in turn are driven externally by disturbances in the solar wind[1], which ultimately originate from solar activity. Geomagnetic storm forecasts, therefore, must consider the originating solar phenomena, the evolution of these structures as they propagate and interact in the space between the Sun and the Earth, the coupling between the solar wind and the sun-facing side of Earth's magnetosphere, as well as the processes involved in the magnetosphere and ionosphere that ultimately dissipate this energy. We begin with a consideration of the kinds of solar phenomena which ultimately lead to geomagnetic storms.

[1] The solar wind is a continuous outflow of charged ions and electrons from the Sun which fills the entire solar system.

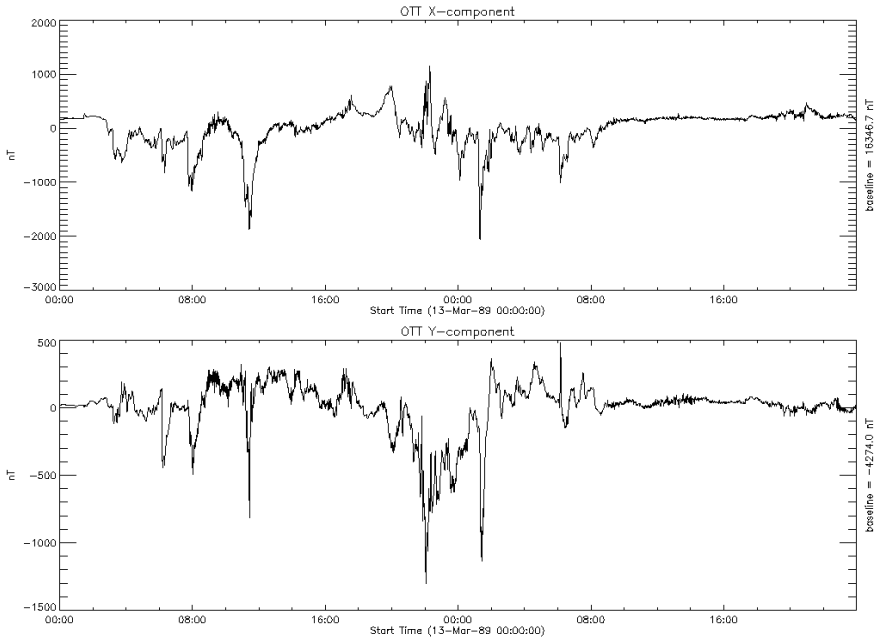

Figure 1: Horizontal components of the geomagnetic field at Ottawa during the March 13, 1989 storm. The maximum peak-to-peak component variation is about 1800 nT which is superposed on a background baseline horizontal magnitude of 16896 nT. Data courtesy of Natural Resources Canada.

Fiori et al. [2015] describe two key types of solar phenomena that cause geomagnetic activity which we briefly review. The first of these are coronal mass ejections (CMEs), which are observed as relatively bright (and therefore relatively dense) material being ejected from the Sun into interplanetary space. The discovery of CME's is relatively recent, usually credited to *Tousey* [1973]. Although the association of solar flares and geomagnetic storms had been long known, it took many years to sort out the respective roles of flares, coronal mass ejections and geomagnetic storms [see *Crooker et al.*, 1997 for a summary of results]. The key result for forecasting is the understanding that the CME is the directly observed feature that actually travels through space and can ultimately lead to a geomagnetic storm. Figure 2 shows a 'head on' view and a 'side view' of two major coronal mass ejections that occurred during a very high solar activity period in late October and early November 2003.

The second phenomena that cause geomagnetic disturbances are high speed solar wind streams originating from solar coronal holes. These high speed streams form and evolve on longer time scales than coronal mass ejections: a typical coronal mass ejection as seen in the coronagraph occurs over a few hours or less, whereas coronal hole high speed streams form and persist on timescales of one or more solar rotations (~27 days). Shown in Figure 3 is a solar image in soft X-ray wavelengths; the coronal hole is the dark feature that appears on the right side of the image. Associated with the coronal hole is a relatively fast outflow of plasma (Hydrogen ions, electrons, and other less abundant ions). As this fast outflow interacts with the surrounding slower moving solar wind, a compression occurs, leading to the formation of a 'co-rotating interaction region (CIR)' just ahead of the high speed stream.

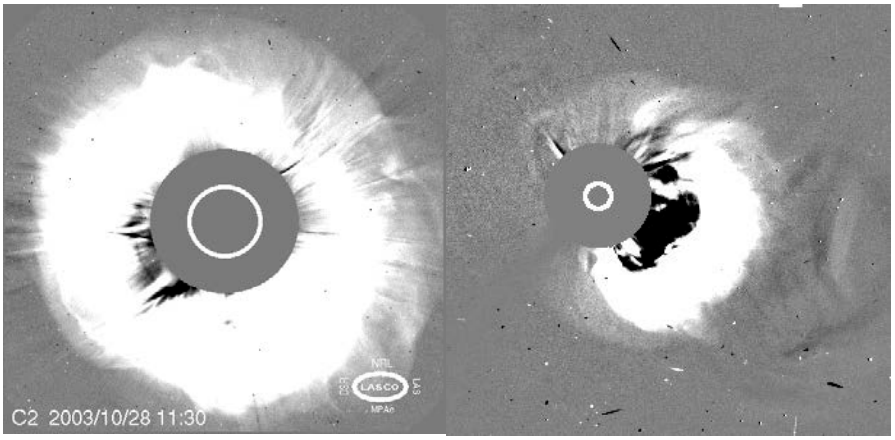

Figure 2: Coronal Mass Ejections observed using the NASA/ESA SOHO coronagraph. The CME on the left occurred on October 28, 2003 and the CME on the right on November 6, 2003. Data courtesy of the NASA/ESA SOHO mission.

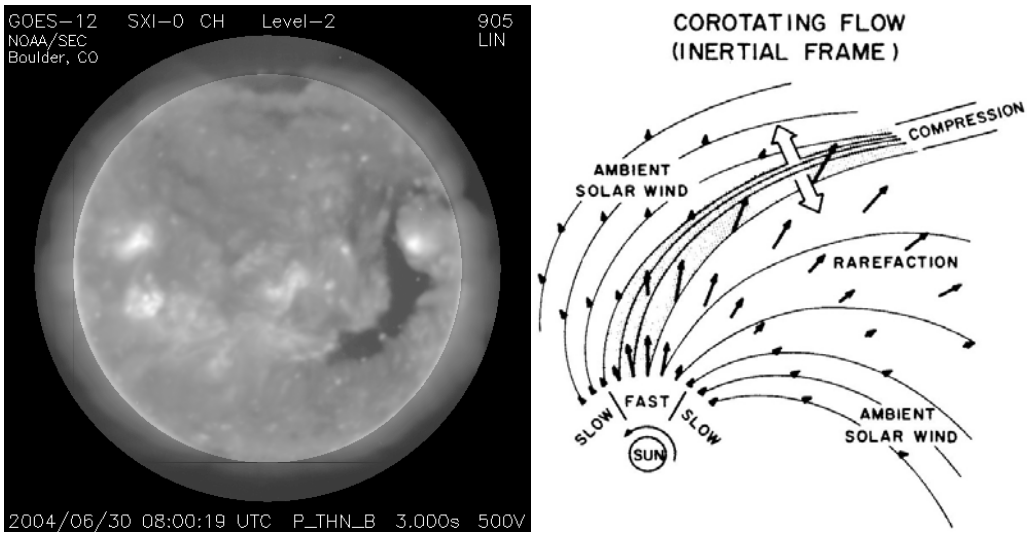

Figure 3: GOES-12 SXI image of a coronal hole. On the right, conceptual model for formation of a co-rotating interaction region [*Pizzo*, 1978]..

Often these high speed streams will persist for many solar rotations. In these instances, enhanced geomagnetic activity will be observed to reoccur at Earth with a period of about 27 days, as the co-rotating interaction region and high speed stream sweep by the Earth once every solar rotation. This effect, called 'recurrence', was already known before the actual discovery of coronal holes, based on studies of geomagnetic activity (The earliest full description of recurrent activity is attributed to Maunder in 1905 although the effect had been described even earlier, see Chapman & Bartels [1940], chapter XII). The solar origins of recurrence had to wait for the advent of space-based telescopes, such as Skylab in the 1970's to be understood [*Zirker*, 1977].

Concerning the geo-effectiveness of coronal holes and coronal mass ejections, we note that the most extreme storms are generally caused by coronal mass

ejections. An analysis by Richardson and Cane [2012], for example, shows that for Kp ≥ 8 storms over four solar cycles (48 years), 111 out of 112 originated from coronal mass ejections[2].

III. Geomagnetic Forecasts with Long Lead Times

There is some limited capability for forecasting geomagnetic activity with relatively long lead times. Long lead times refer to predictions which are made before the occurrence of a coronal mass ejection. The two types of longer lead-time forecasts differ, depending on whether the anticipated source is a coronal mass ejection or a coronal hole high speed stream.

Forecasts based on coronal hole streams are the more likely to be successful, due to the relatively slow evolution of these structures. Prior to direct observation of a coronal hole on the Earth-facing side of the Sun, forecasters will consider a recurrence forecast as a starting point for the longer term prediction. Once a coronal hole is observed on the solar disk, adjustments can be made based on comparison of the coronal hole with its appearance during the previous solar rotation. Since high speed streams have a 'garden sprinkler' spiral configuration (see Figure 3), the coronal hole source region has to rotate somewhere between 30 to 60 degrees past the central meridian before the high speed stream will be observed at Earth[3]. This means that the first appearance of the coronal hole can be used to forecast activity with about 8-10 days of lead time.

In addition to direct observations, forecasters use a physics-based model to guide these predictions. At the NOAA Space Weather Prediction Center (SWPC), forecasters routinely use a model developed by Wang, Sheeley, and Arge [*Arge and Pizzo*, 2000]. The solar magnetic field is the key input, and due to measurement limitations the lead time using the model is about 3-5 days. While useful, the model has limitations which occasionally require forecaster intervention. For example, the input data may have quality issues, or uncertainties about the solar magnetic fields at high latitudes may lead to errors in the model output.

Forecasts for flares from sunspot regions can provide an indication of elevated risk for coronal mass ejections. Forecasters routinely produce region-by-region flare probabilities with a lead time of one to three days. Although not all flares will be associated with a CME, nor will all CME's necessarily be associated with a flare [see *Hundhausen*, 1998], it is still reasonable to assume that the probability for CME occurrence is enhanced if the probabilities for major flare events are elevated. In this way, the flare forecast identifies intervals of elevated activity which are of concern to those affected by geomagnetic storms. A good example of this occurred during the October-November 2003 high activity period and was described by Balch et al. [2004].

IV. Geomagnetic Forecasts with Medium Lead Times

Once a coronal mass ejection is observed, a medium lead time forecast can be formulated. The observation of a CME using a coronagraph provides critical information about the speed, size, mass and direction of the ejected material near the Sun. The speed, direction and morphology provide an indication as to whether the CME is headed in the direction of Earth. For those events that are likely to encounter Earth, the direction and speed also provide information about the time of arrival. Speed and mass also provide some indication of the overall size of a subsequent geomagnetic storm, although there are still uncertainties that limit forecast accuracy from these observations.

CME transit times to Earth typically range from 36-72 hours [*Richardson and Cane*, 2010], but the most extreme events are faster. *Cliver and Svalgaard* [2004]

[2] The Kp index runs on a scale from 0 to 9. For information about the planetary geomagnetic index Kp see the review by Menvielle and Berthelier [1991].

[3] The average solar synodic rotation rate is about 13.2 degrees per day

tabulated the twelve fasted-transit events for years 1859-2003, and find times ranging from 14.6 to 21.8 hours. For the very fastest CMEs, the medium-lead time forecast may provide only 15 hours or so of lead time; more typically, though the lead time will be about 1.5 to 3 days.

One limitation inherent from using a single viewpoint, such as is done today with the SOHO coronagraph, is that the three dimensional CME is projected onto a two-dimensional field of view. This results in uncertainties regarding the true direction and speed of the CME since the coronagraph only shows the CME moving across the observer's field of view. In practice this is addressed by fitting a three dimensional geometric model of the CME front so that the projection of the model CME onto the plane of the sky is reasonably consistent with the imagery. To aid the model fitting procedure, forecasters add external information, such as observations in H-alpha and the lower corona (i.e. EUV and X-ray images) which may provide guidance regarding the initial source and trajectory of the CME. Through experience SWPC has also found a correlation between the plane of sky speed and the 'cone angle' parameter for the model CME. This further bit of information allows forecasters to set the initial value of the cone angle in their fitting procedure.

An effective way to reduce the projection uncertainty is to add observations from a coronagraph positioned off the Sun-Earth line and looking across the line of sight of the first viewpoint. This 'two view' capability was achieved for a few years (roughly 2008 to 2012) by the NASA STEREO mission.[4] Observations of this type provide better constraints on CME speed and direction. An example of the 'two view' fitting process is shown in Figure 5. Data from STEREO-A for this application are expected to resume over the next few years as the spacecraft moves once again through favorable heliolongitudes[5]. The advantages of this CME 'triangulation' capability have motivated the space weather community to work toward an ongoing L5 mission[6] as a key component of the future fleet of space weather forecasting assets.

[4] See stereo.gsfc.nasa.gov for more information about the STEREO mission. The STEREO mission actually provided a 'three view' capability from about 2008 To 2012. Unfortunately communication with one of the STEREO spacecraft (STEREO-B) was lost on October 1,2014.

[5] See stereo-ssc.nascom.nasa.gov/where.shtml for the current location of the STEREO spacecraft.

[6] L5 is located at one AU about 60 degrees (relative to the Sun-Earth line) behind the Earth.

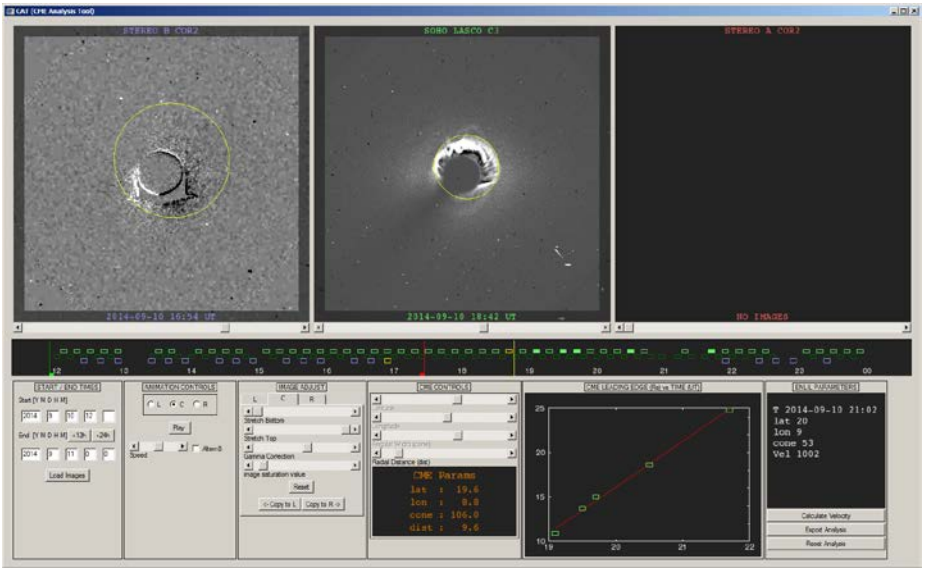

Figure 5. Fitting a cone to a CME using two coronagraphs.

Even without the two view capability, there is still useful information concerning potentially geo-effective CMEs. Typically these CME-based geomagnetic forecasts rely on 'rules of thumb' or various empirical approaches to gauge the arrival time and magnitude of the anticipated disturbance. Some of the key aspects of a CME event and associated phenomena that may be considered include plane-of-sky speed, CME size and brightness, morphology of the CME front, characteristics of any associated soft X-ray signature (e.g. peak or integral flux), and solar radio sweep information.

Many of these techniques still have value today, but difficulties arise because the CMEs evolve and interact with the pre-event solar wind and this affects the characteristics of the solar wind disturbance as it is passes by Earth (see descriptions by *Tsurutani et al.* [1988], *Gonzalez and Tsurutani* [1987], and *Gonzalez et al.* [2011]). Even in the relatively simple case where a fast CME travels through an otherwise nominal background solar wind, a shock will form, and a region of swept up solar wind (the sheath) will develop between the original CME material and the shock. Any given large geomagnetic disturbance may be driven by the sheath, the CME driver material, or both. In more complicated situations, a CME may interact with and modify a co-rotating interaction region, or a CME may catch up to and interact with another CME that erupted previously. There can also be cases where the CME is modified as it crosses into a pre-existing high speed stream coronal hole.

These kinds of interactions are not easily incorporated into observation-based empirical forecasts and this has motivated the development and implementation of physics-based models. Indeed the first operational physics-based model for CME propagation between the Sun and the Earth was implemented relatively recently [*Pizzo et al.*, 2011]. The WSA-ENLIL model uses WSA to initialize the background solar wind (including high speed streams from coronal holes) and allows forecasters to add a CME at the inner boundary. The CME subsequently propagates through the interplanetary medium, interacting with pre-existing structures in a way that is physically justified. An example of the model output is shown in Figure 5. The upper-left circle shows plasma density in the ecliptic plane. The figure shows the presence of a high-speed stream, a co-rotating interaction region, and three distinct CME's which occurred in sequence. In the Figure 6, we see the merging of these structures prior to their arrival at 1 AU.

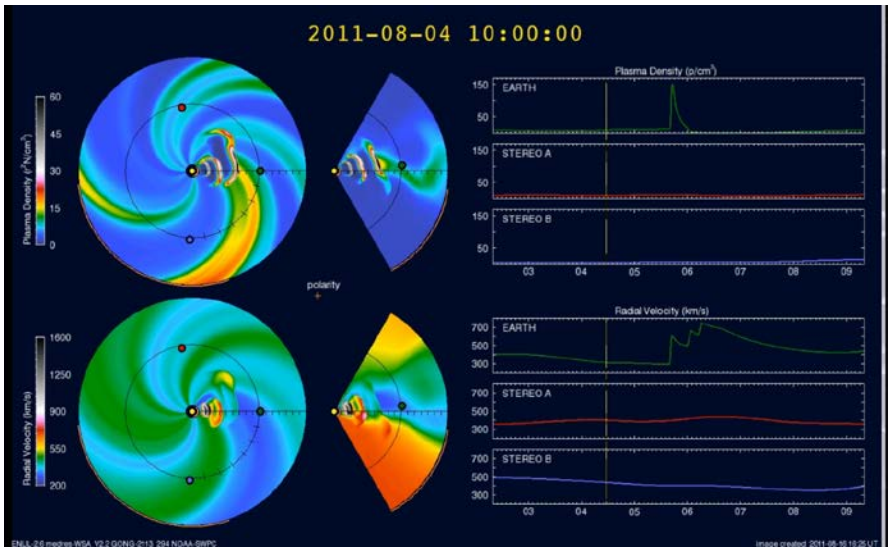

Figure 6. Output from WSA-Enlil-Cone model for series of three CME's observed in August 2011.

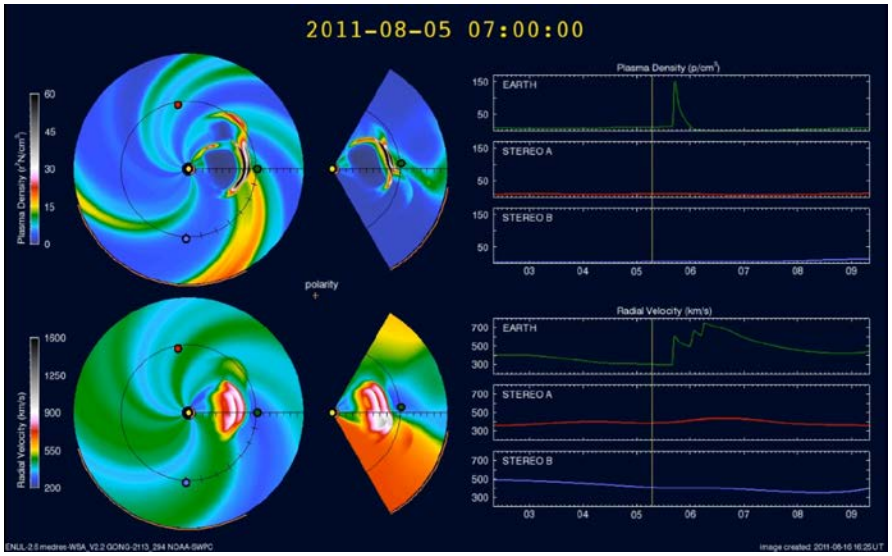

Figure 7. Model output for same case as in previous figure but later in time.

A final point regarding medium lead-time forecasting is the lack of information about the strength and orientation of the interplanetary magnetic field (IMF) prior to in-situ measurements near the Earth. This contributes to uncertainty for the medium lead-time forecasts because the strength and orientation of the IMF is the dominant characteristic that determines how strongly the solar wind energy couples into Earth's magnetosphere and ionosphere [*McPherron et al.*, 1988]. At this time there are not any well-developed techniques to directly measure this property of a CME and this problem is truly a 'grand challenge' for the space weather research community. It should be noted, however, that the CME-generated sheath field is modeled in the MHD codes, so there is a possibility of predicting the sheath field in the

relatively near term. It should also be noted that the presence of a fast CME generally ensures that the IMF is strong and there is certainly an elevated probability that strong southward IMF may be observed at Earth. There is no doubt that the risk for a strong geomagnetic storm is much higher in the presence of such events, even though we cannot say that it is a certainty.

V. FORECASTS WITH SHORT LEAD TIMES

A geomagnetic forecast with relatively short lead time is possible because of solar wind observations by the NASA ACE spacecraft at the L1 Lagrange point[7]. The ACE spacecraft routinely measures key solar wind parameters in-situ and the data are transmitted, processed and made available to forecasters in near real time. With the ACE spacecraft about 1.5 x 10^6 km upstream, nominal solar wind flows of 400 km/s take about an hour to reach Earth. It should be noted that this lead time is smaller when the solar wind is faster. Typical fast CMEs in the 1000 km/s to 1500 km/s range have approximate L1 to earth transit times of 25 minutes to 17 minutes. In a more extreme case, the 29 October 2003 shock took 13 minutes to travel from L1 to Earth, consistent with a speed of about 1900 km/s. The L1-to-Earth transit time, however, is only one part of the lead time this data provides for geomagnetic forecasts. Processes in the magnetosphere and ionosphere which transfer energy from the solar wind into the near space environment have their own timescales and add to the overall prediction lead time.

The initial impact of a CME occurs when the associated interplanetary shock hits the dayside of the magnetosphere; the dayside boundary is compressed and strong currents at the magnetopause are observed at ground magnetometers as a sudden jump in the horizontal magnetic field component. This 'sudden impulse' phenomena (sometimes called a 'sudden storm commencement') is described in more detail by Joselyn [1990]. The prediction of a sudden impulse using ACE data is straightforward and the Space Weather Prediction Center routinely issues warnings when these shocks are observed at L1.

Following the sudden impulse is a 'directly driven' response mechanism which generally involves a delay of about 20 minutes after the arrival of disturbance at the magnetopause [*Klimas et al.*, 1991; *McPherron et al.*, 1988]. The directly driven activity results from currents that flow in response to the dragging of magnetospheric field lines over the polar caps of the Earth by the solar wind and operates when the solar wind magnetic field has opposite orientation (i.e. southward pointing) to Earth's northward pointing magnetic field at the subsolar point.

A second pathway for energy transfer involves the building up of magnetic flux in the night-side magnetosphere [*Klimas et al.*, 1991; *McPherron et al.*, 1988]. Just like the directly driven activity, this mechanism requires southward orientation of the IMF. Eventually the building up of flux reaches a point of instability and an explosive release of energy occurs through magnetic reconnection. This causes greatly enhanced currents in the magnetosphere and the ionosphere, which are seen on the ground as strong geomagnetic variations. These 'substorm' events last about two hours and are predominantly observed in the auroral zone, a roughly oval-shaped region centered on the magnetic poles, although numerous other current systems in the magnetosphere are also enhanced (see Figure 7). The time scale for pre-event build up and subsequent releases of energy for these events varies from storm to storm, but tends to be in the 1-2 hour range [*Rostoker et al.*, 1980]. During longer, sustained geomagnetic storm periods, the auroral oval will expand to lower latitudes.

[7] The L1 point is about 1% of the Earth-Sun distance away from the Earth towards the Sun. The net gravitational pull of the Sun and the Earth at this point is such as to maintain the spacecraft's position between the Earth and the Sun. The ACE spacecraft, launched in 1997 will be replaced by the newer NOAA DSCOVR mission in 2016.

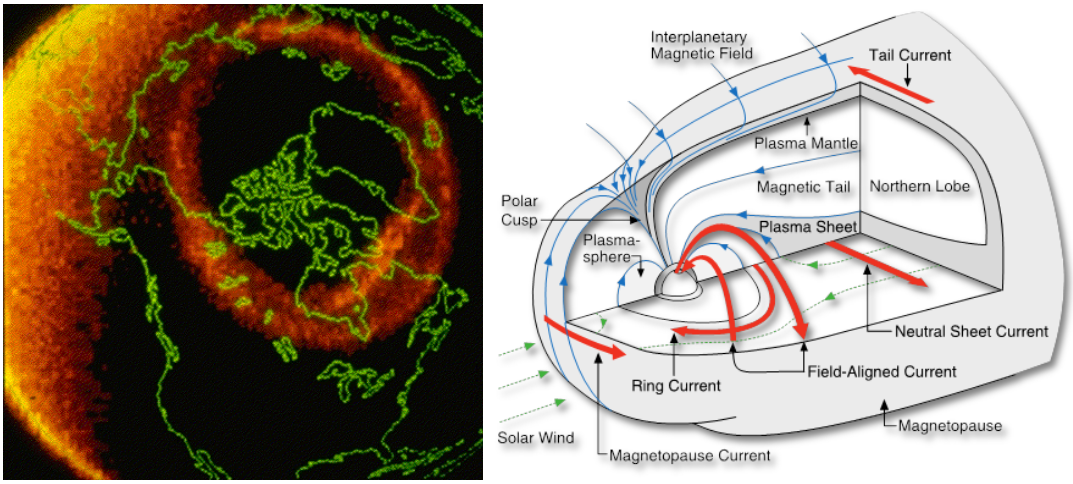

Figure 7: Left – image of the auroral oval from the Dynamics Explorer 1 Satellite (Source - Louis Frank). Right - Conceptual model of the Magnetosphere. (Source - C Russell, IEEE Trans. on Plasma Science, 2000).

Forecasts using solar wind data today rely on empirical algorithms [*Wing et al.*, 2005], rules of thumb [e.g. *Gosling et al.*, 1991; *Tsurutani and Gonzalez*, 1997][8], and forecaster experience. Based on these tools, forecasters at the Space Weather Prediction Center will issue warnings for imminent geomagnetic activity in terms of the global, planetary-averaged index, Kp.

Modeling and research on solar wind driving of geomagnetic activity has been quite extensive and operational forecast centers, such as SWPC, are working to transition some of these models to operations [see *Pulkkinen et al.*, 2013]. Such models may run predictively using solar wind parameters asured at L1. One type of model prediction will be for geomagnetic variations at particular locations on the ground, thereby providing regional forecasts of geomagnetic activity. These operational products are in development at SWPC for 2016. Figure 8 below shows a prototype, the regional geomagnetic forecast that was generated during the March 17, 2015 geomagnetic storm.

VI. Space Weather Forecast Products

NOAA's Space Weather Prediction Center operates 24 hours/day, seven days/week and produces routine, as well as event-driven space weather products. The routine forecasts include a 3-Day Forecast product, issued twice per day, which summarizes and predicts geomagnetic activity, radiation storms and radio blackouts. Also issued twice per day is a Forecast Discussion which provides detailed descriptions of observed activity and information about the forecast rationale.

The event-driven products consist of Watches, Warnings, and Alerts. Space weather watches are issued when conditions for a geomagnetic storm are favorable. The majority of these watch products are based on the medium lead-time forecast paradigm, i.e. in response to observations and model results for a coronal mass ejection. However, there can be occasions where coronal hole analysis justifies the prediction of a geomagnetic storm, so these watches will occasionally be based on a longer lead time forecast.

[8] An example rule of thumb from Gonzalez and Tsurutani states that intense storms (Dst < -100, Kp ≥ 6) may generally be expected when IMF Bz ≤ -10 nT is maintained for at least three hours.

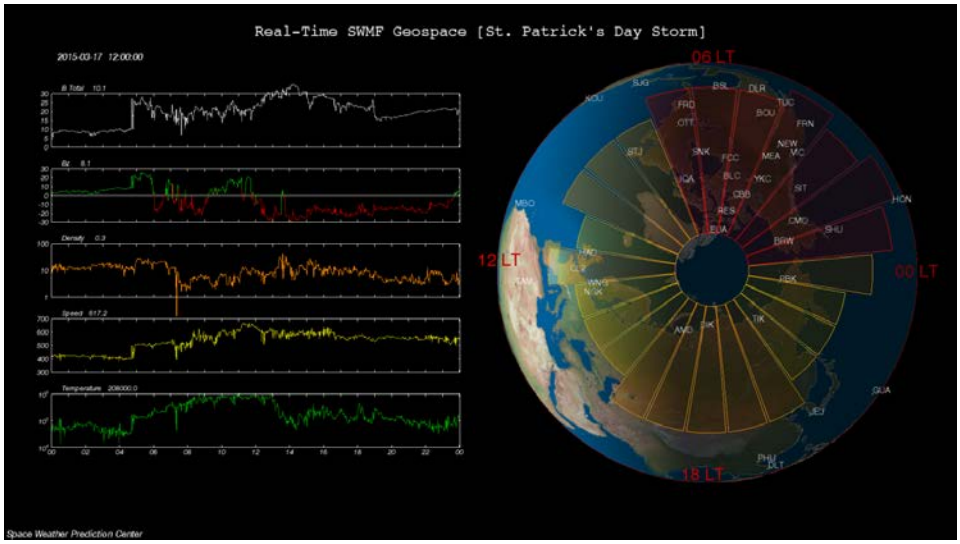

Figure 8: A regional geomagnetic forecast prototype product that was generated during the March 17, 2015 geomagnetic storm. Regional K indices are predicted with 29 minutes lead time for 60 degrees magnetic latitude in different longitudinal sectors. (Image courtesy of George Millward, NOAA/SWPC).

Geomagnetic Warnings are typically issued when a disturbance is detected at the L1 spacecraft. These warnings may be issued for an expected sudden impulse at Earth, or they may be issued when the Kp index is expected to reach storm levels (≥5). The SWPC also issues 'persistence warnings' which indicate how long an ongoing disturbance should be expected to continue.

Geomagnetic Alerts are issued when geomagnetic storm levels are actually observed in real time. This product has proven to be an important part of the space weather product suite as it provides the final confirmation that storm level activity has been attained.

VII. SUMMARY

Geomagnetic storms can have a serious impact on the electrical power grid. This impact is caused by geomagnetically induced currents, which in turn are driven by a time varying geomagnetic field. Some mitigation is possible through system planning and design, but there are also strategies that can be used operationally which are guided by space weather forecasts and nowcasts. In this paper we discussed aspects of geomagnetic forecasting, following the chain of cause and effect which ultimately traces back to solar activity. We identified two main phenomena that ultimately lead to geomagnetic storms; high speed streams from coronal holes and coronal mass ejections.

High speed streams from coronal holes may be forecast with relatively long lead-times because the structure evolves relatively slowly. These features tend to re-occur every solar rotation as the high speed solar wind stream sweeps by the Earth. However, this source for geomagnetic activity almost never leads to severe levels of geomagnetic activity

Coronal mass ejections are not well forecasted many days in advance, but it is possible to get a general indication that the probability of such events is elevated based on analysis of solar active regions. Once a CME occurs, a medium lead-time forecast is possible using a combination of observations and modeling. Typically this will give 36-72 hours of lead time for the CME to transit from the Sun to the Earth, but since the more extreme events are faster, this lead time can be significantly shorter in some cases. These forecasts indicate if conditions are favorable for a

geomagnetic storm and determine when SWPC will issue a geomagnetic watch.

As the CME propagates towards the Earth, it can interact with other pre-existing structures, and this interaction can have an effect on the overall geo-effectiveness of the event once the phenomena reach Earth. Recent transition of physics-based models to operations has improved the prediction and understanding of these kinds of interactions. Once the CME and any associated structures reach the L1 spacecraft, direct measurements of the solar wind parameters are made in real time. This allows forecasters to issue a higher confidence, short lead-time geomagnetic warning of imminent geomagnetic activity.

For the shorter lead-time forecast, space weather operation centers are actively transitioning physics-based geospace models of the magnetosphere-ionosphere system to allow the L1 data to be used to generate regional geomagnetic forecasts. Once the disturbance is actually observed to occur, real-time observations are used to issue alerts as a final link in the chain from the Sun to the Earth.

Bibliography

Arge, C. N., and V. Pizzo (2000), Improvement in the prediction of solar wind conditions using near-real time solar magnetic field updates, *J. Geophys. Res.*, *105*(A5), 10465-10479.

Balch, C. C., W. Murtagh, D. Zezula, L. Combs, G. Nelson, K. Tegnell, M. Crown, and B. McGehan (2004), Service Assessment - Intense Space Weather Storms October 19 - November 07, 2003, *Service Assessment Rep.*, National Weather Service, Silver Spring, Maryland.

Balma, P. M. (1989), Geomagnetic effects on a bank of single phase generator step-up transformers, paper presented at Geomagnetically Induced Current Conference, EPRI, San Francisco, 1992.

Barlow, W. H. (1849), On the spontaneous electrical currents observed in wires of the electric telegraph, *Phil. Trans. Roy. Soc. London*, *139*, 61-72.

Boteler, D. H., R. Pirjola, and H. Nevanlinna (1998), The effects of geomagnetic disturbances on electrical systems at the earth's surface, *Adv. Space Res.*, *22*, 17-27.

Chapman, S., and J. Bartels (1940), *Geomagnetism*, Oxford University Press, Oxford.

Cliver, E. W., and I. Svalgaard (2004), The 1859 Solar-Terrestrial Disturbance and the Current Limits of Extreme Space Weather Activity, *Solar Physics*, *224*, 407-422.

Crooker, N. U., J. A. Joselyn, and J. Feynman (1997), *Coronal Mass Ejections*, 299 pp., AGU, Washington D.C.

Czech, P., S. Chano, H. Huynh, and A. Dutil (1989), The Hydro-Quebec system blackout of 13 March 1989: system response to geomagnetic disturbance, paper presented at Geomagnetically Induced Currents Conference, EPRI, Millbrae, California, 1992.

Davidson, W. F. (1940), The magnetic storm of March 24, 1940 - effects in the power system, *Edison Institute Bulletin* 365-366 and 374.

Fiori, R. A. D., B. H. Boteler, L. Trichtchenko, L. Nikolic, H. L. Lam, D. Danskin, and L. McKee (2015), An Overview of Space Weather and Potential Impacts on Power Systems - A Canadian Perspective, *IR*^{3}, *1*(3), 18-25.

Gonzalez, W. D., and B. T. Tsurutani (1987), Criteria of interplanetary parameters causing intense magnetic storms (Dst of less than -100 nT), *Planet Space Sci*, *35*(September 1987), 1101-1109.

Gonzalez, W. D., E. Echer, B. T. Tsurutani, A. L. Clua de Gonzalez, and A. Dal Lago (2011), Interplanetary Origin of Intense, Superintense, and Extreme Geomagnetic Storms, *Space Sci. Rev.*, *158*(1), 69-89.

Gosling, J. T., D. J. McComas, J. L. Phillips, and S. J. Bame (1991), Geomagnetic Activity Associated with earth passage of interplanetary shock disturbances and coronal mass ejections, *J. Geophys. Res.*, *96*(A5), 7831-7839.

Hundhausen, A. J. (1998), Coronal Mass Ejections: A summary of SMM observations from 1980 and 1984-1989, in *The Many Faces of the Sun: A summary of the results from NASA's Solar Maximum Mission*, edited, pp. 143-200, Springer, New York.

Joselyn, J. A., and B. T. Tsurutani (1990), Geomagnetic Sudden Impulses and Sudden Storm Commencements - a note on terminology, *EOS - Transations of the American Geophysical Union*, *71*(47), 1808-1809.

Klimas, A. J., D. N. Baker, and D. A. Roberts (1991), Linear Prediction Filters for Linear and Non-Linear Modeled Geomagnetic Activity, *Geophys. Res. Lett.*, *18*(8), 1635-1638.

McPherron, R. L., D. N. Baker, L. F. Bargatze, C. R. Clauer, and R. E. Holzer (1988), IMF Control of Geomagnetic Activity, *Adv. Space Res.*, *8*(9), 71-86.

Menvielle, M., and A. Berthelier (1991), The K-Derived Planetary Indexes - Description and Availability, *Reviews of Geophysics*, *29*(3), 415-432.

National Research Council (2008), Severe Space Weather Events - Understanding Societal and Economic Impacts - A Workshop Report *Rep.*, 145 pp, The National Academies Press, Washington D.C.

National Science and Technology Council (2015), National Space Weather Strategy, edited by Office of Science and Technology Policy, p. 19, Office of Science and Technology Policy, Washington D.C.

North American Electrical Reliability Corporation (NERC) (1990), March 13, 1989 Geomagnetic Disturbance *Rep.*, 36-60 pp, North American Electric Reliability Corporation (NERC).

North American Electrical Reliability Corporation (NERC) (2013), Geomagnetic Disturbance Operating Procedure *Rep.*, NERC.

Pizzo, V. (1978), A Three-Dimensional Model of Corotating Streams in the Solar Wind 1. Theoretical Foundations, *J. Geophys. Res.*, *83*(A12), 5563-5573.

Pizzo, V., G. Millward, A. Parsons, D. A. Biesecker, S. Hill, and D. Odstrcil (2011), Wang-Sheeley-Arge-Enlil Cone Model Transitions to Operations, *Space Weather*, *9*(3), 2.

Prescott, G. R. (1866), *History, Theory and Practice of the Electric Telegraph*, 504 pp., Ticknor and Fields, Boston.

Pulkkinen, A., et al. (2013), Community-wide validation of geospace model ground magnetic field perturbation predictions to support model transition to operations, *Space Weather*, *11*, 369-385.

Richardson, I. G., and H. V. Cane (2010), Near-Earth Interplanetary Coronal Mass Ejections During Solar Cycle 23 (1996-2009): Catalog and Summary of Properties, *Solar Physics*, *264*, 189-237.

Richardson, I. G., and H. V. Cane (2012), Solar wind drivers of geomagnetic storms during more than four solar cycles, *J. Space Weather Space Clim*, *2*(A01).

Rostoker, G., S. I. Akasofu, J. Foster, R. A. Greenwald, Y. Kamide, K. Kawasaki, A. T. Y. Lui, R. L. McPherron, and C. T. Russell (1980), Magnetospheric substorms - definition and signatures, *J. Geophys. Res.*, *85*(A4), 1663-1668.

Tousey, R. (1973), The Solar Corona, in *Space Research XIII*, edited by M. J. Rycroft and S. K. Runcorn, pp. 713-730, Akademie-Verlag, Berlin.

Tsurutani, B. T., and W. D. Gonzalez (1997), The Interplanetary Causes of Magnetic Storms: A Review, in *Magnetic Storms*, edited, pp. 77-89, American Geophysical Union, Washington D. C.

Tsurutani, B. T., W. D. Gonzalez, F. Tang, S. I. Akasofu, and E. J. Smith (1988), Origin of Interplanetary Southward Magnetic Fields Responsible for Major Magnetic Storms Near Solar Maximum (1978-1979), *Journal of Geophysical Research, 93*(A8), 8519-8531.

Wing, S., J. R. Johnson, J. Jen, C. I. Meng, D. G. Sibeck, K. Bechtold, J. Freeman, K. Costello, M. Balikhin, and K. Takahashi (2005), Kp forecast models, *Journal of Geophysical Research*, *110*(A04203), 14.

Zirker, J. B. (1977), *Coronal Holes and High Speed Wind Streams, a Monograph from Skylab Solar Workshop I*, Colorado Associated University Press, Boulder.

Identify applicable sponsor/s here. If no sponsors, delete this text box (*sponsors*).

Modernization of the RCMP's Suspicious Incident Reporting (SIR) System

National Critical Infrastructure Intelligence Team (NCIT)
RCMP

I. A Brief Introduction to SIR

Canada is not immune to the threat from terrorism. This was demonstrated most recently by the two terrorist attacks which occurred in October 2014 -- in Saint Jean sur Richelieu, Quebec, and Ottawa, Ontario -- targeting members of the Canadian Forces and Parliament, and by law enforcement disrupting two terrorist plots in 2013 (one targeting rail infrastructure, and the other a provincial government building).

Most terrorist attacks are preceded by pre-attack indicators that can be identified, reported, analyzed and acted upon. Suspicious incidents, such as phone calls from potential customers asking unusual questions about security, business processes or individuals taking photographs of a facility in a manner unusual for tourists may not typically garner the attention of law enforcement; however, these suspicious incidents might be an indicator of terrorist pre-incident planning or other serious organized criminal activity. The reporting of these indicators, when put in a broader context, could help identify a potential threat against national security and prevent an attack from happening.

In this sense, the RCMP's National Critical Infrastructure Team (NCIT) developed the Suspicious Incident Reporting (SIR) system to gather information from industry, government and law enforcement about suspicious incidents that may indicate a potential criminal threat to Canada's critical infrastructure. When this information is received by the various stakeholders, it is reviewed, assessed and combined with other information and intelligence available to the RCMP to assess trends and criminal threats to critical infrastructure, and when appropriate, initiate or support criminal investigations. In April 2010, the Ontario Integrated National Security Enforcement Team (INSET), in conjunction with Toronto Police Service, made the first arrest that was directly associated with a SIR report.

SIR is a cornerstone of the RCMP's critical infrastructure protection initiatives, directly supporting the RCMP's mandate to detect, deter, disrupt and investigate threats to Canadian critical infrastructure. The system has shown itself to be valuable to both the RCMP and private-sector stakeholders, with tangible progress made towards sharing information and intelligence on indicators common to criminal activity relating to critical infrastructure. This information exchange enhances and solidifies partnerships and ensures the RCMP and all its partners have an understanding of the threats and risks surrounding Canada's critical infrastructure.

II. Modernizing SIR

The initial concept for SIR was developed in 2007. NCIT engaged and consulted with critical infrastructure stakeholders to further develop the SIR concept, and in 2008 rolled out a prototype SIR system. After two years of development, that initial system was replaced in 2010 with a web-based version. Unfortunately, the current system has exceeded its life expectancy based on original system development and architecture. The existing system has a number of limitations and shortcomings that necessitate the system to

be modernized in order to better serve both stakeholders and the RCMP by more effectively and efficiently collecting and disseminating information, and facilitating information analysis.

Although there will be a myriad of changes behind the scenes, such as seamless multi-layered security, users will immediately recognize a number of significant improvements, particularly:

- An interactive user interface, customized to the critical infrastructure environment;
- A simplified login process;
- The ability to share some of the information with other stakeholders;
- New notifications; and
- An enhanced, searchable library of information and intelligence products.

The new SIR system will therefore optimize the user experience by balancing analytical needs with ease of use through a redeveloped interface. Forms to submit suspicious incidents will be streamlined for ease of navigation, faster load times and more interactivity making the user experience more user-friendly. The new robust library will also allow for more comprehensive searches, making information easier and quicker to find. Finally, the new dynamic system will be independent from devices and Operating Systems, which will make it accessible through multiple platforms, such as desktops, laptops, hybrids, and will even have a mobile component that will allow it to be accessed from tablets and smartphones.

As with any new system, testing will take place throughout the project. The RCMP has joined in partnership with a large number of Stakeholders to ensure relevant information is captured while providing proper integrity. These Partners are continually engaged regarding the status of the project. Once testing from all Partners is complete, the RCMP will initiate a roll out strategy to all other Stakeholders across the country.

III. Funding the Modernized SIR

In early 2015, the RCMP applied to the Canadian Safety and Security Program (CSSP) for funding to modernize the SIR system. Led by Defence Research and Development Canada's Centre for Security Science (DRDC CSS), in partnership with Public Safety Canada, the CSSP supports federal, provincial or municipal government-led projects in collaboration with response and emergency management organizations, non-governmental agencies, industry, and academia to strengthen Canada's ability to anticipate, prevent, mitigate, prepare for, respond to, and recover from natural disasters, serious accidents, crime and terrorism through the convergence of science and technology (S&T) with policy, operations and intelligence.

On July 30, 2015, the Associate Minister of National Defence announced ten innovative new projects to support the law enforcement community across Canada. The projects were announced as part of a $12 million investment in 24 projects funded through the CSSP's third Call for Proposals, and included the modernization of the SIR system to better enable information sharing. Project partners include multiple units within the RCMP, critical infrastructure representatives, and an industry leader in analytics, business intelligence and data management.

The SIR modernization project will extend into 2017.

The following table includes key project milestones for 2015, 2016 and 2017:

Suspicious Incident Reporting (SIR) Modernization
2015
• DRDC CSSP Competition & Award of Funds • Finalization of Project Plan &Deliverables • Initial Project Development
2016
• Full Project Development • Testing **&** Partner Engagement • Stakeholder Engagement • New System Goes “Live”
2017
• Decommission Old System • Finalize & Close Project

NCIT encourages its partners to report information regarding suspicious or criminal activity to local law enforcement. To report an immediate threat to national security, please call 911 or your local police department. To report information regarding suspicious activity, criminal extremism, or other activities which could pose a threat to Canada’s national security, call:

National Security Information Network (NSIN) at 1-800-420-5805

Canadian Security Intelligence Service (CSIS) at (613) 993-9620

For more information on the RCMP’s SIR system, please contact:

SIR-SIS@rcmp.grc.gc.ca

Security and Operational Resilience Cycle: Facilitated Group Exercise

Connie Delisle, Ph.D.*
Research Associate, Infrastructure Resilience Research Group (IRRG)
Adjunct Professor, Simon Fraser University School of Criminology

Felix Kwamena, Ph.D.*
Adjunct Professor & Special Advisor to the Dean
Faculty of Engineering and Design, Carleton University

Abstract

Although our nation's critical infrastructure (CI)[1] is largely privately owned and operated, both the government and private sector have shared responsibilities to prevent and reduce risks of its disruptions or harm. Risks are increasingly complex and frequent, including natural, intentional and accidental hazards (Public Safety Canada, 2009). Furthermore, risks are heightened by the complex system of interdependencies, among critical infrastructure, which if left unmitigated can lead to cascading impacts exposing vulnerabilities that cross sectors and even borders. Management of infrastructure risks is an emerging capability from mature disciplines, such as finance and insurance, thus security practitioners in government and industry typically rely on experience and their collective knowledge from trial and error. Infrastructure resilience researchers at Carleton University use small group facilitated scenarios to explore and improve CI response processes, risk and planning frameworks. This method was applied at an IRRG Security Resilience and Professionalization Workshop, June 10, 2015, allowing participants to gain a deeper appreciation of the use of facilitated scenarios to explore sector-specific, as well as shared risks and challenges in developing coordinated CI incident response action plans. This paper provides a summary of each groups' approach in developing action plans, as well as interprets the quality of these plans. Scenario-based learning appears to effectively engage participants and improve situational awareness of the challenges and opportunities faced by government, industry and society in developing viable action plans.

I. INTRODUCTION

Policies, plans and processes currently in force establish requirements and guide investments in protecting assets and infrastructure comprising Canada's ten Critical National Infrastructure sectors. However, technological advances in engineering, information technology and data security has increasingly connected infrastructure sectors, and subsequently their risks. Although economic efficiencies are more probable, so too are disruption or destruction of CI as a result of novel ways to exploit interdependencies. For example, Industrial Control Systems (ICS) operate with coded signals over communication channels, providing off-site control of city water and sewer supply systems.

A broader appreciation of individual asset owners' risks and risks shared with other stakeholders is particularly important between physical and IT security functions. This requires building and sharing of knowledge so as to ensure expertise, plans and processes are in place to manage risks and ensure the resilience of stakeholders' assets and connected infrastructure. However, being risk-informed requires a constant reappraisal of capabilities, vulnerabilities (what may impact assets) and threats that are most likely to exploit vulnerable

[1] "Critical infrastructure refers to processes, systems, facilities, technologies, networks, assets and services essential to the health, safety, security or economic well-being of Canadians and the effective functioning of government." (Public Safety Canada, 2010A)

assets. Scenarios applied to multi-stakeholder infrastructure protection challenges are effective in developing common situational awareness and exploring 'critical' uncertainties to infrastructure from multiple points of view (Optimal Risk, 2015).

Along with a more conventional keynote and subject matter expert presentations, the "Enhancing Security Resilience and Professionalization Workshop" held June 10, 2015, also provided a venue for participants to engage in the small group scenario-based exercise. In keeping with IRRGs mandate to build knowledge and encourage information sharing in efforts to achieve secure and resilient CI, the results of the scenario-based exercise in this Workshop were consolidated for publication in the online journal (Infrastructure Resilience Risk Reporter). The intent is for the reader to reflect on this information, raise questions and engage their organizations in an ongoing dialogue about priorities for safety and security procedures, and investments in processes, technology and controls from multiple perspectives: physical / IT / cybersecurity, emergency management, and business continuity management.

II. METHOD

Participants were divided into three groups on the basis of their experience. Each group was directed by a team of two facilitators who guided the group in selecting and compiling a short scenario that considered three parameters:

- *Who was affected?*
- *How were they affected?*
- *What was the response*?

After developing their scenario, each group was required to design a "Comprehensive Operational Resilience Action Plan" that respected both resilience (capacity to recover quickly from difficulties) and community resilience.[2] In carrying out their roles and responsibilities (assuming roles and responsibilities of government, private sector or society [GPS]), each group was asked to be aware of the five Fs:

- *Failure of Initiatives,*
- *Failure of learning from the past,*
- *Failure of credibility,*
- *Failure of coordination, and*
- *Failure of imagination.*[3]

The facilitators engaged in collaborative discussion and encouraged critical dialogue in the course of developing their action plan, which was recorded by one volunteer within each group. At the end of the exercise, the volunteer recorders each presented their group's action plan to all three groups. Responses to questions arising from the presentations were fielded by facilitators, as well as by members of the group who had experience or made observations about particular points raised.

Post workshop, group recorders and facilitators were given several weeks to compile and provide to the Workshop host (IRRG) their notes from the scenario-based session. These submissions formed the basis for the development of this article.

III. RESULTS

Three scenarios were developed to set the stage for discussions during the course of the workshop and establish a context from which to develop an action plan. Each scenario is summarized as follows:

[2] The Community and Regional Resilience Institute Report (2013) defines Community Resilience as the "capability to anticipate risk, limit impact, and bounce back rapidly through survival, adaptability, evolution, and growth in the face of turbulent change."

[3] Five Fs concepts presented by Sundelius Bengt in his Keynote Address in March 2015.

Scenarios

- **Group A:** *Government*

The scenario focused on global events that triggered policy decisions by the federal government about tabling an emergency budget. These decisions ran counter to proposed plans to increase taxes, cut programs and services and fund the national security agenda. In response to the government's cost cutting initiatives, the scenario included the creation of a pan-Canadian coalition that would force the government to reverse all its cost cutting initiatives. Social activists, public and private sector unions and environmentalists were protesting for the past two weeks, blocking access to constituent offices, marine ports on both coasts, and Canada–US commercial trucking routes – all with the message to the Prime Minister to stop financial cuts. The scenario also included details that Public Safety Canada advised the Departmental Security Officer community that a major demonstration of over 20,000 people was to be held downtown Ottawa; vehicles were to be randomly parked (unattended) at intersections; fires set; and intelligence indicated that suspicious packages would be delivered to various federal buildings.

- **Group B:** *Private Sector*

This scenario concerned a power outage that affected the Greater Ottawa Region, including all municipalities bordering the Ottawa River, from Stewartville in the West, to Hawkesbury in the East, North of Highway 43, including surrounding municipalities (Kanata, Nepean in the west, Barrhaven, Kemptville in the south, and Orleans in the east). The hot summer morning threatened temperatures exceeding 30 degrees Celsius. Due to uninhabitable building conditions, the President of the Treasury Board (as the employer) ordered the evacuation of all effected Government of Canada buildings within the affected area. Because commercial facilities, light industry, and residential consumers were also affected, the scenario included details concerning how these sectors were being impacted.

- **Group C:** *Society*

The scenario was based on Canada's 150th birthday celebration centered on Parliament Hill, with a specific trigger being the threat of a suspicious package. The first consideration in assessing the threat was to determine who the likely potential threat agents were. After careful consideration by the group, it was determined that there was no one specific threat agent, and that it was possible that anyone from the general public or even first responders could potentially be threat agents. With that in mind, the group considered what security controls were necessary to put in place in an effort to prevent the possibility of a suspicious package being delivered on or around Parliament Hill during the celebration.

Action Plan Considerations and Priorities

Within the remaining time, each group identified key considerations and top priorities in developing an action plan to address their particular scenario. Key points reported by each group are provided in Table 1. Overall, the areas/themes raised by the three groups showed consistency in four areas:

- *Personnel protection* (employee, public or other sector personnel)
- *Communication, notification and situational awareness* (employee, management, responders)
- *Controls, Plans, Procedures* (access control, site restrictions, zones, alternate sites/technology)
- *Stakeholder engagement and collaboration* (awareness of capacity, resources, risks)

Group B was unique in that they chose to compare and contrast each affected stakeholder group (government, private sector, and citizens) in the context of their scenario. The group also highlighted factors, such as access to experts (not just plans) and conduct of a post-event debrief/incident analysis as good security practices. Group A was exclusive in its mention of conducting a threat risk assessment. Finally, Group C delved most fully into options to increase resiliency in recognition that the "show must go on" and impacts could be lessened rather than cancelling the entire event.

Group A Major Demonstration against Government Policy	Group B Power Outage - Multiple Sectors	Group C Suspicious Package Threat to Major Event
Safety and security processes to protect employees and safeguard assets	Root cause of the event (accident or deliberate)	Collaboration with key players in all sectors
Keep employees well informed in advance of and during any event	Common source of information about the event (communications)	Communication Plan (prior, during and after event)
Alert employees to have a personal survival kit at work in case there is a shelter in place order	Government and private sector employee health/safety (habitable building/evacuation of the facilities affected by the outage)	Identification of existing/ necessary surge capacity
Activate Emergency Operations Centers and link to the GOC	Communication and access to timely information (centralized in the Government Operations Centre (GOC) (for government)	Establishment of a zone/perimeter with higher security within the venue
Public Safety Canada would have the federal lead to direct Departmental Security Officers (DSO)	For private sector, continuity of their business, customer safety and profit loss considerations.	Hardening of the area (removal of means to hide a package)
Recognize that the Mayor and city would have the lead with local law enforcement	Clear roles and responsibilities of Treasury Board, Public Safety, other Lead Security Agencies, other governments (local, provincial), services (hospitals, transport), and media.	Screening of personnel entering higher security zone(s)
Departments could conduct a Threat Risk Assessment to ensure processes are robust – take corrective measures	Access to vital sources of information (Business Continuity Planners/ Emergency Operations Centers)	Control of access to the venue
Verify that Business Continuity Plans are up-to-date and ready should they be required	Conduct of a post-incident analysis, to provide corrective measures that could be incorporated into future plans.	Evacuation plan (should a package be discovered on the day)
Confirm that everyone knows their role and responsibility	Private sector communication with Corporate Head Offices/partner companies.	Establishing plans for relocation of part of the event to secondary sites/webcasting
There could be some interdependencies and stakeholder engagement that would be required	Citizens would primarily be concerned with the safety of family and friends, and the ability to communicate. Secondary would access to services and provisions.	Defining alternate routes for VIP's to and from the venue and alternate sites.
Mobility and transportation to and from the downtown core would be disrupted		Setting up off-site staging points and prepositioning resources
Briefing of senior management and ensuring that governance committees are engaged and informed in order to support decision-making		

Table 1: Summary of Considerations and Priorities for Action Plans

IV. DISCUSSION

Key to each of the small group scenario discussions was the notion of collaborative communication[4] – the importance of having relevant and timely information, *and* common situational awareness of the risks, opportunities (options) and interdependencies that confront critical infrastructure in Canada. Collaborative communication takes skill, but it also requires leadership to effectively understand the management of risks that are inherent within critical infrastructure and those risks resulting from ineffective security controls. Considerations deliberated by three groups also covered aspects of how to communicate, which would be sending/receiving information, and what would be their interdependencies. This is consistent with one of the pillars of Canada's National Critical Infrastructure Strategy that states, "Having strong situational awareness of the risks and interdependencies that confront critical infrastructure in Canada is the first step towards a comprehensive risk management process" (Section 4.2, Public Safety, 2010A).

Although participants in the small group discussions were not overtly focused on risk management or providing suggestions on how to conduct a formal risk assessment/treatment, it could be implied that all of the elements of managing risk were discussed during this exercise. Namely, **threats** (whether accidental, intended, or as a result of a natural hazard); **assets** (personnel, sites, physical buildings), "**Critical Infrastructure**", their **vulnerabilities** (to asset/infrastructure safety, security and protection), decisions about what controls to select (**evaluation**), and **options** selected as a means to mitigate/treat risks and manage consequences. While governments are working to promote a common approach to strengthening the resiliency of critical infrastructure, sharing tools, lessons learned and best practices, Public Safety reminds stakeholders that they are ultimately responsible for implementing a risk management approach appropriate to their situation (Section 4.2 Public Safety, 2010B).

While limited in scope and time, the IRRG workshop provided a venue for both the sharing of subject matter expert knowledge, as well as an opportunity to creatively engage stakeholders from both the government and private sector in collaborative dialogue about CI protection. Although a modest step, it is an important demonstrator of the value of collaboration and scenario-based discussion to facilitate collective decision making. In keeping with the Action Plan for Critical Infrastructure (2010), this effort may be viewed as baseline/foundational work on which to build on and conduct exercises to strengthen readiness and response efforts (Public Safety, 2010B, Annex E: Action Plan Summary Table).

As 2017 is quickly approaching, governments and partners may consider developing targeted risk assessment products (e.g., geographic-based risk registers) in response to current/emerging critical infrastructure issues and incorporate an interdependencies model (Public Safety, 2010B, Annex E: Action Plan Summary Table). Paramount will be creation of targeted risk management training offerings for managers/executives to aid in advancing individual and collective understanding. Without instruction and exposure to multi-sector practices and emerging techniques, "group think" in managing risks to CI could inhibit its maturity. Ensuring responsible risk/asset owners have the means to learn, understand management of CI risks is the first step to building a community that is conversant and ready to dialogue about risks and critically examine the degree to which the resilience of critical infrastructure in Canada is being advanced. This would also be an important element of any strategic approach.

[4] Lampron, Raynald J., "Collaborative Communications", *Infrastructure Resilience Risk Report*, Vol 1. Issue 2, Sundelius Bengt, Ph.D, Meeting the Extreme Space Weather Challenge to Societal Security! A Swedish Key Note Approach Address, *Presentation at 2015 International Space Weather Workshop and Training: Extreme events and their effects on Power Systems*, Ottawa, Ontario, March 4-15, 2015.

*Trevor Hanson, P.Eng. is an Assistant Professor of Civil Engineering at the University of New Brunswick and member of the UNB Transportation Research Group. His research has included developing a better understanding of policy issues by exploring them through an engineering lens, including, most recently, understanding the impacts of disruptions to critical transportation infrastructure. He has also undertaken research in rural intelligent transportation systems, rural older driver travel behaviour and safety, and active transportation.

Acknowledgement

*The authors acknowledge the valuable contribution of the facilitators (Sharon Savoie, Tim O'Neil, Susan Gallagher, Jacqueline Dunston and Raynald Lampron) for the success of this Workshop.

References

Public Safety Canada (2010). National Strategy for Critical Infrastructure.

Public Safety Canada (2010). *Action Plan for Critical Infrastructure*

Optimal Risk. Accessed October 2015). Working with Converged Risk Scenarios. http://www.optimalrisk.com

Kwamena, Felix. (2015) Enhancing Security and Resilience and Professionalization Workshop. Security and Operational Resilience Cycle: Facilitated Group Exercises (presentation).

Lampron, Raynald J., "Collaborative Communications", *Infrastructure Resilience Risk Report*, Vol 1. Issue 2.

Sundelius, Bengt. (2015) Meeting the Extreme Space Weather Challenge to Societal Security! A Key Note Approach Address – Extreme events and their effects on Power Systems (presentation)

Identify applicable sponsor/s here. If no sponsors, delete this text box (*sponsors*).

Recommended Critical Infrastructure Security and Resilience Readings

Felix Kwamena, Ph.D.*

"The Case for Simplicity in Energy Infrastructure For Economic and National Security", by Michael Assante, Tim Roxey, and Andy Bochman, Centre For Strategic & International Studies, October 2015.

"The Psychology of Cyber Crime: Concepts and Principles", *Gráinne Kirwan and Andrew Power © 2012 by IGI Global 372 pp.* International Journal of Cyber Warfare and Terrorism, 5(3), 55-57, July-September 2015

"Endgame? Sports Events as Symbolic Targets in Lone Wolf Terrorism", Ramón Spaaij & Mark S. Hamm Studies in Conflict & Terrorism, 38:12, 1022-1037

http://dx.doi.org/10.1080/1057610X.2015.1076695

"From Munich to Boston, and from Theater to Social Media: The Evolutionary Landscape of World Sporting Terror", Yair Galily, Moran Yarchi & Ilan Tamir

http://dx.doi.org/10.1080/1057610X.2015.1076640

"Application of the Critical-Path Method to Evaluate Insider Risks", Eric Shaw and Laura Sellers, *Studies in Intelligence Vol 59, No. 2 (Extracts, June 2015)PP 41-48*

****"Best Practices for Operating Government-Industry Partnerships in Cyber Security"***, by Larry Clinton *Internet Security Alliance*, lclinton@isalliance.org

(Volume 8, Number 4 *Volume 8, No. 4: Winter 2015* - Article 4 of the **Journal of Strategic Security**)

****"Deterring and Dissuading Cyberterrorism"***, John J. Klein, *ANSER*, johnjordanklein@aol.com

(Volume 8, Number 4 *Volume 8, No. 4: Winter 2015* Article 4 **Journal of Strategic Security**)

*Follow these articles and additional works at: http://scholarcommons.usf.edu/jss

"Impact of low prices on shale gas productions strategies", by Konnikova, Svetlana and Gülen Güca,

The Energy Journal, Vol. 36, Special Issue 1, 2015, pg. 43-62.

"Cyber Security at Civil Nuclear Facilities, Understanding the Risks", by Baylon, Caroline, Brunt Rogers and Livingstone, David, Chatham House, The Royal Institute of International Affairs, September 2015.

"The Economic and Political Realities of Regulations: Lessons for the Future", Jamson, Mark A., Energy Regulation Quarterly, Vol. 3, Issue 3, 2015, pg. 17-20.

"The Social Licence to Regulate: Energy and the Decline of Public Confidence in Public Authorities", Cleland, Mike, Energy Regulation Quarterly, Vol. 3, Issue 3, 2015, pg. 21-28.

"The Impact of Energy Prices on Green Innovations", by Ley, Marius, Stucki, Tobias, and Woerter, Martin, The Energy Journal, Vol. 37, No. 1, 2016, pg. 41-75.

"Energy Sector Innovation and Growth: An Optimal Energy", by Hartley, Peter, B. Medlock III, Kenneth, Temzelides, Ted, and Zhang, Xiuy, The Energy Journal, Vol. 37, No. 1, 2016, pg. 233-258.

.

"Petro-Nationalism: The Future Search for Oil Security", by Griffin, James M. The Energy Journal, Vol. 36, Special Issue 1, 2015, pg. 25-41

**Dr. Kwamena is an adjunct Professor/Special Advisor to the Dean of Faculty of Engineering and Design, Infrastructure Resilience Research Group (IR^2G), as well as Director, Energy Infrastructure Security Division, Energy Sector, Natural Resources Canada*