VOL 1, ISSUE 8 **June 2019**

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. Dr. Fiori can be reached at robyn.fiori@canada.ca.

This Issue

The eighth issue of IR^3 explores a variety of topics relating to critical infrastructure protection, including the use of UAVs for security, response and decision making both prior to and during a major incident, and the use of ionospheric modelling for improved detection of explosive events.

This issue opens with an article by **Doug Powell** on the adoption of UAV technology for security applications. Although UAVs have the potential to be useful for enhancing security efforts, implementation of the technology requires serious forethought to ensure effective and appropriate use of the technology. This paper identifies issues and concerns for consideration prior to adopting UAV technology.

Bill Isaacs provides an introspective look at balancing "*who you know*" versus "*what you know*" from an emergency management perspective. The response to a major incident requires both a strong network of contacts and the knowledge and ability to make the best use of that network.

Ross Johnson applies the Design Basis Threat (DBT) approach to critical infrastructure protection ensuring that as much experience and information as is needed is to handle threat assessment. In this Article Johnson discusses the Vulnerability of Integrated Security Analysis (VISA) process by stepping through a detailed example related to residential security. VISA is shown to be a valuable tool for both the design and enhancement of physical protection systems when used with DBT.

Amaury Caruzzo and John Gyakum discuss the natural hazard-related decision-making processes for the protection of critical infrastructure. They introduce decision analysis in the context of examining space weather hazards that have the potential to have both direct and cascading indirect impacts to critical infrastructure. Decision science is used to create an interdisciplinary research design to address stakeholder concerns.

Ionospheric monitoring is a vital component to the development of space weather operational services with impacts, for example, to high frequency radio communication and GNSS services. **Cheryl Huang et al**. introduce the importance of ionospheric modelling for the detection of explosive events. They suggest that ionospheric sensing could play an important role in the confirmation of explosive events required, for example, by the Comprehensive Nuclear Test Ban Treaty.

Next Issue:

We invite authors to contribute articles for Issue 9 relating to their experience in the field of infrastructure resilience. Draft articles of 2500 - 4000 words are requested by August 30, 2019. You may not have much time or experience in writing 'academic' articles, but IR's Editorial Board can provide guidance and help. Your experience is valuable and IR^3 provides an ideal environment for sharing it.

Applying Diligence to the Adoption of UAV Operations

*Doug Powell, CPP, PSP**
BC Hydro
Email: doug.powell@bchydro.com

I. Introduction

The security industry, once labour intensive, has long sought to reduce business costs by replacing workers with technology. One might conclude that security has often been a grudge expenditure and that security guard costs have rarely been considered a priority in overall corporate spending. When applying security operations to complex environments, security staffing costs are often the least palatable making technology applications more favorable, overall. Security departments have therefore been early adopters and innovators in the application of many technologies. Security technology (which is just technology applied to security functions) has become a booming business over the past 20 to 30 years as a result.

Security technology has also represented one of the largest investment disappointments over the same period because technology has not always been applied correctly for a variety of reasons. This has most often been due to a limited understanding or lack of research about product limitations and the correct applications of technology. Technology has too often been promised to solve problems where benefits were not subsequently realized. For example, many millions of dollars have been spent on motion sensor technology over the years. These sensors often end up being decommissioned or have caused operational nuisance value because the technology was incorrectly applied. This has been an ongoing, wide-spread problem. This is also true of video technology and many other forms of technology adapted for security uses.

Vendors and manufacturers of various technologies have not always understood the limitations of their products in various environments and have often sold their products without required field testing or research & development work. Field testing is necessary to ensuring the proposed solution meets the intended need. Unfortunately, use cases are often only developed after years of trouble-shooting in an operating environment. This is a painful way to adopt technology. Security technologies have been applied in countless applications without the appropriate skill sets in place to provide technical assurance and good oversight. Without technical competencies applied, with testing in place and use cases researched, adopting new technologies can become a disappointment and lead to additional expenditures to compensate for the problems caused by the failed application. This has negative consequences within the organization as poor buying decisions do not lend themselves well to future funding requests or program support.

Industry has been quick to consider UAV technology for security applications, for a variety of well-intentioned uses. When considering UAV operations we are typically only speaking of segments of the security industry, or industries where UAV operations might reasonably enhance security efforts. An important concern regarding the diversity of the security industry is not in the possible applications for UAV technology, but rather the manner in which new technology is adopted. Serious forethought and diligence are needed prior to adopting UAV technology, but may not always be well applied. Deploying UAV technology comes with important questions and requirements that need to be addressed as a first priority. The technical competencies needed to apply technologies to security solutions are too often missing and may not even be thought of as necessary.

Adopting UAV technology requires that lessons of the past be considered and not repeated. Technology and IT project management practices have also become leading edge and need to be applied to the adoption of UAV technology. This paper considers some of the fundamental issues and questions that should be inherent in the decision process leading up to UAV adoption.

II. Practical Considerations

Needs and Competencies

Any organization considering the use of UAV technology must consider what problems this technology is intended to resolve. To avoid leaping into new territory and all the work a technological shift requires, addressing need and understanding the problem (or gap) to be solved is a necessary first step. By committing to this level of operational awareness, the organization can consider the new technology in a more comprehensive manner while also addressing other options to achieve the desired resolution. Too often, we are guilty of adopting "new" and shiny things without sound reason. Onboarding any new technology without reasoned forethought goes against the grain of a fiscally responsible organization and becomes more like impulse buying.

Perhaps one of the most practical considerations of all is whether the organization has the requisite skill sets to operate UAVs responsibly, with least impact on the organization from a cost and safety perspective. Recognizing that needed skill sets are not yet part of the organization’s skills inventory, a meaningful study must be committed to in order to understand all of the requirements to obtain and sustain competencies for UAV operations. This can include operator competencies, as well as operational needs like launch sites, public safety programs, worker safety programs and other factors that must be developed and delivered to ensure safe UAV operation. Understanding how UAV operations fit into the governance structure of the organization is important. Determining how decisions about UAV operations are made, whether a communications strategy is needed, what the reporting requirements are, how program reviews will be carried out and what policies, procedures and standards will be applied should be required ground work prior to UAV operations receiving the green light. Any mobile technology, especially one that can fall from the sky, requires a comprehensive "safety-by-design" check-list leading to development and sign-off.

Assuming the required skill sets to accredit UAV operators is not present in the organization careful study is needed to understand competency requirements, legal requirements and training requirements. If they are not well defined, it will be challenging to understand whether UAV operators (and operations) are at the required technical level prior to launching. No organization would consider it a responsible action to allow unqualified persons to operate vehicles, forklifts or other dangerous equipment. The same kind of diligence is required of UAV operators, tested across a comprehensive set of environmental conditions. Even understanding UAV technology at the engineering level, so that technical challenges can be overcome or compensated for is a critical step in the process. As an example, we become better vehicle operators (drivers) the more we know about the vehicle we are driving and driving conditions.

Jurisdiction and Social Responsibility

When considering UAV technology, leading factors in the decision-making process should include social and environmental responsibility. UAVs interact with the environment and with people in a variety of ways. A comprehensive impacts analysis should lead the discussion about UAV adoption. Not all environments are suitable for UAV operations. Government regulation may help to determine this for an organization. For example, regulations exist to govern UAV use near airports (and heliports), and UAV use in high-density high-rise areas, over schools, playgrounds, recreational facilities and public gatherings. In other areas, social and environmental responsibility, as well as public safety and social acceptance may be less clear or require more definition. Understanding restrictions and applying a good neighbour filter should lead an organization to carefully consider whether using UAVs in certain situations is a wise choice. The voices of local citizens, advocacy groups, local government and police agencies are important to listen to in this regard.

UAV operations may have competing jurisdictions that need to be understood so that safe and lawful operation of the organization's UAV addresses these concerns. Local police organizations may use UAVs or may have other technologies or operations in place that other UAV operations might interfere with. During special events and large public gatherings, special operations undertaken by local municipalities and policing or emergency management organizations may include UAV or aircraft operations. It will be very important to understand the local operating environment in this context, as well as the process for engaging on these topics, to full understanding the potential for conflicts and restrictions.

It is also important to communicate with officials at all levels of government in your operating area so they understand your intentions and so they have this background information to address a variety of other concerns like public complaints. Overall, public safety planning and civic responsibility are addressed through effective external consultation. Understanding the issues that may arise beforehand allows the organization to consider communication and coordination strategies. Good public engagement strategies will diminish the potential for negative fallout to UAV operations. Within security circles, it is also true that cooperation between private business and law enforcement, such as the sharing of information acquired through UAV operations (e.g., video footage) can be beneficial in developing two-way cooperation. In any event, deploying UAVs comes with a set of responsibilities which need to be contemplated and addressed and which may fall outside the scope of normal daily operations.

On the topic of public concerns, any company using a UAV probably needs a process for receiving and responding to public questions and concerns about the UAV operations. UAV safety incidents and accidents also need to be communicated responsibly and lost or downed UAVs should be communicated in such a way that recovery operations are well coordinated with the public in mind. Even rural operations that have the potential to impact livestock, or which may interact with wildlife in a manner that draws public or government agency scrutiny need to be factored into UAV use. Communications policies and procedures may need to be developed or reinforced in addition to establishing a public inquiries portal.

Adapting Technology

UAV technology is already quite diverse in terms of type of aircraft, available onboard technology, ground operator tools, communications options, and more. Size of aircraft and operating capabilities are also evolving. Like any technology, new advancements are constantly being realized requiring a comprehensive understanding about the technology, its advantages and disadvantages, operator requirements, applications and similar information. Size of UAV likely determines what operating class a UAV falls within. Identifying a UAV for commercial use versus recreational (hobby) use will have a bearing on registration, licensing and other regulatory restrictions associated with operating one.

Knowing where to find the information necessary to make an informed buying decision is as important as for other technologies. Understanding software licensing and version upgrades (as may be applicable), as well as managing possible impacts on the organization's computing infrastructure need to be considered.

New vulnerabilities and technology challenges factor into the decision-making process. UAV operations should be applied to networks in accordance with best IT standards and not become a weak link in the organization's cyber program.

Operating Requirements

There are a variety of operating considerations that also need to be factored in to UAV use. In addition to basic operating requirements like flying during meteorological events, other factors should be considered. If nighttime operations are anticipated, additional technological features necessary for night time operation may be needed and additional operator competencies may also be required. As mentioned earlier in this article, there may be sensitivities associated with the operating region that could also require consultation with external bodies. These include regional variations like operating the UAV in a forested area, over water, operating seasonally (such as during bird nesting season), operating near (but not within) restricted aerodromes, operating over private property, including on the boundaries of other industrial operations, operating in and around environmentally sensitive areas, over farming operations or near roads and highways. Operating a UAV in a closed work environment and in close proximity to other workers, leaves open the possibility of worker distraction. Using a UAV inside an active work area requires a process for clear safety communication in and around UAV operating zones. There are many environmental, regional and situational circumstances where UAV operations may be unwise, illegal or require additional precautions. These need to be identified and factored into UAV use as applicable. A fulsome study and engagement are needed before UAV operations are adopted.

Considering Other Options

When considering any of these practical issues related to UAV operations, one must also consider the practicality of adopting UAV operations versus using other technology and other operating models. In the analysis, actual benefits derived from UAV operations must be factored against defined risks.

Sometimes, organizations consider security threats without fully measuring the impact of these threats. This can lead to operating decisions where costs and new problems caused by the new technology are not well measured against the benefits. It may be that the desired outcome from UAV operations is not substantially beneficial in terms of the time, costs and other considerations associated with UAV operations. In fact, it may be that the particular threat being addressed has such low frequency that use of UAVs does not contribute substantially to the mitigation effort, so that cost actually outweighs the benefit. Other operating models may be more appropriate and easier to apply.

Camera technology that is applied well, as part of a more integrated security program, may be a better solution and less costly overall. Working with neighbouring organizations, police agencies and the intelligence community might offer advantages for maintaining situational awareness that brings in better information and improved security operations through these cooperative ventures. Even human capital can be applied cost-effectively at times when used in manner consistent with the type of threat to be mitigated. It will be valuable for the organization to address options when looking at the value proposition of the solution being proposed.

III. Cost Considerations

Return on Investment

In addition to the more practical considerations of UAV use, cost needs to be considered as with any security application. The security industry regularly touts return on investment (ROI) and cost-benefit analysis as necessary parts of security solutions assessment. Security funding traditionally comes via one of two channels. Within the normal planning processes, security is asked to carefully weigh costs, benefits and alternatives when seeking funding for their initiatives. This is expected, and justification is not always easy given some risks are concerned with massive damage potential and high casualty estimates, but where frequency is expected to be rare (terrorism events). It is easy for senior managers to defer spending in these situations. The other funding channel relates to what many organizations experience in response to an unexpected event or to an imminent threat, which is more impulse in nature. Organization will often fund operations on a contingency basis because of perceived consequences, but where no formal risk evaluation has taken place. In such cases, security departments and consultants often find themselves in a windfall situation.

It might be argued that if UAV use were to be applied as an interim measure, it is better applied as a short-term application using an outside, experience contractor who will also bear the majority of the risk associated with UAV operations. However, even when contracting third party suppliers, the organization is not released from its requirement for good judgement resulting from effective research into UAV use. When applying analysis associated with longer term (normal operating environments), however, financial analysis is an important component of the decision-making process and often leads to the most difficult questions being asked.

Given that operator skill and competency is a key factor in UAV deployment, the organization will also need to consider short-term, intermittent and occasional UAV deployment as viable options over in-house operations. It may be more cost-effective to seek out and contract a third-party service for those times when the service is needed. If flying a UAV only makes sense during special circumstances, as for protest management, crowd surveillance, world-class events, etc., at least part of the discussion should be about the best available value, weighing third-party services against in-house operations.

Insurance costs associated with UAV operations also become a factor in these discussions. If the organization intends to be self-insured, claims history and documented claims related to UAV use are required in order to draw reasonable conclusions and cost projections. Even when transferring risk through a third-party, claims experience and history (and litigation experience) associated with UAV use is important to understand.

Operational Costs

Associated technology costs, training costs, facility upgrade costs (safety, etc.), maintenance costs, IT costs, replacement and end-of-life costs, insurance and claim costs and other such costs all need to be factored into the cost equation. Understanding how the technology will be used and pairing use case with UAV technology options is an important first step in the cost analysis process. Given most organizations do not employ UAV technology specialists within their organization, the learning-curve, information gathering and consultation in this phase may be extensive and also carries a cost.

More advanced UAV applications may require software packages to operate the craft and to derive full benefit from its onboard systems. In a controlled IT environment, these applications need to be considered in context of the existing networks, network security, ongoing maintenance, including software licensing, and other technology costs like firmware upgrades and future technology enhancements. Encrypting UAV communications may be challenging depending on the nature of the communication protocols used by the manufacturer and the maturity of the technology. Adapting one technology to another assumes more risk, more time expenditure and more cost to the organization. Executed poorly, "Band-Aid solutions" represent more risk to the organization.

Organizational costs and contributions to the UAV operations also need to be considered in terms of time commitments and direct labour costs. These can include Human Resources department contributions, governance development, facilities costs associated with upgrades to accommodate safety enhancements and other upgrades. Safety program changes (OSH standards), consultation requirements, steering committee involvement, executive engagement, communications costs and other collaboration and business-driven costs need to be factored in. Adding a UAV to the organization may be contemplated as only an asset acquisition, but UAV operations require that considerable diligence be completed and that a full impacts and cost analysis be completed beforehand. Unlike the procurement of photocopy paper, for example, UAV procurement is more than a commodity purchase.

Ongoing Maintenance Repair and Replacement Costs

If a UAV itself is going to cost the company more than $5000 for the aircraft, it is probable that the organization will not tolerate many UAV crashes caused by operator error, which lead to full replacement cost. If even minor accidents resulting in repair costs are likely, then a decision as to the organization's tolerance for down time, when the UAV is not in service and decisions about back-up units and related concerns need to also be made. Certainly, replacing a UAV due to accidental damage will not be an ongoing allowance for many reasons. Early adopters of UAV technology in a variety of industries have indicated that use of UAVs were curtailed or put on hold for just this reason. UAV limitations and operator error have led to significant damage-related costs.

IV. Risks Associated with UAV Operations

Risks associated with UAV operations have already been touched on in other sections of this paper. Contribution to enterprise risk should be expected from UAV use, depending on the complexity of the organization deploying the technology and depending on the uses contemplated for the UAV. These risks include:

- safety risk – both in terms of worker and public safety;
- reputational risk – the UAV is ever used for unauthorized purposes, involved in a serious regulatory violation or is even perceived as breaching privacy regulations; and,
- financial risk – for a wide variety of reasons, including those from negligent operations or unrealized benefits.

On balance, a determination also needs to be made as to whether the UAV operation will represent more risk to the organization than it reduces.

If video surveillance is required or contemplated, risk discussions need to include the security of recorded video, as well as protection against hacking of the video feed and of the UAV control module. A compromised UAV could result in more than just embarrassment to the organization. Impacts associated with law enforcement fines, public opposition, union grievances (which can include workers believing they are being spied on) and other such concerns can result in financial penalties, unwanted press and damaged relationships. Effective change management practices are needed to address operational risk. Carrying out effective change management prior to UAV operations should be imperative.

Operator Competency

When considering UAV operator competency, a variety of topics should be included in the discussion. To begin with, the organization will want to be sure it fully understands all requirements associated with use of UAVs (air restrictions, safe operations, registration requirements and operator training requirements) where requirements are either in force or expected to be put in force. Knowing who to speak to, what resources are available for consulting, what government agencies hold authority and what experience exists that an organization can tap into are important considerations. Opening and maintaining regulatory communication lines might be a new requirement.

Identifying reliable training programs in such a fledgling industry requires some research. Those regulating the industry will have good information to offer, but even training program length and ongoing operator development, as well as identifying the space needed to appropriately training are important to plan for ahead of time. A UAV pilot candidate should not be flying a UAV within an assigned workspace until all competencies have been obtained. It will be important to identify where the worker will continue to advance training and flight time in order to increase experience and to be able to train in variable conditions. Given that UAV operations are still a fairly new phenomenon, the best training schools may not even exist within the organization's geographic area. Travel and housing costs must be considered.

As worker safety in some industries has evolved, exceptional safety requirements like drug & alcohol testing have become commonplace and apply to both hiring criteria and ongoing randomized testing for compliance. Whereas an organization may not use drug & alcohol testing in any other part of its safety management program, deploying UAV services would seem to require a level of safety assurance that should require drug & alcohol testing as for any professional pilot. Furthermore, safe operation of a UAV may stretch the organization's safety program and require additional Occupational Health and Safety standards to be adopted. Background checks may need to be added or expanded to ensure that operators have no prior criminal history that should preclude their being hired to that role.

Consideration and negotiation may also be needed to address union exemptions or new job classifications within the organization.

V. SUMMARY

Purchasing a UAV for use as part of any operation should not be considered without a careful study of needs and requirements whether the intended use of the UAV is for security program applications or other uses. UAV operations represent new risk even while addressing security risks and require a careful and deliberate study and investigation into the proposed uses of a UAV. This is necessary in light of the expected operational impacts and other possible consequences associated with UAV use. Risk mitigation will likely require operational changes in a number of areas of the organization. Risk associated with financial, safety and reputational impacts require careful scrutiny and analysis.

UAV operator competency has a direct link to enterprise risk and must be weighed carefully in the overall operation of UAVs. Corporate diligence and effective community relations may require that UAV operations be considered in the context of good neighbour policies, privacy requirements and general practicality (operating around parks, schools, playgrounds, hospitals, recreation facilities) and other areas of sensitivity. Considering UAV operations in the context of environmental and social responsibility should result in sober second thought.

New technologies are often adopted and put into operation without a careful consideration of requirements, expectations and alternatives. This relates to good cost-benefit analysis, but UAVs also represent hidden and unexpected costs. Thoughtful analysis of UAV deployment with all stakeholders, internal and external, weighing into the discussion is an important step toward a final decision about the viability of UAV adoption.

Resisting the temptation to adopt new technology without having considered the full range of practical, cost and risk issues is important given any technological change affects normal operations. Before UAVs are deployed the need must be quantified and weighed against the cost of uptake. Costs must also include consideration of negative consequences and alternatives. Input from across the organization allows for a greater likelihood of a good decision-making process.

As with the adoption of any new technology, careful study, vendor qualification, partnering, training, change management and organizational impacts need to be considered fully to ensure the successful article submission to the *Infrastructure Resiliency Risk Report* **–** Draft for Editing application and deployment of the technology. UAVs are not merely commodities. They represent change with the potential for serious operational impacts to the organization. A comprehensive diligence exercise prior to deploying UAVs is more likely to result in the adoption of a successful program, with clear objectives and full support for the initiative.

About the Author

**__Doug Powell__ is a security professional with more than 35 years of experience managing security and is considered an expert, internationally, in several disciplines. Doug has worked for BC Hydro since 2006 where he has managed critical infrastructure security through three major projects: the 2010 Winter Olympics, smart grid deployment, and presently with the Site C dam construction.*

Doug demonstrates leadership serving professional committees and organizations internationally. Doug has served ASIS International as Council Vice President and as Chair of the Critical infrastructure Working Group. Doug was also 2nd Vice-Chair of the Utilities Security Council of ASIS. Doug has served at IRRG since 2014 as an advisor to the organization and on the Steering Committee for IRRG's International Urban Security & Resilience Conference. Doug holds two professional security certifications: Certified Protection Profession (CPP) and Physical Security Professional (PSP).

Doug is an accomplished speaker and educator, internationally who has authored 15 white papers, as well as having several articles published in professional journals. Doug has won awards, including CSO of the Year (2010), Security Program of the Year (2011) and was named recipient of the prestigious ASIS Roy Bordes Award for volunteer leadership in 2017.

Balancing "What You Know" Verses "Who You Know" in Emergency Management

*W.T. (Bill) Isaacs, C.E.T., **
President, Crisis Leadership Ltd.
Email: crisisleadership@gmail.com

I. Introduction

Does the old saying "it's not what you know but who you know" apply to emergency management?

I am sure you have heard this saying before which implies that even if you know very little you can still get ahead and be successful in an organization by knowing someone important or influential.

I have spent over 46 years in the energy industry in various capacities. Early in my career, when most organizations were all top down driven (believe it, there are still some out there), I saw evidence of this phenomenon. I witnessed people who potentially knew very little, but attached their careers to the coat tails of others to ride their way to success. There were situations where the perception was unqualified individuals received accolades and promotions simply because they were good friends with senior leaders. What I also observed was that over the longer term, if these individuals did not produce measureable results, they didn't last long. They were eventually found out and left the organization. In today's business climate of achieving maximum profits, senior leaders can seldom support individuals who are not achieving results.

So how does this apply to emergency and security management? To be successful in the world of emergency and security management, it has been proven time and time-again that if you do not know what you are doing, you will be found out after a major incident. Emergency management is one of those few areas of responsibility that can quickly expose flawed planning or unmanageable processes during an emergency event. It is the Emergency Managers responsibility to develop appropriate company response plans to incidents, as well as resilient processes to support the organization.

In the field of emergency management, I suggest "it is not so much who you know, but who you should know". Essentially it may be great to know some influential people, but during an emergency event *"who you should know"* in order to assist you and your organization during a crisis is more important. I have found "who should you know" is of greater value than some influential senior positions who either may not be available when you contact them or will be busy with their own issues when you need them. You need to develop a network of those "go to" individuals who can and will help you succeed in times of crisis.

In this field your networking skills is key. Being responsible for an organization or agency's emergency and security plan development, as well as ongoing maintenance, is an important role. Your employer trusts you to develop tested and compliant response plans in the unlikely event that a significant emergency situation arises. Your planning efforts should mitigate the risks and offer clear instructions, processes and procedures for employees and senior leaders to follow in order to reduce the impact to the public, employees and the organization as a whole. You cannot fulfill this role on your own. You will require support within your organization from the departments that have interdependencies with your area during an event. This requires relationship building with all interested parties in your company. Key areas; such as Engineering, Health and Safety, Media Relations and Legal (to name a few) are critical. Do not forget departments; such as Procurement, IT, Human Resources or Accounting, as these activities can and will supply invaluable administrative support to a resilient and effective emergency response. During a crisis, it is imperative to establish trust and solid working relationships with key internal departments. Emergency and Security Management Plans need to include all of these departments to understand how they will be impacted by an incident and what resources they will be asked to supply in a crisis. They need to support the company emergency plan and be offered adequate training to help in their understanding and support of these emergency plans.

You will also require support externally. This could be in the form of local first responders, emergency response organizations, municipalities, provincial and/or federal agencies, police services etc., as shown in Figure 1. Developing and maintaining this networking circle will require more effort on your part. You will have to make yourself known to each group by meeting with them face to face, joining local emergency or security working groups or associations, or being involved with local emergency exercises where available. These external relationships must be built proactively before the actual incident occurs. Handing out your business card or making an introductory phone call at the onset or on the scene of an emergency situation is way too late.

Networking with your internal and external peers builds contacts with individuals who can assist you either with your day-to-day plan development or during an incident. Learn to be a good listener. Your contacts may have experience in areas you have not yet come across and can supply vital insights into how to deal with these situations. Rare incidents, such as large earthquakes or terrorist threats require a specific response and you are not expected to have first-hand experience or expertise in all hazards.

Peers may have resources, equipment or supplies available that you could call upon if you found yourself needing this assistance. Alternatively, they may need resources, equipment or supplies that you may provide. Share the areas where you could assist them in the event of a major emergency situation. It is not just about resources; it is about building relationships. You can learn a great deal by sharing experiences and first-hand knowledge with others having the same responsibilities for their organization or department.

II. KNOWING A CRISIS LEADER

A good leader during a crisis has the ability to lead the staff under them, but also lead up and across to other teams. Having the ability to foster relationships with the multitude of people that emergency managers will work with is integral in accomplishing the necessary tasks during a crisis. Decisions must be made in a timely fashion as there is no time for "management by committee". An emergency situation exhibits true leadership skills. Learn from the mentors you have come to know and hone those skills they exhibited that impressed you during an emergency situation. A key element is the ethical component of decision-making. This is dealing with the challenges of knowing that the right decision was made even when that choice was unpopular. Making the decision to shut down a pipeline or evacuate a facility could cost an organization hundreds of thousands of dollars. On the contrary, diverting greater environmental damage or injuries to employees or the public is a far greater saving.

Improving collective decision-making capacity needs to begin at the leadership level. Crisis Management Structures should mirror the current workforce. Know the diversity of your resources. By increasing the amount of diversity among the organizations' leaders and teams, this will increase the collective knowledge base among those individuals working together. Consider diverse backgrounds and gender differences to yield different opinions and methods of examining an issue. The demographics of the emergency management community are quickly evolving due to retirements and internal company changes to leadership teams. Therefore, teams need to reflect those changes to maximize their collective intelligence. The decision-making chain should be automatic during an event embracing the collaboration culture.

Internal and external contacts are key during the recovery phase of an incident. Recovery is truly an area where *"who you should know"* could greatly affect the outcome of a crisis. The recovery component of an incident is comprised of a diverse set of needs and each is essential in the overall recovery of a community or an organization after an incident. Most organizations do not prepare detailed plans for recovery and seldom ever practice these plans during emergency exercises. Recovery plans are complicated and can vary from one type of incident to the next. Many organizations and agencies do not spend much time or effort and certainly not much money in the development of recovery plans for those reasons, but it can be done. An important shift needs to occur, but this shift will be slow until the spending and planning for recovery efforts increase. Response and recovery departments are often separated from one another, and in larger organizations, may not know one another. Successful recovery efforts are those that link all affected external and internal stakeholders to support the community to rebuild itself to feel safe again.

Exercising protocols of your emergency or security management plans develops what I refer to as "process muscle memory" that allows emergency professionals to react quickly. It is essential that the training is conducted in a way that allows for flexibility during an incident. Emergency situations do not care about provincial or international borders, areas of jurisdiction, time of year or if you are prepared. Emergency situations are going to occur whether you are prepared or not.

Conventional emergency training programs have benefits in process muscle memory and habits, but these could be detrimental during an event where flexibility is required. Situations like workplace violence incidents or natural disasters, such as forest fires where control of the situation is dynamic and constantly changing events require flexibility to respond to and recover. Training programs that offer working with interactive groups and solutions instead of simply reviewing stringent company policies can lead to elasticity in your processes and provide your crisis management team members with the ability to rely on their experience, education and training. They will also get to know each other better and work as a team.

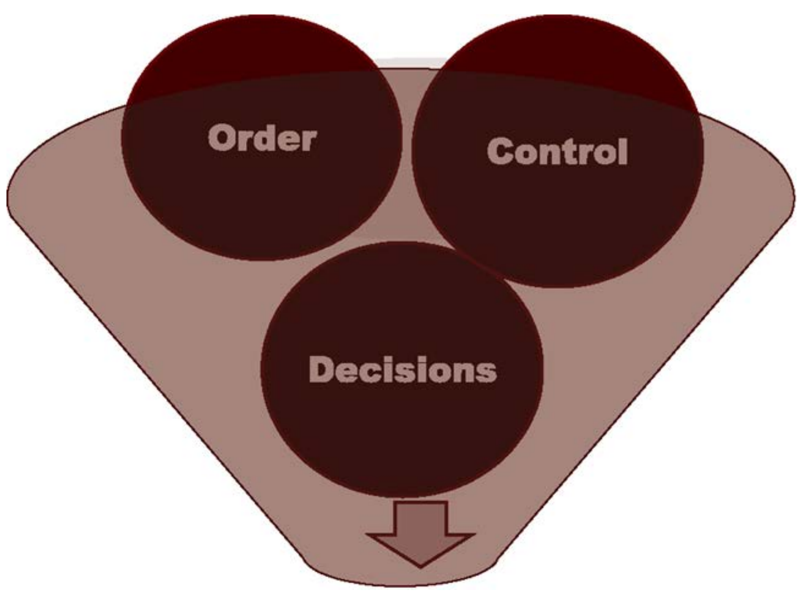

Figure 2

Time

Leaders need to learn to identify the difference between order and control during an emergency, as control can hinder order. See Figure 2. Incident Command Systems attempt to control incidents via objective setting, forecast-based planning and a hierarchical structure. Complex company crisis management structures, along with rigid company response processes can hinder company response by controlling the decisions and not the incident as time is critical. I often remind clients, *"To successfully come out of a crisis, it will not depend on the number of levels in your crisis management structure, but the quality of the leaders in your crisis management structure."*

In my experience, I have found emergencies have two high-level dimensions, the:

1) Operational issue (fixing the problem), and
2) Communications issue

Providing an imperfect operational response to a crisis, but led with a strong communications aspect, means the organization will likely survive the scrutiny to follow. However, providing a strong operational response coupled with a failed communications aspect means you are going to struggle with your recovery.

Part of the education process is allowing team members to use the internal tools available to them allowing for more fluidity of responsibility during an emergency. Share with employees their involvement of your Business Continuity Plan or emergency and security plans -- let them get to "know who they should know". Empower employees with the processes, procedures and training to use in a crisis. Emergency planning should be approached as a cost saver, not a cost centre. Detailed emergency plans that will stand up to today's high level of scrutiny and executed with trained staff can save a company or an emergency service millions of dollars versus utilizing outdated plans causing lost revenue and damage to the organization's brand image. Our employees, customers and shareholders deserve it, and public safety expects it.

During times of crisis it gets down to how much you know, "*who you should know*" and how you lead with that knowledge that will make the difference.

About the Author

***Bill Isaacs** has over 40 years of experience in the natural gas industry and has held positions of increasing responsibility, including engineering, gas transmission and distribution field operations, operations training and Emergency & Security Management.*

Bill is an original member of the Technical Committee responsible for the development of CSA Standard Z246.l Security Management for the Petroleum and Natural Gas Industry, as well as the Technical Committee for CSA Standard Z246.2 Emergency Preparedness and Response for the Petroleum and Natural Gas Industry.

Bill has performed emergency recovery work for natural gas systems in the damaged areas of Hurricane Katrina and Hurricane Sandy. He is the recipient of the 2013 Canadian Gas Association's Lifetime Safety Achievement Award (published in the Ontario Technologist and the Infrastructure Resilience Research Group, Faculty of Engineering & Design, Carleton University.

Using Design Basis Threat in Critical Infrastructure Protection

*Ross Johnson**
Bridgehead Security Consulting Inc.
Email: ross@bridgeheadsecurity.com

Abstract
This article explains what a design basis threat is and attempts to show how it is used in assessing physical protection systems. This is just an article, though, and not a substitute for formal training.

Discussions of attacks on critical infrastructure are sensitive, and to avoid the problem I have demonstrated how the process works using a simpler target – a house.

I. BACKGROUND

In ear1y 2016, the Electricity Information Sharing and Analysis Center in Washington, DC, released a document called the Design Basis Threat for the Electricity Sector. This product was created by the Physical Security Analysis Group (PSAG) -- a team of 25 experienced electricity sector security professionals. Through two-and-a-half days of discussions and arguments facilitated by a representative from the U.S. Department of Energy's Pacific Northwest National Laboratory (PNNL), we sought to define the likely threats to bulk electric system assets by answering a few questions:

- For each category of threat (low, moderate, and high), how many people would likely be involved? How motivated are they? What kind of weapons, equipment, tools, knowledge, and skills will they have? Are they insiders or outsiders, or both? In other words, what would the adversary, and their actions, look like?
- What are the unacceptable consequences of an attack? What are the kinds of activities they would undertake which, if successful, would be considered a 'win' for them and a 'loss' for us?

A design basis threat (DBT) has its roots in the nuclear industry. The U.S. Nuclear Regulatory Commission defines a DBT as: *"A profile of the "type, composition, and capabilities of an adversary."* [1] The International Atomic Energy Agency states that: *"A fundamental principle of physical protection is that it should be based on the State's current evaluation of the threat."* [2]

This principle performs three functions. It:

1) Reduces conflicts of interest by removing from the organization who must address the threat and the responsibility of also defining the threat;
2) Ensures the State's security and intelligence support to the solution of the protection problem; and
3) Implies approval of funding to solve the protection problem.

---

[1] https:/lwww.nrc. gov/reading-rm/basic-ref/glossary/design-basis-threat-dbt.html
[2] http://www-ns.iaea.org/security/dbt.asp?s=4

We created the Design Basis Threat for the Electricity Sector (DBT-ES) "to be used to assess the physical BES infrastructure based on current reasonable and credible threat considerations." It is a starting point for threat assessments, and it is expected that local conditions would have an impact on its conclusions.

II. The VISA Process

The DBT provides the foundation for threat assessments and is also used to test security measures and plans. PNNL uses a process called Vulnerability of Integrated Security Analysis (VISA) to use the product of the DBT to design attack scenarios which are then war-gamed in detail against the target's security measures.

The VISA process starts with the selection of a core System Effectiveness Analysis (SEA) team. The team should consist of:

- a security systems or security operations specialist;
- a physical protection systems subject matter expert familiar with the physical protection system under evaluation;
- a cybersecurity subject matter expert; and,
- on-site security supervisor, or someone with overall security responsibility for the site. Depending on the complexity or purpose of the site, someone intimately familiar with site operations should be included on the team and if outside security resources figure into the protection plan then they must be included as well.

At its most basic level, the VISA process uses a team approach to search for vulnerabilities in the site protection plan, designs realistic and credible scenarios to exploit those vulnerabilities then tests the scenario against those components of the protection plan that lie in the path of the adversaries.

The SEA test involves two assessments. In the first assessment, the team compares the time required by the adversaries in their attack, and the time required by the response force to stop the attack. If the adversaries reach their objective before the response force stops them, then the adversaries 'win', and the physical protection system fails. The second assessment involves rating the effectiveness of the security measures in place on the attack path, and by extension an overall rating of the effectiveness of the physical protection measures.

After this first assessment, the group then considers detailed technological and procedural enhancements to the physical protection system and re-runs the simulation to see if the system effectiveness is improved by these changes. The process is repeated as necessary until the team is satisfied that their proposed system will meet their needs.

Using this process, the team can both improve the system and provide quantifiable data that can be used to build the business case for security system upgrades.

---

[8] Bulk Electric System, defined by the North American Electric Reliability Corporation as, with exceptions, electrical grid assets of 100Kv and higher. Please see https:/lwww.nerc.com/files/glossaryofterms.pdf for a more precise definition

[4] The Design Basis Threat for the Electricity Sector is available through the Electricity Information Sharing and Analysis Center (E-ISAC). Considered a sensitive document, it is available only to NERC members.

An Example

We will use residential security as an example of the VISA process because it's the simplest and everyone can relate. A homeowner, concerned about the safety of her family, conducts a threat and vulnerability assessment on her home with the assistance of two friends – a police officer and a firefighter. As a result of this assessment, she believes that the most serious reasonable and credible threats come from fire, carbon monoxide poisoning from her furnace, and a single intruder breaking into her home to steal her valuables. Her physical protection plan is based on the requirement to deter thieves, detect them, accurately assess their intentions, and delay their progress to allow law enforcement to respond and apprehend the intruder. Her physical protection system includes solid wood external doors, high quality deadbolt locks, and the installation of an intrusion detection system (IDS).

The homeowner contracts a national security system company to do the work. She has door sensors installed on all external doors and motion sensors covering the hallways on the main floor. She has carbon monoxide detectors and smoke alarms wired into the IDS as well.

To test her physical protection system, she puts together a small team that includes the security company sales representative, a carpenter with security experience, and the police officer who assisted her earlier. They walk through the home, searching for vulnerabilities. They assess that the weakest part of the physical protection system is the ground floor windows.

The team develops a scenario where an intruder enters the backyard in the daytime when the family is out of the house, breaks a kitchen window, and enters the main floor. He then goes upstairs and steals jewelry and electronic devices. He leaves through the front door.

Any assumptions about the scenario should be clearly stated and recorded. In this case, the assumptions are:

- The intruder is not seen by a neighbor while in the backyard.
- The security company alarm centre remains in contact with responding law enforcement, updating them on the status of sensor alarms in the home.

This attack path is broken into tasks that the intruder must complete in order to complete his mission. They are described in the following steps. Intruder:

Step 1: Enters backyard and approaches kitchen window.

Step 2: Breaks kitchen window and climbs into home.

Step 3: Stops and listens for activity in the home.

Step 4: Goes upstairs.

Step 5: Searches for and steals valuables.

Step 6: Goes downstairs and out the front door

Step 7: Leaves the area

All seven steps must be accomplished before law enforcement arrives. The response force timeline is as follows:

Response Force Time-Line	Time (sec)
IDS alarm triggered and security company alarm centre calls homeowner	60
Homeowner confirms with security company that the alarm has not been accidently triggered	30
Security company alarm centre calls 9-1-1 on behalf of homeowner and briefs operator	30
9-1-1 operator dispatches police officer	15
Police officer travels to residence	300
Police officer arrives on scene and conducts assessment	60
Total response force time	495

We now know that the intruder must accomplish all seven steps within 495 seconds, or 8 minutes and 15 seconds.

The next step is to assess the steps against the security measures. Pd, P., P., and Pn, refer to the probability that the protection system would detect the intruder, accurately assess the intruder's activity, engage the intruder, and finally, neutralize the intruder. They are expressed as Very Low, Low, Moderate, High, and Very High. (Because of space, only the first letter is used in the table presented below.) The step score is the lowest of all the probabilities in that step, so if they are all high and one is low, the step score is low. At the end of the simulation, the highest step score becomes the overall system effectiveness score.

In Step 1, 'Intruder enters backyard and approaches kitchen window' takes 15 seconds. The cumulative time is 15 seconds, and as law enforcement has not yet been dispatched, 495 seconds remain on the response clock. As the protection system does not cover the backyard and outside the window, the chance that it would detect, assess, engage, or neutralize the intruder at this point is very low.

In Step 2, 'Intruder breaks kitchen window and climbs into home' the intruder takes 30 seconds. The total accumulated time of the attack is 45 seconds, but as the motion detectors on the main floor only cover the hallways and not the kitchen, the IDS has not been triggered and the response force has not been dispatched, so they are still at least 495 seconds away. The probability of the protection system detecting, assessing, engaging, or neutralizing the intruder remain very low.

Step 3 takes 30 seconds, and the protection system has still not been triggered so nothing changes on the rest of the row.

The IDS alarm is finally triggered in Step 4 when the intruder enters the hallway to go upstairs. In this case, the probability of detection is very high, but the alarm itself is insufficient to accurately assess the situation, so it and the other probabilities remain very low.

In Step 5, the intruder is upstairs searching the bedrooms. There are no security sensors upstairs, so the IDS is not contributing anything at this point. The response force clock is running, though, and at the end of this step, there are 375 seconds left before the police arrive.

In Step 6, the intruder goes downstairs and out the front door. It takes him 15 seconds. The IDS will pick up the movement in the hallways and when the front door opens, and we will assume that this will be communicated to law enforcement by the security company alarm center. This information would help the responding officer to accurately assess the situation.

In Step 7, the Intruder gets into his vehicle and leaves the area. The police are still 340 seconds away.

Step	Step Time (sec)	Cumulative Time (sec)	Remaining Response Time (sec)	Step Description	pd	P.	P.	P.	Step Score
1	15	15	495	Intruder enters backyard and approaches kitchen	VL	VL	VL	VL	VL
2	30	45	495	Intruder breaks kitchen window and climbs into	VL	VL	VL	VL	VL
3	30	75	495	Intruder stops and listens for activity in the home	VL	VL	VL	VL	VL
4	15	90	495	Intruder goes upstairs	VH	VL	VL	VL	VL
5	120	210	375	Intruder searches for and steals valuables	VL	VL	VL	VL	VL
6	15	225	360	Intruder goes down the stairs and out the door	VH	M	VL	VL	VL
7	20	245	340	Intruder leaves the area	vL	[illegible]	vL		VL
								Overall System Effectiveness	VL

At this point, it is clear to us that the IDS has done little to help protect the home beyond perhaps reducing the amount of time the criminal spent inside looking for valuables. The homeowner and her team discuss changes to the physical protection plan that could improve detection and assessment. Some potential improvements might be:

- The addition of a glass break sensor on the main floor would instantly trigger the alarm the moment the criminal broke the kitchen window, which would start the response force activity 60 seconds earlier
- CCTV cameras outside the home and on the main floor would help in three ways: it would deter many thieves because it shows that the home has a security system; it would improve the probability of accurate assessment of the situation; and it would also provide valuable evidence for law enforcement when conducting the investigation.
- Laminated glass windows on the ground floor are very difficult to break without making a lot of noise and potentially attracting attention. Use of this type of glass could easily add several minutes onto Step 2.
- Security bars on ground floor windows will act as a deterrent and make it very difficult for a thief to get through. The options would shrink to trying to get through a door, which would take time and set off the IDS when it opened, or to use a ladder and try a second-floor window. This would be a bold move in daylight, and thief would be most likely to move on and try another house instead.

In this case, the homeowner elects to go with the glass break sensor, CCTV cameras, and laminated glass windows. The team reruns the simulation, and as you can see, the improvements have improved the response from 340 seconds after the intruder leaves the area to 160 seconds. It is still not enough to defeat the intruder in this scenario, but we are seeing progress.

Step	Step Time (sec)	Cumulative Time (sec)	Remaining Response Time (sec)	Step Description	pd	P.	P.	P.	Step Score
1	15	15	495	Intruder enters backyard and approaches kitchen window	VL	VL	L	VL	VL
2	120	135	360	Intruder breaks kitchen window and climbs into home	V H	VL	V L	VL	VL
3	30	165	330	Intruder stops and watches for activity in the home	VL	VL	v L	VL	VL
4	15	180	315	Intruder goes upstairs	v H	v H	v L	VL	VL
5	120	300	195	Intruder searches for and steals valuables	VL	VL	v L	VL	VL
6	15	315	180	Intruder goes down the stairs and out the door	v H	v H	v L	VL	VL
7	20	335	160	Intruder leaves the area	VL	VL	v L	VL	VL
									VL

At this point, the homeowner can make informed decisions about the cost and benefit of any other security system upgrades, such as using window bars on the ground floor. Other scenarios should be tested as well.

III. Lessons Learned from VISA Simulations

You can learn a lot about the effectiveness of physical protection systems by using the VISA process. Some of them are:

- Be sure to carefully consider what winning and losing looks like. What is the aim of the adversary? Can you thwart the aim by means other than brute force?
- Measures that enhance resilience are good insurance against the failure of a physical protection system.
- If possible, use performance testing to determine how long the intruder would take on each step. If you cannot performance test, there is good research available on the Internet. (For example, it takes two men 12.5 minutes to cut a four-square-foot hole in 3/8" mesh X 11-gauge fence.[5] Another excellent source of information on security measures and their effectiveness is the U.S. Army's field manual FM 3-19.30 Physical Security, available for download free at the link in the footnote)
- Winning against an outsider high threat is a lot harder than it looks – do not expect to be successful in the first few simulations.

- Bring in the experts:
  - Talk to law enforcement to determine how they would handle the response to your scenario. We may assume that they would show up and make an arrest, but you may find that their procedure would be to stand off, assess the situation, and call in backup, which would add a lot to the response time and could allow the adversary to achieve their aim. You may be able to mitigate this by installing additional security measures that they could use to help with their scene assessment, such as additional cameras.
  - Bring in Operations early in the DBT and VISA process. They are best suited to tell you what is worth protecting, and what isn't. You may be surprised how that changes your assessment.
- Some security measures are more effective than others, and cost often has little to do with it.
- Anything you can do to start the response force earlier will help you in the end.
- Procedural security methods cost little and can be more effective than technological measures.

IV. CONCLUSION

The DBT is an important tool for the protection of critical infrastructure because the process ensures that as much experience and information as necessary is brought to bear on the threat assessment. The VISA process, if it is done carefully and properly, is an excellent tool to help us use the DBT to design and enhance our physical protection systems.

---

[5]http://www.associationsites.com/clfma/collection/CLF-TP0211 Tested and Proven Performance.pdf

[e]https:/lwww.wbdg.org/FFC/ARMYCOE/FIELDMAN/fm31930.pdf

About the Author

***Ross Johnson**, CPP is the founder of Bridgehead Security Consulting, Inc. He is the Co-Chair of the Physical Security Analysis Group - a team of subject matter experts who support the Electricity Information Sharing and Analysis Center (E-ISAC) in advising electricity industry participants and governmental agencies on threat mitigation strategies, incident prevention and response, training, emerging security technologies, and other relevant topics to enhance electricity industry physical security and reliability.*

Natural Hazards and Decision Science: An Interdisciplinary Insight for Critical Infrastructure Protection in Space Weather Events

*Amaury Carruzzo, Ph.D.**
Department of Atmosphere & Oceanic Sciences
McGill University
Email: amaury.carruzzo@mail.mcgill.ca

*John Gyakum, Prof.**
Department of Atmosphere & Oceanic Sciences
McGill University
Email: john.gyakum@mail.mcgill.ca

Abstract
Natural hazards impacts are particularly important for Critical Infrastructure (CI) protection. In this instance, like other natural hazards, geomagnetic storm events can occur at any time, and a single space weather episode may produce multiple effects. Facing them demands CI stakeholders to take early decisions that involve trade-offs among impacts, probability and lead-time of a natural hazard forecast. Nevertheless, an interdisciplinary research could provide an innovative approach for customizing the decision aid process to CI managers dealing with those natural events. This paper offers some insights that could bring a new paradigm in natural hazard-related decisions for CI protection, applying up-to-date techniques from space weather science and cutting-edge methods from decision analysis.

I. INTRODUCTION

It has been known throughout human history that different types of natural hazards can affect life on Earth. The potential impacts of natural hazards (e.g., floods, heatwaves, tornados or geomagnetic storms) are particularly important for Critical Infrastructure (CI) protection; such as water systems, energy power facilities, satellite communications, transportation systems, and so on (Gaetano et al., 2013; Quigley et al., 2017). As a part of the decision-making process for disaster risk reduction, it is fundamental to find a set of mitigation actions for the CI protection in a given natural hazard event (Wachinger et al., 2013).

However, mitigation selection under natural hazard uncertainty can be a challenging procedure to the design of a new suite of environmental services, as interdisciplinary research (Wong-Parodi and Small, 2019). According to Hardy (2019), interdisciplinary research *"implies integration that combines separate perspectives through the development of connections between them."* Furthermore, the development of such a study requires input from teams of natural scientists, engineers, social and behavioral researchers to understand how different stakeholders use natural hazard information (observation and forecast) to decide. For example, the ability for CI managers to engage mitigation plans based on early warning systems to avoid both damages to facilities and potential loss of human life following a CI disturbance (Oughton et al., 2019).

To improve the quality of natural hazard management and risk analysis, a customized decision aid model could provide information about impacts, uncertainties, the set of mitigation alternatives, and their associated benefits based on personal preferences (Caruzzo et al., 2018). In the context of a space weather hazard, according to Fiori et al. (2015), and Ngwira and Pulkkinen (2016), a physicist might provide content expertise about solar activity and potential extreme events (Figure 1), such as Solar Flares (explosions of large quantities of energy and radiation) or Coronal Mass Ejections – CMEs (ejections of plasma).

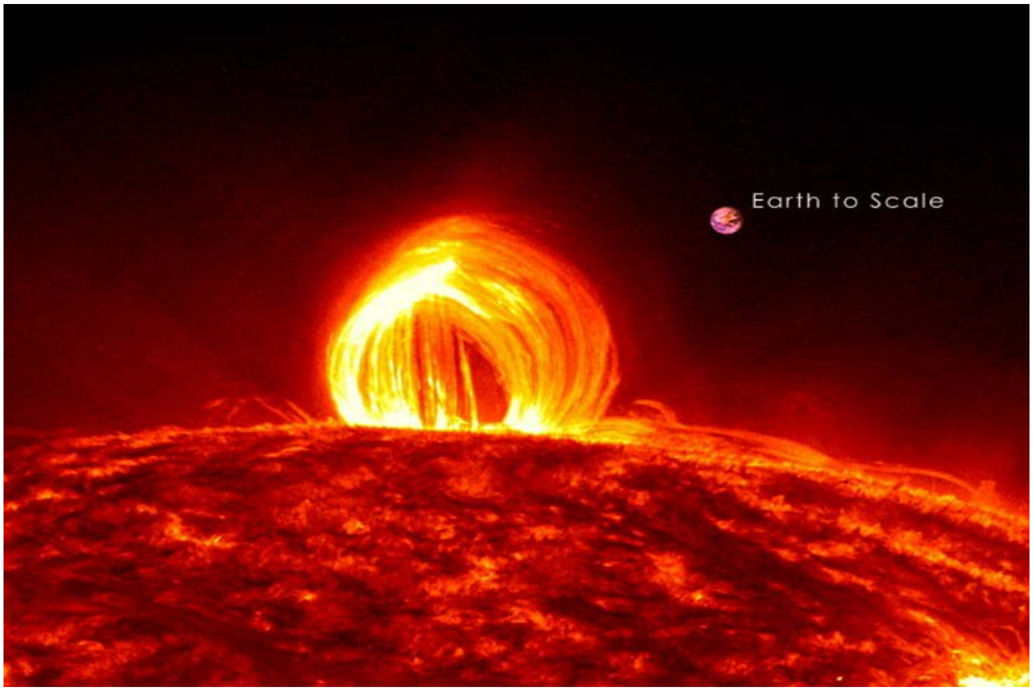

Figure 1: Arcs of plasma on the Sun's surface captured by a high-definition telescope aboard NASA's Solar Dynamics Observatory (Source: courtesy of NASA/GSFC/SDO)

The Sun, our nearest star, is the primary source of space weather. The Northern or Southern Lights (or Auroras, Figure 2) are caused by space weather events (Boteler, 2018). The Auroras are considered to be spectacular examples of space weather, but extreme events could be devastating for our modern technological society because they could directly affect several infrastructure/facilities, such as the power grid or satellite systems (see details in section II).

Figure 2: Images of Aurora Boreal in Yellowknife, Canada (Source: PIXABAY)

Supporting decision-making using space weather data (observation and forecasting) is a very demanding process in which several stakeholders can often have different interpretations of vulnerabilities and impacts. It is important to note that, like other natural hazards, extreme solar events can occur at any time and a single space weather event may produce multiple effects (Cannon, 2013; Krausmann et al., 2016). Boteler (2018) also points out that different space weather events exhibit differences in occurrence across a wide range of temporal scales (minutes to days).

We therefore, intend to provide an interdisciplinary insight as an innovative research design for a natural-hazard decision aid process from the user's perspective. As a demonstration, we applied it in a simplified case study for a Satellite in Geostationary Orbit (GEO) against an extreme space weather event.

II. Background

a) Critical Infrastructure Protection and Space Weather Threats

According to Public Safety Canada (Canada, 2009), 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."* As pointed out by Klatt (2016) and Quigley et al. (2017), the risk to specific CI in Canada is variable, and the overall risk is not well known. In this regard, the resilience of CI may depend on natural hazard forecasts that warn stakeholders to take selected mitigation actions to safeguard their systems and reduce the potential negative consequences.

Space weather impacts are relatively unfamiliar to the general public, but geomagnetic storms are recognized as a new natural hazard of the modern technological age (WEF, 2019). According to Oughton et al. (2019), space weather is a high impact, low frequency (HILF) event. Also, as pointed out by Wasson (2018) and Boteler (2018), space weather phenomena are an international issue and not restricted by national borders. Furthermore, increasing reliance on technological systems is creating new potential vulnerabilities to extreme space weather; for example, interference in Global Navigation Satellite System (GNSS) signals for the timing of financial and control systems (Klatt, 2016).

Despite the clear benefit of taking an anticipated measure to protect against and prepare for natural hazards (Oughton et al., 2019), most organizations that are responsible for CI do not have a systemic emergency plan for extreme space weather events (Krausmann et al., 2016). As discussed by Cannon (2013) and Boteler (2018), there is a lack of awareness of the extent of space weather impacts on CI around the World. Furthermore, Fergunson et al. (2015) and Wasson (2018) present that other crucial operations (e.g., water supply) may be affected by space weather-related outages as a cascade effect. Fergunson et al. (2015) also discuss that with the advent of space-based communication systems since the 1950s, the potential space weather impact on long-distance telecommunications has increased extensively. So, all kinds of satellites in space are subject to space weather threats. Alongside space debris (Ribeiro et al., 2018), space weather remains a major concern for all aerospace operations today (North, 2017).

b) Space Weather Events and Economic Impacts

At present, several space-based and ground-based platforms are monitoring the Sun and the near-Earth space environment (Lam, 2016; Fiori et al., 2018). These data provide essential information for the mitigation of extreme space weather events (Ngwira and Pulkkinen, 2016). Although the impacts of geomagnetic storms are broadly recognized in past events (see Balch, 2015; Ferguson et al., 2015), establishing all the potential vulnerability and consequences of such an extreme event has proven to be very hard (Krausmann et al., 2016).

Regardless of the capability limitation for forecasting geomagnetic storms with relatively long lead times, Oughton et al. (2019) demonstrated that with a tailored warning system, early mitigation actions could reduce economic losses to £2.9 billion instead of £15.9 billion (only in the United Kingdom), based on current space weather forecasting capabilities. Despite the space weather 'deniers' (Ferguson et al., 2015), studies based on solid technical-scientific articles discuss the economic impacts of a severe space weather event. In the satellite segment alone, Odenwald et al. (2006) projected economic damage at around 70 billion USD. Eastwood et al. (2017) highlight the economic impact of an extreme event could reach 3.4 trillion USD worldwide.

Past Episodes and Lessons Learned

In September of 1859, the British astronomer Richard Carrington recorded the biggest solar storm ever observed (Elvidge and Angling, 2018). According to Odenwald et al. (2006) and Ferguson et al. (2015), a major event, such as the 'Carrington-event' would devastate civil and military communications and could collapse the global economy. Assessing potential impact, MacAlester and Murtagh (2014) say a Carrington event impacting the Earth could result in an extreme increase in the anomalies experienced across the satellite constellation in Earth's orbit.

In other natural hazards, several researchers have to assess the impact on critical infrastructure interdependence. For example, MacAlester and Murtagh (2014) and Krausmann et al. (2016) concluded that from previous experience of disaster events; such as hurricanes or earthquakes, the impact of power loss would build over time and affect others' CI in sequence (e.g., healthcare facilities or banking/finance systems). So, any facilities without backup power will fail immediately, even though the comprehension of extreme space weather's impacts on modern technology assets is incomplete (Cannon, 2013).

Despite the uncertainties inherent in space weather hazards, the threats are real. On July 23, 2012, the Sun launched a massive Coronal Mass Ejection (CME) that was not Earth-directed, but the fastest ever observed by NASA's STEREO-A (Solar Terrestrial Relations Observatory) spacecraft (Ngwira et al., 2013). This 2012 event offers an excellent opportunity to explore the effects of extreme space weather event, in particular, a massive CME (Carrington-caliber superstorm) within situ observations (Ngwira et al., 2013), as in Figures 3 and 4.

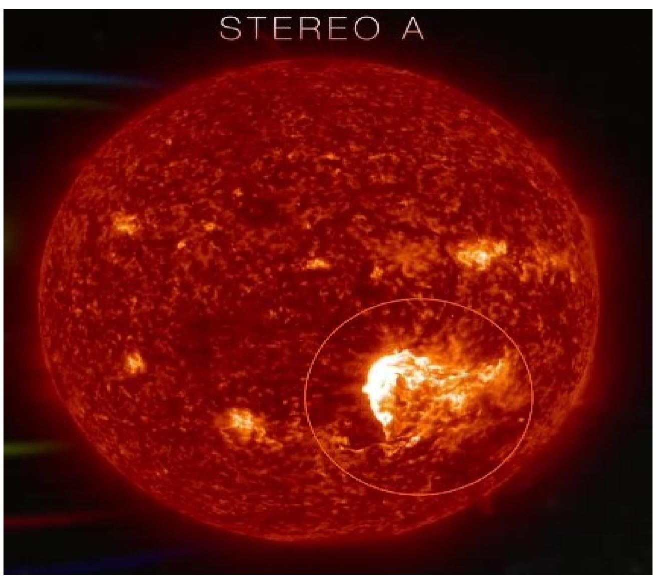

Figure 3: Image of a CME in July/2012 captured by NASA's STEREO-A spacecraft (Source: courtesy of NASA/GSFC)

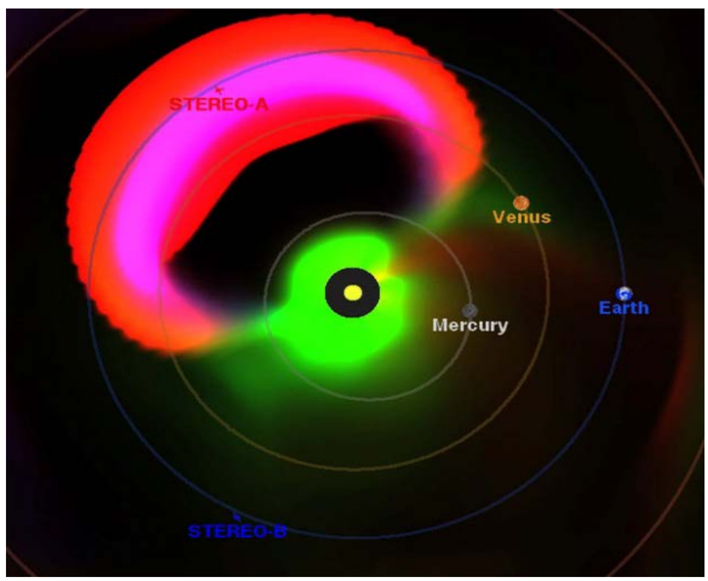

Figure 4: Simulation of CME that hit the STEREO-A spacecraft on July/2012 (Source: courtesy of NASA/ GSFC).

In this view, North (2017) stresses that this prompted the need for increased risk analysis of space weather threats. Based on this assessment, some authors call this as "Space Situational Awareness" and it has concerned several military and civilian organizations (Ferguson et al., 2015). To do so, space weather prediction and real-time observation are essential for CI protection (Oughton et al., 2019).

c) Decision Under Uncertainty and Inter-Disciplinary Research

In everyday situations the effects of natural hazards on tasks may be trivial, but in an extreme event the impacts are considerably more significant (Kox et al., 2015; Elvidge and Angling, 2018). Decision making for these high impact events typically involves many stakeholders, frequently with different interpretations of the natural hazards, which further complicates the process (Caruzzo et al., 2018). In this context, using an interdisciplinary research design has been gaining attention in natural hazard studies in recent years (Hardy, 2019; Wong-Parodi and Small, 2019). These examples also demonstrated that successful interdisciplinary studies incorporate the main ideas by each contributing area.

From a behavioral point of view, Kox et al. (2015) and Caruzzo et al. (2018) have demonstrated that the process by which practical problems are simplified into a decision aid model could be subjective, dependent on the stakeholders and the type of decision. For such problems, the users of natural hazard forecasts want to choose an alternative decision that minimizes the impacts or/and maximizes monetary gain. For example, shutting down a power station to prevent harm from geomagnetically induced currents will result in a loss of income, but could prevent serious damage to electrical power systems (Weigel et al., 2006; Fiori et al., 2015). In fact, according to MacAlester and Murtagh (2014), the vulnerability of electric power to an extreme geomagnetic storm remains the primary concern from an emergency management perspective.

Forecast-based action

In certain extreme events, stakeholders are required to identify the best mitigation actions to save human life and/or protect infrastructure. To address these challenges on the practical side, one of the innovative approaches shows a prediction based on actions, instead of the natural hazard variable (Caruzzo et al., 2018). For example, "tomorrow all schools will be closed," as an alternative for "tomorrow there will be 60 cm of snow." In accordance with this new design, some humanitarian organizations have been applying a similar approach, e.g., Forecast-based Financing – FbF (Coughlan-de-Perez et al., 2015) or Early Warning Early Action Systems – EWEA (FAO, 2018). These methods use impact levels as a trigger to take early mitigation action. From the end-user perspective, that is a new way to customize products/services to anticipate measures and tailor risk communication based on natural hazard impacts for each decision context.

Probability and lead-time trade-off

Deciding under natural hazard uncertainty can be a subjective and complex process. That is, non-expert stakeholders choose according to their personal experience and natural hazard perception (Wachinger et al., 2013; Kox et al., 2015). Several recent studies used decision theory related to or motivated by analysis of space weather hazard problems (Elvidge and Angling, 2018). Weigel et al. (2006) evaluated a prediction model's performance from the user's perspective based on the user seeking to maximize monetary gain. Park et al. (2017) applied decision-making based on skill scores to a Solar Flare Forecast Model in cost-loss ratio situations. They propose a minimum probability threshold for the action to minimize economic expense based on data from the flare forecast model.

Some best practices from other areas are also of interest (Henley and Pope, 2017). In the hydro-meteorological community, there have been alot of practical studies done to improve decision making using terrestrial weather information (Uccellini, 2016; Alley et al., 2019). For example, the analysis of the users' weather hazard perspective shows evidence that individual characteristics are related to probability and lead-time weighing variations (Caruzzo et al., 2018). There are alot of potential explanations for this finding: a lack of risk perception, prior experience, human behavior under uncertainty, and risk profile, among others (Wachinger et al., 2013; Caruzzo et al., 2015; Kox et al., 2015). Applying questionnaires, surveys, and interviews (as methods of eliciting preferences), these studies showed that evaluating preferences may be best understood by considering how the decision makers interpret the natural hazard resulting from uncertain information or warning messages, and the trade-off between probability and lead-time.

The findings about the relationship among natural hazard information, risk communication, and early decision under uncertainty could be a good starting point for the space weather community. For example, according to Caruzzo et al. (2018), the key element is the understanding of the temporal (lead-time) and uncertainty (likelihood) dimensions of the natural hazard impacts (Figure 5).

According to current practice (Fiori et al., 2015; Lam, 2016), the end-user (e.g., critical infrastructure manager) receives a space weather bulletin or warning message and makes a decision according to their personal experience and space weather risk perception. They may have a question if the probability is high enough (e.g., above 70%) and lead-time is short enough (e.g., less than 10 hours) to take action for preventing economic loss (Scenario A on Figure 5).

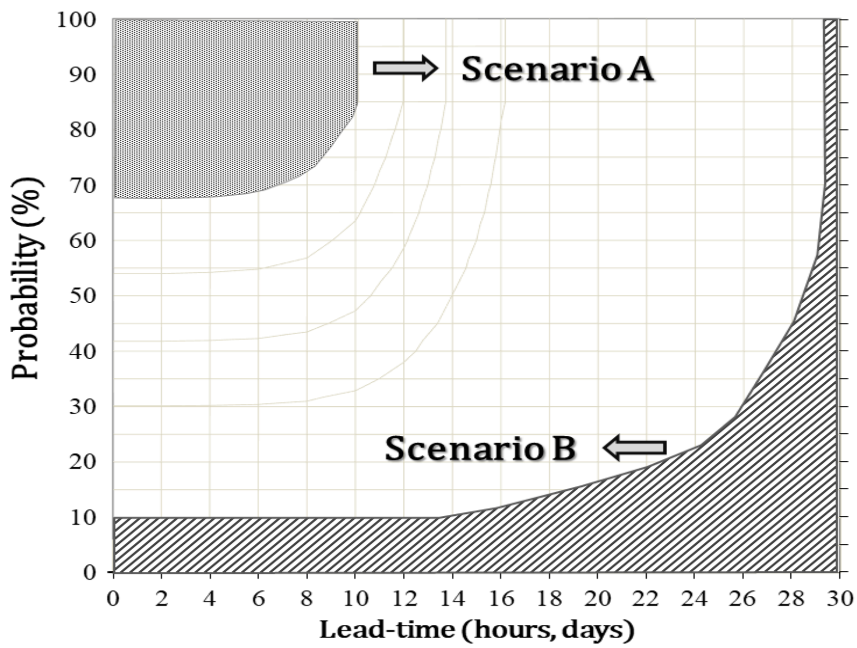

Figure 5: Natural hazard probability and lead-time trade-off, where Scenario 'A' has a high probability and short lead-time, and Scenario 'B' has a low probability or long lead-time (Source: adaptation Caruzzo et al., 2018)

d) Probabilistic Space Weather Forecast and Decision Making

Over the last few years, significant progress has been made in space weather observation and forecasts, and there are a number of ongoing efforts to apply several techniques (e.g., Nikitina et al., 2016; Fiori et al., 2018). Research and modeling of space weather and solar-terrestrial geomagnetic activity have been extensive and operational forecast centers, such as the Canadian Space Weather Forecast Centre – CSWFC (Fiori et al., 2015; Lam, 2016).

More broadly, according to Henley and Pope (2017) and Murray (2018), the international space weather community is trying new approaches used by other research communities to enhance current predictions (e.g., probabilistic forecasting). That is, when mathematical techniques or multiple predictions from different methods are combined to create an ensemble forecast with a likelihood (Figure 6). One of the most recognizable examples of probabilistic weather forecasting for the public is a prediction for a hurricane (Figure 7).

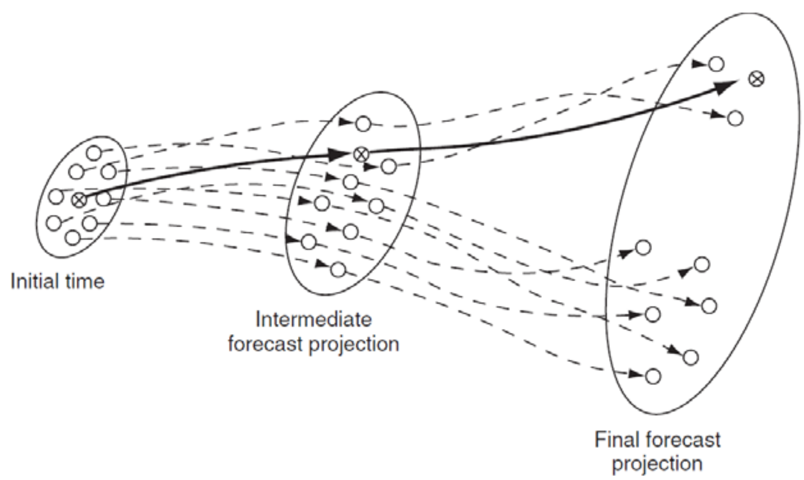

Figure 6: Illustration of ensemble forecasting, where the dashed lines represent the individual ensemble members (probabilistic), and the solid line represents the deterministic forecast (Reproduced with permission: Wilks, 2011, p.271)

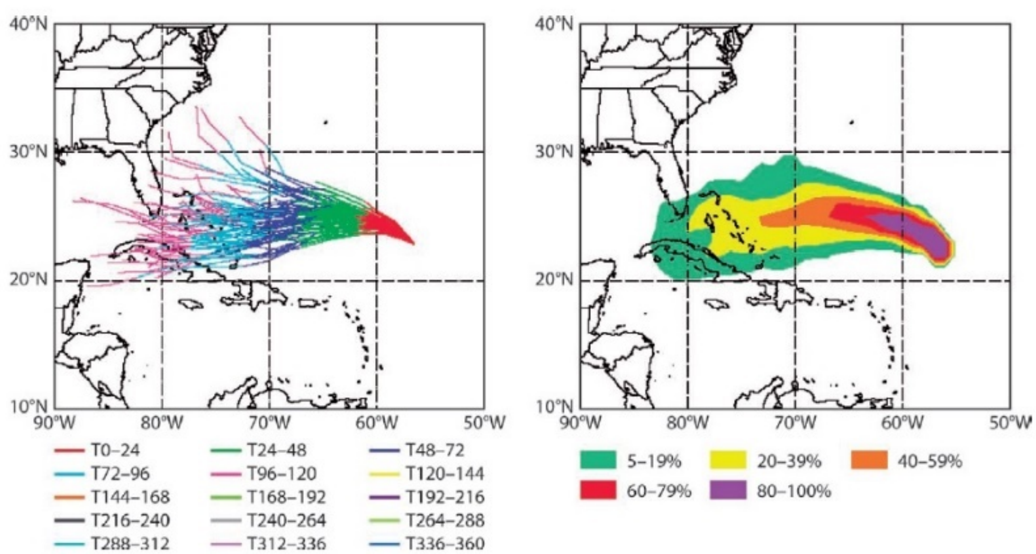

Figure 7: Ensemble forecast tracks (left) and strike probabilities (right) for hurricane Ike (Reproduced with permission: Bougeault et al., 2010, p.1071)

Probabilistic space weather forecasting based on a numerical model or other probabilistic techniques has been applied in several initiatives (see examples in Murray, 2018). On the other hand, while researchers have focused on the physical characteristics of extreme space weather events or the effects on the GNSS/power grids (Klatt, 2016; Ngwira and Pulkkinen, 2016), there is almost no research on the links between those impacts and decision behavior under uncertainty from the end-user's perspective. It is surprising that, so far, this real-world decision problem has received hardly any attention in scientific/technical papers. Nevertheless, this gap is a good opportunity for interdisciplinary research.

It should be noted that there has been a lot of progress by space weather researchers using probabilistic forecasts for uncertainty estimation in extreme events. However, following atmospheric science's example (Uccellini, 2016; Alley et al., 2019) the space weather community should apply decision analysis approaches, such as behavioral or risk perception. The important point here is not only to gain a better understanding of the physics of solar events, but also how stakeholders interpret and use probabilistic space weather forecasts and early warning messages. Henceforth, we could develop an innovative set of products, then, for better risk communications and a shift toward action-based decision support and early warning services. As a best practice, it is widely recognized that customized Early Warning Systems (EWS) are an excellent option, enabling advance implementation to select mitigation actions.

Further research will encompass the relationship between natural hazards and decision science. Although, these insights identify several subjects to develop innovative and customized decision support and early warning systems for CI protection (Figure 8).

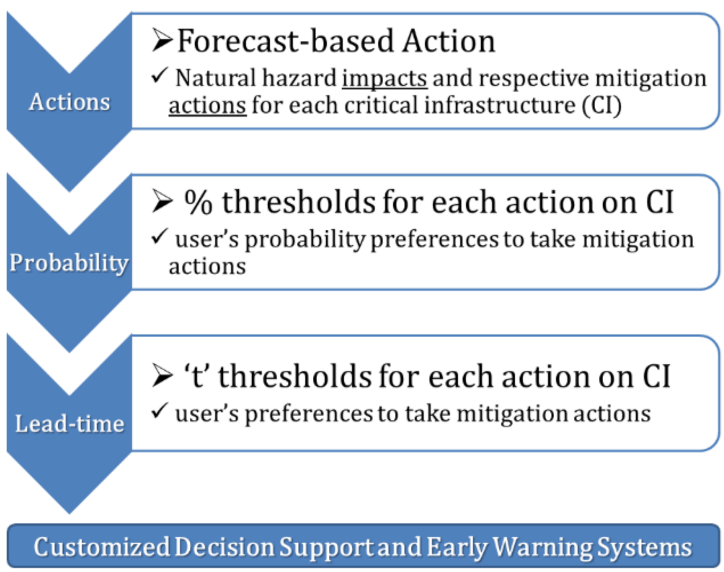

Figure 8: Flow chart for customized decision support and early warning systems based on user`s preferences about impacts, probability, and lead-time in natural hazard prediction.

III. Practical Application For Space Weather Hazards

By way of demonstration, we put together a simple application for an orbital maneuver of a Satellite in Geostationary Orbit (GEO) under emergency conditions. The GEO operator receives two independent early warnings at the same time: a) space debris proximity in the next 48 hours, and b) potential extreme geomagnetic storm. So, the decision problem (see details in Figure 9) is selecting one of two alternatives:

1) perform the orbital maneuver as planned in the procedure
2) postpone the orbital maneuver for 24 hours to avoid telecommand signal failures to the satellite

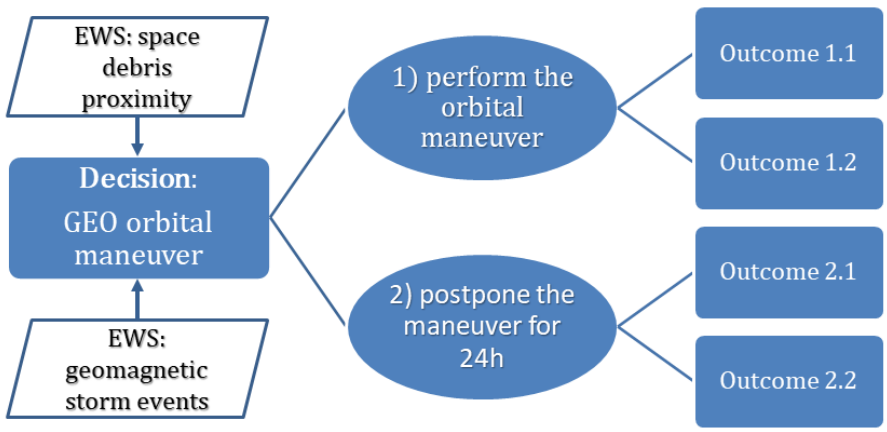

Figure 9: Traditional decision analysis with simplified decision-tree based on Early Warning Systems (EWS) for space debris proximity and geomagnetic storm event information.

Naturally, various criteria should be assessed in the satellite operation, but as a hypothetical application we used the scenarios in Figure 5 as a probabilistic space weather prediction:

- Scenario A: high probability (above 70%) and short lead-time (below 10h)
- Scenario B: lower probability (below 10%) or long lead-time (after 24h)

The final decision is related to two hazard impacts: debris; and a geomagnetic storm. In traditional decision analysis, the best outcome is the highest expected value (for details, see Clemen, 1997). However, equally important, the decision is based on stakeholder preference profile, that is, their trade-offs between probability and lead-time. These characteristics are consistent with several studies in the literature (Wachinger et al., 2013; Kox et al., 2015; Caruzzo et al., 2018). For example, in Scenario B, the satellite manager can continue the maneuver schedule because of the low likelihood forecasts or longer lead-time (alternative 1 on Figure 9). On the other hand, with Scenario A, the manager could decide to postpone the action (alternative 2 on Figure 9). In fact, Park et al. (2017) point out in a solar flare forecast, the decision makers may tend to choose a larger probability threshold when cost becomes relatively higher. These conditions suggest the existence of motivational risk-decision-making biases related to probabilistic natural hazard forecast issues and should affect decisions related to space weather and CI protection as well.

IV. Summary and Directions For Future Research

This article has discussed some aspects for interdisciplinary research into natural hazard decision problems in real-world situations. Improving early decision using a probabilistic forecast is a grand challenge all over the world. It is our understanding, then, that an interdisciplinary research design provides what stakeholders think about all aspects of the decision problem. The potential application of this innovative research could bring about a paradigm shift in natural hazard-related decisions. That is, selection of mitigating action alternatives no longer depends only on ‘impacts table’ or ‘risk matrix,’ but also on end-users’ preferences about the trade-offs between probability and lead-time.

From a space weather hazard perspective, the new Solar Cycle (number 25) will start in the next two years, and the Solar maximum of sunspots is expected in 2025 (Pesnell and Schatten, 2018). It is important to note that space weather centers around the world have been developing numerous products that provide general information about solar activities. In spite of their usefulness, however, it is possible to advocate that space weather-hazard impacts alone for critical infrastructure protection is not at all recommendable or able to support a good decision-making choice. In other words, a single criterion approach centered on ‘impact only’ is no longer supportive and robust enough in contemporary decision problem evaluation.

Though all of these advances are relatively recent in other operational communities (e.g., hydro-meteorology), it is widely accepted that this issue requires an interdisciplinary research approach, applying the up-to-date techniques from space science (observations and forecast) and robust methods from decision sciences. Nevertheless, to reduce economic impacts associated with space weather threat prediction, it is essential that CI has an effective operational mitigation plan. Based on the insights, we believe this research design could provide a step toward new procedures and protocols for space weather-risk assessment.

As a final comment, it is interesting to notice that in the upcoming decade, space weather will become more and more relevant. Today, we are more vulnerable to space weather hazards than in the past, and in the future, our modern, technological society is going to be more vulnerable than it is today. To address this challenge, researchers at the Department of Atmospheric and Oceanic Sciences at McGill University are currently undertaking interdisciplinary research in which the various dimensions of natural hazards are used to develop new approaches and risk communications to support better decisions using experience from other cutting-edge research in the literature, through a multi-methodological and innovative scientific-technological approach.

Acknowledgments

The authors are grateful to the Editor Dr. Robyn Fiori for supporting the research. The first author was supported by FAPESP (Sao Paulo Research Foundation), under grant nº 2017/25767-3. However, any opinions, suggestions or conclusions in this article are those of the authors and do not necessarily reflect the views of the FAPESP.

About the Authors

Amaury Caruzzo *is a Postdoctoral Researcher at the Department of Atmospheric and Oceanic Sciences at McGill University. Dr. Caruzzo received his B.Sc. (Atmospheric Science) at the University of Sao Paulo and Ph.D (Aeronautical Engineering) at the Aeronautics Institute of Technology (ITA, Brazil). His research interests include Atmospheric/Space Science and Operations Research with an emphasis on natural hazards, critical infrastructure protection, risk analysis, and decision under uncertainty.*

John Gyakum *is a Full Professor and Chair of the Department of Atmospheric and Oceanic Sciences at McGill University. Dr. Gyakum received his B.Sc. (Atmospheric Science) at The Pennsylvania State University and Ph.D. at the Massachusetts Institute of Technology (MIT). His research interests include synoptic and dynamic meteorology and natural disasters.*

References

Alley, R. B., Emanuel, K. A., & Zhang, F. (2019). Advances in weather prediction. *Science*, *363*(6425), 342–344. https://doi.org/10.1126/science.aav7274

Balch, C. C. (2015). Space Weather Forecasting for the Electrical Power Grid. *Infrastructure Resilience Risk Reporter*, *1*(4), 21–34. Retrieved from http://carleton.ca/irrg/wp-content/uploads/Vol-1-Issue-4-IRRG-Journal-FINAL-FINAL.pdf

Boteler, D. H. (2018). Dealing with Space Weather: The Canadian experience. In N. Buzulukova (Ed.), *Extreme Events in Geospace* (1st ed., pp. 635–656). Elsevier. https://doi.org/10.1016/B978-0-12-812700-1.00026-1

Bougeault, P., Toth, Z., Bishop, C., Brown, B., Burridge, D., Chen, D. H., … Worley, S. (2010). The THORPEX Interactive Grand Global Ensemble. *B Am Meteorol Soc*, *91*(8), 1059–1072. https://doi.org/10.1175/2010BAMS2853.1

Canada, G. of. (2009). *National Strategy for Critical Infrastructure*. Ottawa. Retrieved from https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/index-en.aspx

Cannon, P. (2013). *Extreme space weather: impacts on engineered systems and infrastructures*. *Royal Academy of Engineering*. London. Retrieved from http://www.raeng.org.uk/news/publications/list/reports/Space_Weather_Full_Report_Final.PDF

Caruzzo, A., Belderrain, M. C. N., Fisch, G., & Manso, D. F. (2015). Mapping of the aerospace meteorology in the Brazilian Space Program: challenges and opportunities to rocket launch. *J. Aerosp. Technol. Manag.*, *7*(1), 7–18. https://doi.org/10.5028/jatm.v7i1.461

Caruzzo, A., Belderrain, M. C. N., Fisch, G., Young, G. S., Hanlon, C. J., & Verlinde, J. (2018). Modelling weather risk preferences with Multi-Criteria Decision Analysis for an aerospace vehicle launch. *Meteorol Appl*, *25*(3), 456–465. https://doi.org/10.1002/met.1713

Clemen, R. T. (1997). *Making Hard Decisions: An Introduction to Decision Analysis* (2nd ed.). Boston: Duxbury Press.

Coughlan-de-Perez, E., Hurk, B. van den, Aalst, M. K. van, Jongman, B., Klose, T., & Suarez, P. (2015). Forecast-based financing: an approach for catalyzing humanitarian action based on extreme weather and climate forecasts. *Nat Hazard Earth Sys*, *15*, 895–904. https://doi.org/10.5194/nhess-15-895-2015

Eastwood, J. P., Biffis, E., Hapgood, M. A., Green, L., Bisi, M. M., Bentley, R. D., … Burnett, C. (2017). The Economic Impact of Space Weather: Where Do We Stand? *Risk Anal*, *37*(2), 206–218. https://doi.org/10.1111/risa.12765

Elvidge, S., & Angling, M. J. (2018). Using Extreme Value Theory for Determining the Probability of Carrington-Like Solar Flares. *Space Weather*, *16*(4), 417–421. https://doi.org/10.1002/2017SW001727

FAO, Food and Agriculture Organization. (2018). *Impact of Early Warning Early Action*. Rome. Retrieved from http://www.fao.org/emergencies/fao-in-action/ewea/en/

Ferguson, D. C., Worden, S. P., & Hastings, D. E. (2015). The Space Weather Threat to Situational Awareness, Communications, and Positioning Systems. *IEEE T Plasma Sci*, *43*(9), 3086–3098. https://doi.org/10.1109/TPS.2015.2412775

Fiori, R. A. D., Boteler, D. H., Trichtchenko, L., Nikolic, L., Lam, H.-L., Danskin, D., & McKee, L. (2015). An Overview of Space Weather and Potential Impacts on Power Systems - A Canadian Perspective. *Infrastructure Resilience Risk Reporter*, *1*(3), 18–25. Retrieved from http://carleton.ca/irrg/wp-content/uploads/Vol-1-Issue-3-Final.pdf

Fiori, R. A. D., Koustov, A. V., Chakraborty, S., Ruohoniemi, J. M., Danskin, D. W., Boteler, D. H., & Shepherd, S. G. (2018). Examining the Potential of the Super Dual Auroral Radar Network for Monitoring the Space Weather Impact of Solar X-Ray Flares. *Space Weather*, *16*(9), 1348–1362. https://doi.org/10.1029/2018SW001905

Gaetano, F., Oliva, G., Panzieri, S., Romani, C., & Setola, R. (2013). Analysis of Severe Space Weather on Critical Infrastructures. In *Critical Information Infrastructures Security* (pp. 62–73). Switzerland: Springer. https://doi.org/10.1007/978-3-319-03964-0_6

Hardy, R. D. (2019). A Sharing Meanings Approach for Interdisciplinary Hazards Research. *Risk Anal*, in press. https://doi.org/10.1111/risa.13216

Henley, E. M., & Pope, E. C. D. (2017). Cost-Loss Analysis of Ensemble Solar Wind Forecasting: Space Weather Use of Terrestrial Weather Tools. *Space Weather*, *15*(12), 1562–1566. https://doi.org/10.1002/2017SW001758

Klatt, C. (2016). Precise Timing from Global Navigation Satellite Systems and Implications for Critical Infrastructure. *Infrastructure Resilience Risk Reporter*, *1*(5), 3–9. Retrieved from https://carleton.ca/irrg/wp-content/uploads/VOL-1-ISSUE-5-FINAL-IRRG-Journal.pdf

Kox, T., Gerhold, L., & Ulbrich, U. (2015). Perception and use of uncertainty in severe weather warnings by emergency services in Germany. *Atmos Res*, *158–159*, 292–301. https://doi.org/10.1016/j.atmosres.2014.02.024

Krausmann, E., Andersson, E., Gibbs, M., & Murtagh, W. (2016). *Space Weather and Critical Infrastructures: Findings and Outlook*. Ispra, Italy. https://doi.org/10.2788/152877

Lam, H.-L. (2016). The Genesis and Development of Space Weather Forecast in Canada. *Infrastructure Resilience Risk Reporter*, *1*(5), 10–25. Retrieved from https://carleton.ca/irrg/wp-content/uploads/VOL-1-ISSUE-5-FINAL-IRRG-Journal.pdf

MacAlester, M. H., & Murtagh, W. (2014). Extreme Space Weather Impact: An Emergency Management Perspective. *Space Weather*, *12*(8), 530–537. https://doi.org/10.1002/2014SW001095

Murray, S. A. (2018). The Importance of Ensemble Techniques for Operational Space Weather Forecasting Special Section. *Space Weather*, *16*(7), 777–783. https://doi.org/10.1029/2018SW001861

Ngwira, C. M., & Pulkkinen, A. (2016). Understanding and Defining Extreme Space Weather. *Infrastructure Resilience Risk Reporter*, *1*(5), 26–33. Retrieved from https://carleton.ca/irrg/wp-content/uploads/VOL-1-ISSUE-5-FINAL-IRRG-Journal.pdf

Ngwira, C. M., Pulkkinen, A., Mays, M. L., Kuznetsova, M. M., Galvin, A. B., Simunac, K., … Glocer, A. (2013). Simulation of the 23 July 2012 extreme space weather event: What if this extremely rare CME was Earth directed? *Space Weather*, *11*(12), 671–679. https://doi.org/10.1002/2013SW000990

Nikitina, L., Trichtchenko, L., & Boteler, D. H. (2016). Assessment of extreme values in geomagnetic and geoelectric field variations for Canada. *Space Weather*, *14*(7), 481–494. https://doi.org/10.1002/2016SW001386

North, D. W. (2017). Space Weather: Introducing a Survey Paper and a Recent Executive Order. *Risk Anal*, *37*(2), 204–205. https://doi.org/10.1111/risa.12778

Odenwald, S., Green, J., & Taylor, W. (2006). Forecasting the impact of an 1859-calibre superstorm on satellite resources. *Adv Space Res*, *38*(2), 280–297. https://doi.org/10.1016/j.asr.2005.10.046

Oughton, E. J., Hapgood, M., Richardson, G. S., Beggan, C. D., Thomson, A. W. P., Gibbs, M. Horne, R. B. (2019). A Risk Assessment Framework for the Socioeconomic Impacts of Electricity Transmission Infrastructure Failure Due to Space Weather: An Application to the United Kingdom. *Risk Anal*, in press. https://doi.org/10.1111/risa.13229

Park, J., Moon, Y. J., Choi, S., Baek, J. H., Cho, K. S., & Lee, K. (2017). Application of decision-making to a solar flare forecast in the cost-loss ratio situation. *Space Weather*, *15*(5), 704–712. https://doi.org/10.1002/2016SW001532

Pesnell, W. D., & Schatten, K. H. (2018). An Early Prediction of the Amplitude of Solar Cycle 25. *Solar Physics*, *293*(7), 1–10. https://doi.org/10.1007/s11207-018-1330-5

Quigley, K., Bisset, B., & Mills, B. (2017). *Too Critical to Fail: How Canada Manages Threats to Critical Infrastructure* (1st ed.). Montreal: McGill-Queen’s University Press.

Ribeiro, J. R., Pelicioni, L. C., Caldas, I., Netto Lahoz, C. H., & Belderrain, M. C. N. (2018). Evolution of policies and technologies for space debris mitigation based on bibliometric and patent analyses. *Space Policy*, *44*, 40–55. https://doi.org/10.1016/j.spacepol.2018.03.005

Uccellini, L. W. (2016). Restructuring the National Weather Service. *Public Admin Rev*, *76*(9), 842–843. https://doi.org/10.1111/puar.12633

Wachinger, G., Renn, O., Begg, C., & Kuhlicke, C. (2013). The risk perception paradox - implications for governance and communication of natural hazards. *Risk Anal*, *33*(6), 1049–1065. https://doi.org/10.1111/j.1539-6924.2012.01942.x

Wasson, R. J. (2018). Zaps and Taps: Solar Storms, Electricity and Water Supply Disasters, and Governance. In M. A. Miller, M. Douglass, & M. Garschagen (Eds.), *Crossing Borders* (1st ed., pp. 261–277). Singapore: Springer. https://doi.org/10.1007/978-981-10-6126-4

WEF, World Economic Forum. (2019). *The Global Risks Report 2019*. Geneva. Retrieved from www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf

Weigel, R. S., Detman, T., Rigler, E. J., & Baker, D. N. (2006). Decision theory and the analysis of rare event space weather forecasts. *Space Weather*, *4*(5), 1–8. https://doi.org/10.1029/2005SW000157

Wilks, D. S. (2011). *Statistical Methods in the Atmospheric Sciences* (3rd ed.). New York: Academic Press. Retrieved from http://www.sciencedirect.com/science/bookseries/00746142/100/

Wong-Parodi, G., & Small, M. J. (2019). A Decision-Centered Method to Evaluate Natural Hazards Decision Aids by Interdisciplinary Research Teams. *Risk Anal*, in press. https://doi.org/10.1111/risa.13261

Ionospheric Detection of Explosive Events

*C.Y. Huang**
*J.F. Helmboldf**
*J. Park**
*T.R. Pedersen**
*R. Willemann**
Air Force Research Laboratory, Space Vehicles Directorate, Kirtland AFB, New Mexico, USA
Naval Research Laboratory, Washington, DC
Oregon State University, Corvallis, Oregon, USA

Abstract

The ionospheric response to explosive or impulsive events that occur at or below the Earth's surface has been noted since the first detonations of nuclear devices during the early period of above-ground testing. Acoustic Gravity Waves and Traveling Ionospheric Disturbances (TIDs) were detected in association with test explosions carried out by the USSR in Novaya Zemlya in 1961.

While research in this area has continued, the standards accepted by the Comprehensive Nuclear Test Ban Treaty for detection and confirmation of nuclear explosions have been based on (1) seismic; (2) hydroacoustic; (3) infrasound; and (4) radionuclide monitoring from ground detectors. We suggest that ionospheric sensing offers a complementary methodology which may allow for robust confirmation of explosive events.

One method of ionospheric monitoring of explosive events is analysis of Total Electron Content (TEC), available by processing data from Global Navigation Satellite System receivers distributed globally on land masses. TIDs observed by their signature in TEC have been used to detect and confirm mine collapses and blasts, earthquakes, volcanic eruptions, meteorite strikes, as well as underground nuclear tests. While an integrated measurement, like TEC, is not as sensitive to small-amplitude density perturbations as other methods, the existence of large networks of continuously operating GNSS stations make this an intriguing new monitoring asset.

I. INTRODUCTION

Above-ground nuclear explosions have been detected by ionospheric monitors since 1958, when nuclear tests were carried out on Johnston Island, southwest Hawaii. Disturbances, which propagated large distances and caused changes in ionospheric electron densities, were detected as far away as Brisbane, Australia. From times of arrival at Brisbane, the speeds of propagation of the disturbances were deduced to range from 200 m s1 to 840 m s1 approximately the sound speed at the altitude of the detonation.

During 1961, a series of Soviet above-ground nuclear tests were carried out at Novaya Zemlya and Semipalatinsk, Kazakhstan. Ionospheric disturbances were detected globally. The perturbations were attributed to atmospheric waves, in particular acoustic gravity waves (AGWs) [Hines, 1960], with wave periods of several minutes. As we discuss below, AGWs couple to the ionosphere and generate Traveling Ionospheric Disturbances (TIDs) which were detected in association with the tests near Hawaii and Novaya Zemlya [Hines, 1967; Breitling et al., 1967]. A study of variations in the electron density peak indicated propagation velocities between 50 and 900 m s1 corresponding to a mix of shock and acoustic waves.

There have been significant changes to nuclear testing and detection since these early days. Above-ground testing was banned in 1963 by the Limited Test Ban Treaty, leading to below-ground tests. A second change is a large increase in the number of ionospheric observations available on a regular basis. The main contributors to ionospheric electron density measurements are large networks of Global Navigation Satellite System (GNSS) stations, such as the freely available International GNSS Service (IGS) (http:www.igs.org/) [Dow et al., 2009]. From the Total Electron Content (TEC) derived from GNSS data, perturbations in electron density corresponding to TIDs can be extracted. This has been done successfully [Park et al., 2011; Yang et al., 2012] for the 2006 and 2009 Underground Nuclear Explosions (UNEs) carried out by North Korea.

The wide availability of GNSS data enables nearly continuous global monitoring of the ionosphere, and in principle, of explosive events. In addition to nuclear tests, other impulsive events (earthquakes, mining explosions, volcano eruptions) generate waves that couple to AGWs and TIDs. TIDs are also detected in the ionosphere for a large range of natural phenomena including high-latitude magnetic activity [Hocke and Schlegel, 1996; Hunsucker, 1982; Richmond, 1978], tropospheric forcing [Forbes, 1995], and tsunamis and other ocean surface waves [Meng et al., 2015].

Figure 1 illustrates the basic concept of ionospheric responses to natural and man-made explosive events, and possible methods for detection. The explosions and earthquakes are shown over the green land mass, and tsunamis in the ocean generated by earthquakes in the ocean at lower right. Explosive events generate seismic waves that propagate at the Earth's surface. These are illustrated as dark circles over land. In addition, surface waves due to impulsive events give rise to shock and acoustic waves shown as light concentric circles propagating upwards through the lower atmosphere. When these waves intersect with the ionosphere, gravity and acoustic waves generate TIDs illustrated as dark bands in the F-region of the ionosphere. TIDs create perturbations in GNSS observations, symbolized by yellow zigzags, which can be observed by receivers, sounders and radio telescope arrays on the ground. In addition, the effects of TIDs generated in the conjugate hemisphere can be detected remotely. These new technical means combined with increasing tensions between nuclear powers stimulated this review of current and future methodologies for detection of explosive events.

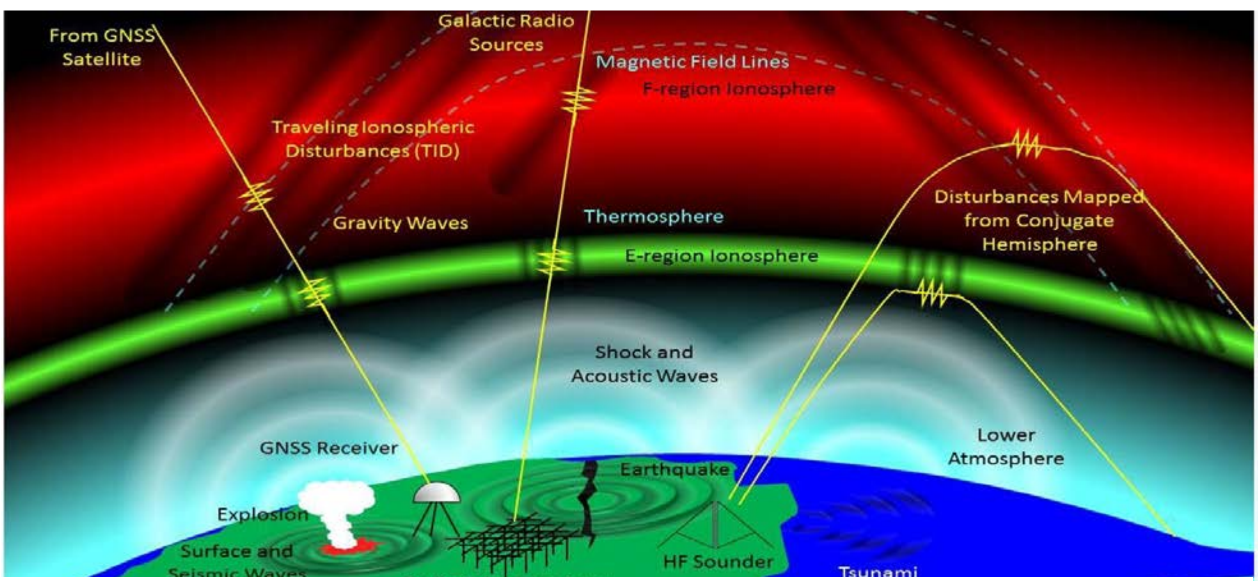

Figure 1: Schematic illustrating ionospheric response to natural and man-made explosive events.

Explosions on land are shown at bottom left, earthquakes at bottom center; tsunamis due to earthquakes are shown in the ocean at bottom right. The surface and seismic waves on land are shown as concentric dark circles over land. The tsunami waves are shown as dark ripples in the ocean. The disturbances generate shock and acoustic and gravity waves are illustrated as light circles propagating through the atmosphere. When the waves reach the ionosphere, they generate Traveling Ionosphere Disturbances (TIDs) shown as dark bands in the F-region of the ionosphere. These perturb signals from GNSS satellite and galactic radio sources. The perturbations, illustrated by yellow zigzags, can be detected on the ground by GNSS receivers, High Frequency sounders and radio telescopes. Remote detection of waves generated in the conjugate hemisphere can also be observed.

The Comprehensive Nuclear Test Ban Treaty

The Comprehensive Nuclear Test Ban Treaty (CTBT) was opened for signature in 1996 and was signed by 183 member states of the United Nations in September 2017. The CTBT is comprehensive both in the sense that it bans tests everywhere (in space, the atmosphere, oceans, and underground) - in the sense that it bans any test involving an uncontrolled nuclear chain reaction, down to zero yield [Dahlman et al., 2009].

The CTBT has not yet entered into force because several of the states have not yet ratified the Treaty. Nevertheless, the U.N. General Assembly authorized the CTBT Preparatory Commission (PrepComm) to organize a Provisional Technical Secretariat (PTS), which is funded by contributions from the CTBT States Signatory to build and operate a worldwide monitoring system.

On behalf of the PrepComm, the PTS is required by the CTBT to use equal diligence in monitoring all geographic regions of the world and only the technologies that are described in the CTBT. The PTS collects data from the International Monitoring System (IMS) and analyzes the data at its International Data Center (IDC) to determine the locations and sizes of the events that produced signals in the IMS data. The IDC prepares a "screened" list from which it excludes events that are almost certainly not nuclear tests, based on criteria prescribed in the CTBT and updated with the approval of the PrepComm. Despite the existence of screening criteria, the CTBT does not authorize either the PTS or the PrepComm to announce conclusions on the nature of any of the events that it detects [CTBTO, 2012].

The four monitoring technologies named in the CTBT and used by the PTS are seismic, infrasonic, hydroacoustic and radionuclide. Among these, only radionuclide data provide a "smoking gun" positively confirming that an event involved an uncontrolled nuclear chain reaction. The effectiveness of the IMS in detecting nuclear tests in different settings has been the topic of many studies and several comprehensive reviews [National Research Council, 2012].

The hydroacoustic component of the IMS is very likely to detect even the smallest possible nuclear explosion anywhere in the oceans. In addition, a nuclear test in the ocean would be detected by both the seismic and radionuclide components of the IMS, by monitoring systems operated by several states signatory to the CTBT.

The infrasonic component of the IMS has a threshold for detecting nuclear explosions in the atmosphere that varies geographically and seasonally with changes in stratospheric winds. Nevertheless, infrasonic monitoring is effective against realistic scenarios of nuclear testing in the atmosphere.

There is concern that an underground nuclear test could evade detection by the CTBTO because, at least in some geographic regions, the detection threshold of the IMS misses the smallest possible test. Even if an underground test is detected, IMS data may not be sufficient to distinguish a small test from other "confounding" seismic events, which include naturally occurring and induced earthquakes, and mining explosions. Among the confounding seismic events, naturally occurring earthquakes are by far the most numerous.

Atmospheric Effects

The reaction of the neutral atmosphere to nuclear explosions has been observed since the early days of above-ground testing. Analysis by Hines (1960) led to acceptance that the waves emitted by explosions are atmospheric gravity waves.

There are two classes of waves emanating from explosive events, predominantly gravitational or acoustic. The first class restricts wave propagation to the horizontal surface with no phase propagation in the vertical direction. These surface waves are excluded in this paper on the basis of wave observations showing vertical propagation. The second class of waves is described by Hines (1960) as "internal" acoustic waves. These are further divided by frequency into acoustic waves above the acoustic frequency, and gravity waves below the buoyancy frequency. Typical values for the acoustic and buoyancy frequencies are around 3.3 mHz and 2.9 mHz, respectively.

Internal atmospheric gravity waves increase in amplitude with upward propagation. Countering the amplification are damping effects due to energy dissipation, the effect of which is to remove higher frequency waves as they propagate upwards. Wave amplitudes reach a maximum value before being damped within a short altitude range that is frequency dependent.

Acoustic and gravity waves are further separated by their propagation characteristics. Acoustic waves (AWs) propagate isotropically outwards, while gravity waves (GWs) propagate primarily in the horizontal direction. There is a class of AWs which arises when the buoyancy force is comparable with the gravitational force, and the waves, while compressional, exhibit oblique propagation. These waves are described as Acoustic Gravity Waves (AGWs).

Different propagation characteristics of AWs and GWs allow us to distinguish between naturally occurring internal GWs, such as Traveling Atmospheric Disturbances (TADs) which typically propagate horizontally from high to low latitudes as a result of Joule heating, from AGWs generated by explosions which propagate obliquely outwards from the explosion site [Hines, 1967].

While the amount of energy radiated into the atmosphere is not large, there are few competing wave sources with compatible frequency and horizontal wavelength [Artru et al., 2004]. As earthquakes occur frequently and generate AGWs with similar characteristics as man-made explosions, attribution of observed waves is a critical aspect of remote detection which will be discussed in the section on Challenges.

As another trigger of AGWs, nuclear explosions have also been studied. Since nuclear testing in oceans, the atmosphere, or space was banned by the Limited Test Ban Treaty, testing has been carried out in underground cavities since this date. This method reduces the seismic signal by about two orders of magnitude relative to atmospheric testing [Latter et al., 1961; Herbst et al., 1961]. Distinguishing between waves generated by explosions and those triggered by earthquakes became a topic of much discussion [Argo et al., 1995].

As mentioned, AWs grow in amplitude with upward propagation to the lower ionosphere [Hines, 1960]. This factor, combined with the high percentage of upward wave energy, suggests that it is plausible to monitor wave emissions from explosions remotely. To first approximation, acoustic waves amplify as they propagate vertically. In a realistic atmosphere, effects such as a non-isothermal atmosphere, background neutral winds, viscosity, ion drag and heat conduction complicate calculation of wave amplitudes [Yeh and Liu, 1974]. Model calculations indicate a peak in acoustic wave velocity at altitudes over 100 km [Drobzheva and Krasnov, 2003]. At these altitudes, coupling to ions can generate Traveling Ionospheric Disturbances (TIDs) which are the ionospheric manifestation of AGWs originating at the Earth's surface.

Ionospheric Effects

TIDs can be generated by GWs, AGWs, or AWs by different mechanisms. They are classified into large-scale TID (LSTID), medium-scale TID (MSTID), and small-scale TID (SSTID), solely based on the velocity, duration, and the wavelength regardless of their generation mechanism.

The horizontal velocities of the LSTID, MSTIC and SSTID are 400 – 1000 m s^{1} and lower than 200 m s^{1}, respectively, and the durations, or wave periods, are 30 minutes – 3 hours, 12 minutes – 1 hour, and few minutes, respectively, and the wavelengths of LSTID, MSTID and SSTID are greater than 1000km, 100 – 1000km, and 10 – 100 km, respectively [Rieger and Leitinger, 2002]. Among the different types of waves, GW and AGW tend to generate LSTIDs or MSTIDs while AW generates relatively smaller scales of MSTIDs or SSTIDs.

II. TRAVELING IONOSPHERIC DISTURBANCES INDUCED BY NATURE

In this section, we briefly introduce several specific types of natural and man-made events in a different range of altitudes from underground, near surface, up to the atmosphere.

Geomagnetic storms are one of the common geophysical events known to generate perturbations in the ionosphere, typically LSTIDs. Richmond (1978) concluded that the most likely source of high-latitude gravity waves is Joule heating. Ho et al. (1998) observed two long lasting geomagnetic storms in 1993 and 1994 using a global network of GPS receivers. In both events, the 1EC enhancement occurred within 1 hour of each event, and large-scale ionospheric structures were identified. From the event in 1994, the clear signature of a TID with a propagation velocity of up to 460 m s-1 was detected.

Unlike geomagnetic storms, other natural and artificial events induce smaller scale TIDs, either MSTIDs or SSTIDs. Yuen et al (1969) examined seismic, atmospheric, and ionospheric data after the Hachinohe earthquake in 1968. During Rayleigh wave propagation along the Earth's surface with the velocity of about 3.5 km s1 upward traveling acoustic waves are produced that cause disturbances in the atmosphere up to heights of at least 300 km [Yuen et al, 1969]. The acoustic waves are Shock Acoustic Waves (SAWs) that propagate upward from the focal area in narrow cone of zenith angles with the sound speed at the corresponding altitudes. The sound speed of upward propagation depends on altitude and range from about 250 m s1 near the surface to 800 m s1 at 300 km altitudes. During upward propagation, the SAW is amplified exponentially due to the decrease of atmospheric density before interacting with the ionospheric plasma.

Tsunamis are another trigger of TIDs. Unlike the vertical propagation speed of the AW, which is of the order of 300 – 1,000 m s -1, the GW induced from a tsunami in the ocean propagates obliquely upward with a vertical velocity of about 50 m s-1 and takes a few hours for the wave to reach the ionosphere [Artru et al., 2005]. In the ionosphere, the AW generated by the tsunami wave generates TIDs, which then propagate horizontally with a velocity of the order of about 200 m s·'-2 TID from explosive events.

Ionospheric disturbances generated by impulsive events near the surface or at low altitudes have been observed from volcanic eruptions and nuclear detonations. TIDs of several volcanic eruptions were studied using data from ionospheric sensors and GNSS receiver networks.

Roberts et al. (1982) detected TIDs induced by the explosion from the volcanic eruption of Mt. Helens in May 18, 1980, at 1EC monitoring stations at ranges of less than 2000 km and up to 4950 km in range. The authors claimed that the TIDs from this volcanic eruption were induced by a gravity wave excited by the explosive activity. Several studies investigated the ionospheric signatures released from a series of strong eruptions at Mount Pinatubo in 1991, Lgarashi et al.

(1994) observed the TIDs from this event at five ionospheric sounding stations in Japan. More recent studies, waves released from volcanic eruptions have been interpreted as acoustic waves based on the detected propagation speed.

TIDs are also generated by artificial events, such as nuclear explosions at tropospheric altitudes, the lower atmosphere, near the surface, and underground. The ionospheric responses due to atmospheric nuclear explosions have also been studied since the 1960's. Barry et al. (1966) applied linear acoustic theory to predict the ionospheric signature from a ground-level explosion. The prediction model was confirmed by the experimental results of 500-ton explosion in disturbance onset time, shape, and duration [Barry et al., 1966].

Since the Partial Test Ban Treaty (PTBT) was opened for signature in 1963, atmospheric nuclear tests have been significantly reduced while more underground nuclear explosions (UNEs) have been carried out. As a source of acoustic fluctuations driving the magnetosphere and ionosphere [Mikhailov et al., 2000], UNEs and corresponding TIDs have been investigated for several decades. Assuming hemispherical upward propagation of acoustic waves, Rudenko and Uralov (1995) calculated the ionospheric effects from the acoustic radiation of a UNE and determined a relationship between the UNE parameters (depth, explosion yield, and mechanical property of the rock) and the vertical displacement of the ionosphere, which is produced by the shock wave above the blast site.

The UNE-generated TID was observed from GNSS-based TEC shown in [Park et al., 2011; Yang et al., 2012]. Unlike naturally occurring TIDs, the event-related TIDs can be identified based on the characteristics of the TIDs; such as the arrival time of the waves, the period, amplitude, etc. Park et al. (2011) detected the spatial signature of a TID induced by 2009 North Korean UNE by processing OPS data observed at multiple Continuously Operating Reference Stations (CORS) in South Korea, Japan, China, and Russia as shown in Figure 2 taken from Figure 2 in Park et al., 2011.

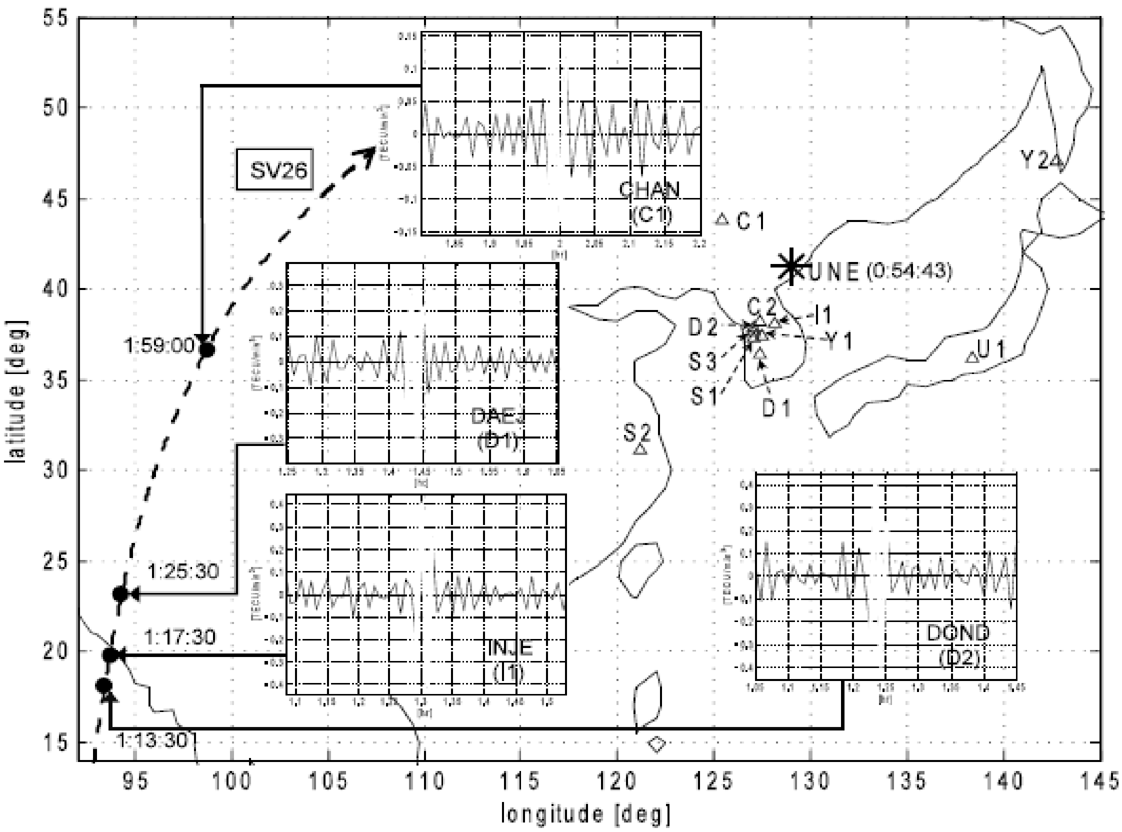

Figure 2: The locations of the underground nuclear explosion (UNE) and GNSS stations Cl

(CHAN), C2 (CHLW), DI (DAEJ), D2 (DOND),11 (INJE), Sl (SUWN), S2 (SHAO), S3 (SOUL), Ul (USUD), YI (YANP), Y2 (YSSK) on the coastline map around Korea, China, and Japan. The grey-shaded signals highlight examples of the detected TID's Slant TEC (STEC) numerical third order 3-point derivatives for stations Cl, Dl, D2, 11. The bold dashed line gives the ground track for satellite PRN 26 with dots that indicate the arrival times of the TIDs at their IPPs. All time labels in the figure are in UTC. (taken from Figure 2 in Park et al., 2011).

III. Discrimination of TIDs Between Explosive Events and Other Sources

Numerous studies have investigated TIDs generated from various sources at different regions. These studies support the fact that TIDs can be identified with respect to the causative mechanisms/sources. This section introduces efforts to discriminate the TIDs induced by explosive events from the TIDs of other sources.

Roberts et al. (1982) compared the TIDs from volcanic eruptions with large-scale explosions based on the findings reported in the literature. The authors distinguished the characteristics of TIDs from different sources in terms of propagation velocity. The characteristics of volcano eruptions were compared to other literature, and it was concluded this type of event generated large acoustic perturbations with periods of 4-5 minutes and propagation speed of 300 m s^{-1}. The TIDs induced from 1-13 megaton explosions propagated at roughly uniform speeds of 630 m s·1 and 770 m s-1 while the TIDs from the Mount St. Helens' volcanic eruptions propagated with an average velocity of 355 m s·1 up to 550 m s^{1}.

Another approach for discriminating the TIDs from a particular event is to analyze the wave property of them. Garrison et al. (2007) and Park et al. (2011) applied cross-correlation analysis to the TID candidate waveforms considering the similarity between the ionospheric disturbances released from one source event and recorded at multiple stations. Garrison et al. (2007) generated a TEC time series from GPS data collected at 175 stations. By computing the cross-correlation between the filtered time series, a coherent disturbance was identified. Park et al. (2011) also focused on the correlation between the TID candidates to identify TIDs from multiple candidate waveforms by applying cross-correlation techniques. Using one distinctive signature as a reference TID, the correlation coefficients (CC) were computed in the filtered TEC time series from other GNSS stations that enabled semi-automatic processing.

Innovative Techniques

1. Passive High-Frequency *Nery* High Frequency (HFNHF) Sounding

While the GNSS analysis techniques described above create the possibility of a new global ionospheric monitoring scheme, the fact that they rely on integrated TEC measurements is problematic for monitoring far from the site of a low-altitude/surface explosion. While infrasound waves can be ducted around the world, the top of this duct is at approximately 120 km altitude, squarely within the E-region. Integrated TEC measurements are much more sensitive to fluctuations within the F-region where the bulk of the ions reside. Thus, a very "quiet" F-region is required for GNSS-based detections of E-region disturbances.

Because of this, monitoring the bottom-side ionosphere via HF sounding may be a more ideal approach. However, there is no network of HF sounders with anywhere close to the global coverage of continuously operating GNSS receivers. This is largely due to the relatively inexpensive nature of GNSS receiver stations compared to HF sounding/radar systems. The cost difference derives from the fact that the transmitters for GNSS receivers are free to the users, that is, the GNSS satellites are transmitters of opportunity (ToO), and a GNSS receiver system has a much smaller physical footprint. However, several investigators have shown the utility of HF*IMF* systems that use terrestrial ToOs to sound the ionosphere and characterize disturbances (e.g., Helmboldt et al., 2013). These methods, coupled with new, relatively low-cost, electrically short antenna technology enable portable/re-locatable monitoring systems.

Because MF systems are still broadcasting all over the world (e.g., AM radio), and HF systems are often still used for timing (e.g., WWV in the United States; BPM in China), a relatively low-cost worldwide network of HF*IMF* receivers could be fielded specifically to target the bottom-side ionosphere and act as a supplement to any GNSS-based system.

Because the top of the thermosphere infrasound duct is at -110-120 km altitude, such HF systems could sound regions of the bottom-side ionosphere that are hundreds of kilometers away from any potential sites of interest and watch for the impact of ducted infrasound waves.

Additionally, since many high-power HF/MF ToOs support ionospheric propagation over distances of thousands of kilometers, the receiver systems could likewise be thousands of kilometers from the ionospheric regions to be monitored. Thus, a relatively low-density network of such receivers could be employed worldwide and enable monitoring over denied regions, such as the middle of the Pacific Ocean.

In addition to human-made ToOs, the sky is also populated with naturally occurring radio sources; such as supernova remnants, active galactic nuclei, quasars, and radio galaxies. Many such sources have radio-frequency spectra that increase rapidly with lower frequency, making them useful *HFNHF* beacons. The signals from such sources are very noise-like, therefore cannot be used as beacons in the same way as OPS signals. However, if multiple high-gain antennas are pointed toward the same cosmic radio source, cross-correlating the signals between each pair of antennas yields a very strongly peaked signal at a predictable time difference of arrival (TDOA). Gradients in TEC between two antennas' lines of sight cause this TDOA to be slightly off from the predicted value, making the phase of the cross-correlation quite sensitive to the local TEC gradient.

This cross-correlation of cosmic radio signals is the basis of modem radio frequency (RF) interferometry. For many decades, ionospheric fluctuations were the main limiting factor to the size of HF*NHF* interferometers, which in turn severely limited their angular resolution.

However, innovative techniques developed in the 1980’s and 90’s broke this ionospheric barrier, allowing for a renaissance for low-frequency RF interferometry. Consequently, new interferometers operating in the HF and VHF regimes have been and are being developed, including the low-band system on the Karl G. Jansky Very Large Array (VLA) in New Mexico, the Low Frequency Array (LOFAR) in the Netherlands / Europe, Murchison Widefield Array (MWA) in Australia, Long Wavelength Array (LWA) in New Mexico and California, and Low Frequency Aperture Array (LFAA) of the Square Kilometer Array (SKA) in Australia.

It was recognized early on that the ionospheric calibration methods that make high angular resolution synthesis imaging possible could also be used as high-precision probes of ionospheric structure. In particular, interferometers, like the VLA that also operate at higher frequencies, require extremely stable, atomic clock-based timing systems that allow for very precise measurements of fluctuations in baseline phases.

With the development of methods to monitor several (-20-50) moderately bright sources over the relatively wide 74 MHz field of view of the VLA, Cohen and Rottgering (2009) and Helmboldt et al. (2012) were able to perform larger-scale studies of both wavelike and turbulent ionospheric fluctuations. The key is not only the high precision of the measurements, but also the fact that interferometers are directly sensitive to the gradient in TEC rather than to absolute TEC.

Figure 3 shows examples of small-amplitude TEC gradient fluctuations following two separate explosion tests conducted at the Energetic Materials Research and Testing Center (EMRTC) near Socorro, NM. These were measured with the VLA using 340 MHz observations of the bright cosmic sources Cygnus A (10 March 2015) and Perseus A (25 July 2017) in the upper and lower panels, respectively. Cygnus A is significantly brighter than Perseus A, and it, therefore, enabled TEC gradient measurements with an order of magnitude better precision. In both cases, a significant disturbance is apparent 5-8 minutes after the blast after bandpass filtering the time series. In both cases, the arrival times are consistent with infrasound ray tracing calculations, illustrating the potential for this method to monitor for moderate-yield and/or well-buried explosions.

The advent of new technologies that use electrically short, active antennas makes re-locatable arrays for monitoring purposes much more feasible. While interferometers like the VLA that use large parabolic antennas are fixed to one location and extremely expensive to reproduce elsewhere, dipole-based phased arrays are more economical and re-locatable. Several arrays already utilize this technology in fixed configurations (LOFAR, MWA, LWA), and re-locatable systems based on these are being developed. A system designed specifically for ionospheric monitoring would also benefit from the fact that only the brightest cosmic sources need to be observed, which greatly reduces the required collecting area/number of antennas. Such a re-locatable system can be located a few hundred kilometers from the region of the ionosphere to be monitored, and requires a relatively large footprint (several antennas with baselines of -1km or more). Therefore, this type of platform may be better suited to targeted monitoring campaigns rather than a global monitoring network.

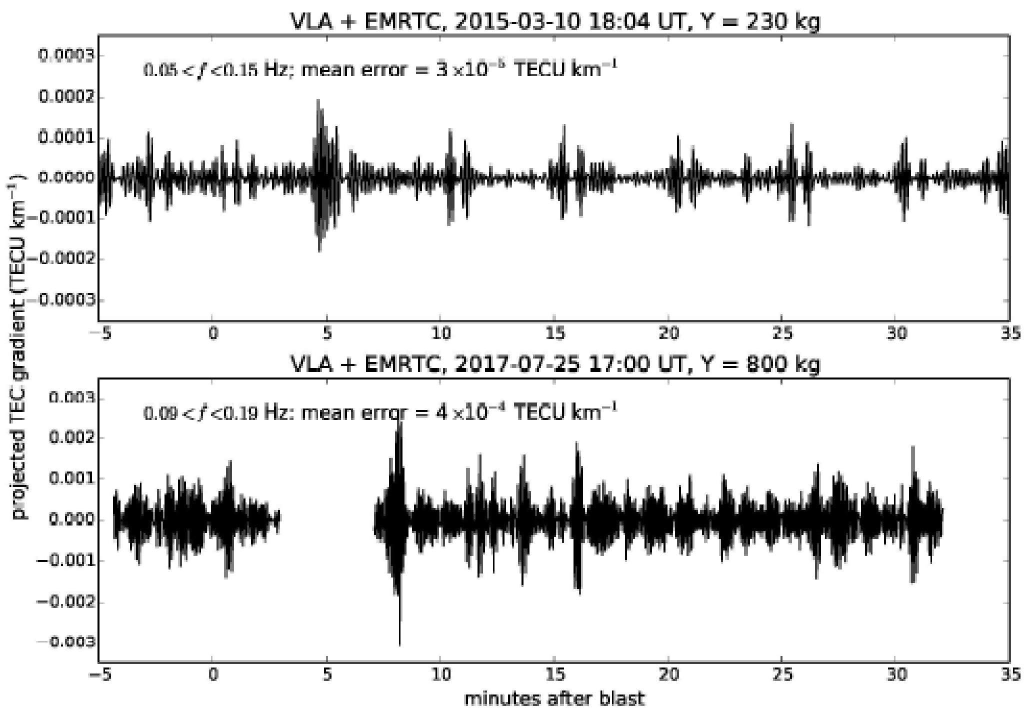

Figure 3: The 1EC gradient as a function of time relative to the detonation times for two EMRTC explosion tests.

The plots show the gradients projected along the vector pointing from the EMRTC site to the approximate ionospheric pierce point location. The date/time and yield of each event is given above each panel. In both cases, the time series were bandpass filtered to highlight the detected disturbances. The frequency ranges used for the bandpass filters are printed within each panel. The I-sigma uncertainties in TEC gradient are also given within each panel. The error in the time series within the upper panel is order of magnitude lower because a brighter source was observed (Cygnus A versus Perseus A).

2. Numerical Modeling

As shown in previous sections, TIDs are generated by a wide range of physical processes. In attempting to separate TIDs from impulsive events (detonations, earthquakes, rocket launches) which are generated by environmental processes (upward forcing from the troposphere, magnetic activity), models can play an important role.

While physics-based models of the ionospheric impacts of nuclear test explosions are generally not openly available, a number of models to specify and predict TIDs have been developed and published. These range from the empirical [Seker et al., 2009] and semi-empirical [Fedorenko et al., 2013] to physics-based [Shiokawa et al., 2005; Huba et al., 2015]. We will focus on models with particular relevance to TIDs from impulsive sources.

Models serve three major purposes in this area of research: (1) they can be used to confirm attribution of the sources of TIDs; (2) the combination of models and observations enables more accurate specification and forecast of ionospheric response; (3) accurate modeling can be used to specify potentially affected spatial regions when direct observations are absent.

In some versions of explosion simulations, the focus is placed on the generation of acoustic waves, treating the disturbance as pressure pulses that can be reduced to geometric rays. A variation of this ray-tracing approach is to combine empirical data with a physics-based model [Marchand and Berthelier, 2008] in order to explore the ionospheric response to the generation of acoustic modes by explosive events.

Meng et al. (2015) use a different physics-based model, the Global Ionosphere Thermosphere Model (GITM) [Ridley et al., 2006] to simulate the gravity waves generated by a tsunami, specifically the vertical displacement of the ocean surface that is modelled as a combination of sine waves. The actual tsunami wave field is presumably more complex, but may be treated as a linear superposition of the simple wave used as input in this simulation. The characteristics of the tsunami in the Pacific triggered by the Tohoku earthquake were used as input to the Wave Perturbation-GITM (WP-GITM) [Meng et al., 2015].

New numerical methods continue to advance the accuracy and extent of ionospheric modeling.

In the specific area of man-made impulsive events, modeling is still relatively untested, but tools developed to treat natural explosive phenomena may prove useful in extending the simulations to characterize and forecast the effect of man-made explosions on the ionosphere.

Challenges

As mentioned, TIDs are generated by a wide range of sources. The primary challenge to ionospheric monitoring of explosive events is reliable attribution of ionospheric perturbations. Upward forcing from the troposphere generates GWs and AGWs which are routinely observed in the ionosphere. These are detected under all conditions and have their own climatology. High-latitude TIDs are generated by magnetic activity. These are observed to propagate away from the high-latitude region. A wide spectrum of impulsive events (earthquakes, mining explosions, volcano eruptions) also generate TIDs. All of these sources of naturally occurring TIDs provide a background against which waves generated by explosive events must be extracted. In cases of small explosions, the signal to noise ratio is close to one, or even less than unity.

There has been little attempt to determine source characteristics or climatology of the wide range of TIDs. In particular, it is unclear if TIDs generated by explosions can be reliably separated from the high background of naturally occurring and man-made waves. We have described above the characteristics of ionospheric waves, which indicate that wave speeds, frequencies and spectral coherency analysis may provide a basis for wave attribution.

An initial effort to monitor TIDs from tsunamis using GNSS-based receivers has been described by Savastano et al., (2017). In the study, a wavelet analysis of the variations in TEC was carried out, and confirmation of tsunami-generated TIDs was made based on combination of observed wave speed and direction of propagation, combined with modeling. The authors conclude that real-time confirmation is probably not yet possible, but post-event confirmation can be done. Similar efforts to classify TIDs based on characteristic frequencies, wavelet coherence and propagation have not been attempted on any significant scale.

Summary

We have reviewed current understanding of the ionospheric response to impulsive events, both man-made and environmental. Currently this topic has high societal relevance because of potential violations of the CTBT which was established to ban all nuclear testing. The CTBT currently includes seismic, infrasonic, hydroacoustic and radionuclide monitoring. The addition of ionospheric monitoring could eliminate some false positives, thus enable more robust confirmation of explosive testing.

Earthquakes, volcano eruptions, tsunamis, bomb detonations, both above and below ground, all generate a wide range of acoustic waves which can be detected at varying distances from the source. Reliable detection of GWs, AWs and AGWs in the neutral atmosphere is complicated by the high background of these waves which occur routinely.

The ionospheric signatures of AWs and AGWs are TIDs which have been detected widely. A range of TIDs is generated, corresponding to the same events which launch AWs and AGWs in the atmosphere. A significant new aspect of TID monitoring is extraction of TID signatures via processing of 1EC from GNSS, a global network of satellites and ground receivers. As TIDs represent perturbations in 1EC, the absolute values of 1EC are not important, thus avoiding the difficulties in estimation of receiver bias. The methodology has been tested in a limited number of event studies, using GNSS receivers.

Innovative techniques have been introduced recently. RF interferometry measurements respond to gradients in 1EC, and not to the absolute values of TEC. This allows small 1EC variations to be resolved which have not been detectable by other methods, greatly expanding the possibility of detection of small underground explosions.

In addition to innovative measurement techniques, physics-based modeling of TIDs has advanced significantly. By coupling ionospheric models that represent transport of wave energy generated in the lower atmosphere, the entire system can be specified. Tiris allows more robust attribution of the observed waves. Use of sophisticated models can assist in interpretation of sparsely monitored signals in areas where detection is difficult.

About the Authors

Dr. Cheryl Huang *is a Technical Advisor for the Geo-space Environment Impacts and Applications Branch at the AFRL Space Vehicles Directorate. Her current research interests are ionosphere thermosphere coupling during magnetic activity. She earned her B.Sc. at the University of Cape Town and M.Sc. at Rhodes University, both in South Africa, and her Ph.D. at the University of Iowa. Prior to joining AFRL, she was a research scientist at the University of Iowa and Boston College.*

Dr. Joseph Helmboldt *has more than 10 years of experience in the fields of astronomy, astrophysics, and ionospheric remote sensing and is the ionosphere project scientist for the VLA Low-band Ionosphere and Transient Experiment (VLITE). His work at NRL has focused on low radio frequency interferometry and its application to astrophysics, ionospheric physics, and passive geo-location. He has extensive experience in developing algorithms for processing and interpreting data from several radio frequency interferometers, has led three NRL Base programs, a separate DTRA-funded effort, and has over 20 peer-reviewed first-author papers. He was also a recipient of a 2013 Dr. Delores M. Etter Top Scientist and Engineer of the Year Award.*

Dr. Jihye Park *is an Assistant Professor of Geomatics in the School of Civil and Construction Engineering at Oregon State University. She holds a M.S. and Ph.D. in Geodetic science and surveying at The Ohio State University and B.S. in Geoinformatics at the University of Seoul in South Korea. Her research interests include GNSS positioning and navigation, GNSS remote sensing, GNSS-Reflectometry and Geodesy.*

Todd Pedersen *grew up in the foothills of the Wasatch Mountains in Utah and attended Brigham Young University where he received a B.A. in Japanese. After working as a translator in Japan and the U.S., he enrolled in the Physics graduate program at Utah State University where he completed his Ph.D. in Space Physics in 1998. Since then, he has been employed at the Air Force Research Laboratory at Hanscom AFB, Massachusetts and relocated with that group to Kirtland AFB, New Mexico in 2011. He has extensive experience in measurements of the ionosphere and upper atmosphere, including active experiments with high-power RF transmitters and chemical releases. He is currently Chief of the Geo-Space Environment Impacts and Applications Branch at the AFRL Space Vehicles Directorate. He enjoys spending his free time outdoors in the scenic Southwest.*

Dr. Willemann *manages the Nuclear Explosion Monitoring Program at AFRL, which is focused on research to improve monitoring of underground nuclear explosions - primarily using seismology, but complemented by InSAR and other satellite geodetic data and imagery, as well as hydroacoustic and infrasonic data. Dr. Willemann was Director of Planning for the Incorporated Research Institutions for Seismology from 2005 through 2016, a university consortium that provides research support services to academic seismologists under cooperative agreements with the National Science Foundation. He was the Director of the International Seismological Centre from 1998 through 2003, where he modernized the system that provides the world's most completed catalog of earthquakes and associated seismic measurements. Prior to then, he was a senior scientist at the Center for Monitoring Research, which was the DOD facility that developed the prototype monitoring system that the U.S. delivered to the Provisional Technical Secretariat for the CTBT Organization. Dr. Willemann earned his Ph.D. in geophysics from Cornell University in 1986 and his B.Sc. in geomechanics from the University of Rochester in 1978.*

References

Argo, P., Clark, R. A., Douglas, A., Gupta, V., Hassard, J., Lewis, P. M., et al. (1995). The detection and recognition of underground nuclear explosions. *Surveys in Geophysics, 16(4),* 495-532. https://doi.org/10.1007 /BF00665683

Artru, J., Ducic, V., Kanamori, H., & Lognonne, P. (2005). Ionospheric detection of gravity waves induced by tsunamis. *Geophysical Journal International, 160(3),* 840-848. https://doi.org/10.1111/j .1365 246X.2005.02552.x

Artru, J., Farges, T., & Lognonne, P. (2004). Acoustic waves generated from seismic surface waves: Propagation properties determined from Doppler sounding observations and normal modelling. *Geophysical Journal, 158(3),* 1067-1077.https://doi.org/10.1111/j.1365246X.2004.02377.x

Barry, G. H., Griffiths, L. J., & Taenzer, J. C. (1966). HF radio measurements of high altitude acoustic waves from a ground level explosion. *Journal of Geophysical Research, 17,* 4173--4182. https://doi.org/10.1029/JZ071i017p04173

Breitling, W. J., Kupferman, R. A., & Gassmann, G. J. (1967). Traveling ionospheric disturbances associated with nuclear detonations. *Journal of Geophysical Research, 72,* 307-315. https://doi.org/10.1029/JZ072i001 p00307

Cohen, A. S., & Rtittgering, H. J. A. (2009). Probing fine scale ionosphere structure with the Very Large Array radio telescope. *Astronomy Journal, 138(2),* 439-447. https://doi.org/10.1088/0004 256/138/2/439

CTBTO (2012). Verification regime. Retrieved from https://www.ctbto.org/verification regime

Dahlman, 0., Mykkeltveit, S., & Haak, H. (2009). *Nuclear test ban: Converting political visions to reality.* Netherlands: Springer.

Dow, J. M., Neilan, R. E., & Rizos, C. (2009). The International GNSS Service in a changing landscape of Global Navigation Satellite Systems. *Journal of Geodesy, 83(3* 4), 191-198. https://doi.org/10.1007/s00190 008 0300 3

Drobzheva, Y. V., & Krasnov, V. M. (2003). The acoustic field in the atmosphere and ionosphere caused by a point explosion on the ground. *Journal of Atmospheric and Solar Terrestrial Physics,* 65(3), 369-377. https://doi.org/10.1016/S1364 6826(02)00141 4

Forbes, J. M. (1995). Tidal and planetary waves. In R. M. Johnson & T. L. Killeen (Eds.), *The upper mesosphere and lower thermosphere: A review of experiment and theory, Geophysical Monograph Series* (Vol. 87, pp. 67-87).Washington, DC: American Geophysical Union.

Garrison, J. L., Lee, S. C. G., Haase, J. S., & Calais, E. (2007). A method for detecting ionospheric disturbances and estimating their propagation speed and direction using a large GPS network. *Radio Science, 42,* RS6011. https://doi.org/10.1029/2007RS003657

Helmboldt, J. F., Clarke, T. E., Craig, J., Dowell, J. D., Ellingson, S. W., Hartman, H. M., et al. (2013). Passive all sky imaging radar in the HF regime with WWV and the first station of the Long Wavelength Array. *Radio Science, 48,* 491-512. https://doi.org/10.1002/ rds.20056

Helmboldt, J. F., Lazio, T. J. W., Intema, H. T., & Dymond, K. F. (2012). A new technique for spectral analysis of ionospheric TEC fluctuations observed with the Very Large Array VHF system: From QP echoes to MSTIDs. *Radio Science, 47,* RSOL02. https://doi.org/ 10.1029/2011RS004787

Herbst, R. F., Werth, G. C., & Springer, D. L. (1961). Use of large cavities to reduce seismic waves from underground explosions. *Journal of Geophysical Research, 66,* 959-978. https://doi.org/10.1029/JZ066i003p00959

Hines, C. 0. (1960). Internal atmospheric gravity waves at ionospheric heights. *Canadian Journal of Physics, 38(11),* 1441-1481. https://doi.org/10.l 139/p60 150

Hines, C. 0. (1967). On the nature of traveling ionospheric disturbances launched by low altitude nuclear explosions. *Journal of Geophysical Research, 72,* 1877-1882. https://doi.org/10.1029/JZ072i007p01877

Ho, C. M., Mannucci, A. J., Sparks, L., Pi, X., Lindqwister, U. J., Wilson, B. D., et al. (1998). Ionospheric total electron content perturbations monitored by the GPS global network during two Northern Hemisphere winter storms. *Journal of Geophysical Research, 103,* 26,409-26,420. https://doi.org/10.1029/98JA01 237

Hocke, K., & Schlegel, K. (1996). A review of atmospheric gravity waves and travelling ionospheric disturbances: 1982-1995. *Anna/es de Geophysique, 14(9),* 917-940. https://doi.org/10.1007/s00585 996 0917.6

Huba, J. D., Drob, D. P., Wu, T. W., & Makela, J. J. (2015). Modeling the ionospheric impact of tsunami driven waves with SAMI3: Conjugate effects. *Geophysical Research Letters, 42,* 5719-5726. https://doi.org/10.1002/2015GL064871

Hunsucker, R. D. (1982). Atmospheric gravity waves generated in the high latitude ionosphere: A review. *Reviews o/ Geophysics, 20,* 293-315. https://doi.org/10. 1029/RG020i002p00293

lgarashi, K., Kainuma, S., Nishimuta, I., Okamoto, S., Kuroiwa, H., Tanaka, T., & Ogawa, T. (1994). Ionospheric and atmospheric disturbances around Japan caused by the eruption of Mount Pinatubo on 15 June 1991.*Journal of Atmospheric and Solar Te"estrial Physics, 56(9),* 1227-1234. https://doi.org/10. 1016/0021 9169(94)90060 4

Latter, A. L., LeLevier, R. E., Martinelli, E. A., & McMillan,W. G. (1961). A method of concealing underground nuclear explosions. *Journal of Geophysical Research, 66,* 943-946. https://doi.org/10.1029/JZ066i003p00943

Marchand, R., & Berthelier, J. J. (2008). Simple model for post seismic ionospheric disturbances above an earthquake epicenter and along connecting magnetic field lines. *Natural Hazards and Earth System Sciences, 8(6),* 1341-1347. Retrieved from www.nat hazards earthsyst sci.net/8/1341/2008/, https://doi.org/10.5194/nhess 8 1341 2008

Meng, X., Komjathy, A., Verkhoglyadova, 0. P., Yang, Y. M., Deng, Y., & Mannucci, A. J. (2015). A new physics based modeling approach for tsunami ionosphere coupling. *Geophysical Research Letters, 42,* 4736-4744. https://doi.org/10.1002/2015GL064610

Mikhailov, Y.M., Mikhailova, G.A. & Kapustina, 0.V. (2000). VLF effects in the outer ionosphere from the underground nuclear explosion on Novaya Zemlya Island on 24 October, 1990 (Intercosmos 24 satellite data).*Journal of Space Weather and Space Climate (C), 25(1-2),* 93-96.

National Research Council (2012) *The Compehensive Nuclear Test Ban Treaty: Technical issues for the United States, Washington,* DC: the National Academies Press. https://doi.org/10.17226/12849

Park, J., Von Frese, R. R. B., Grejner Brzezinska, D. A., Morton, Y., & Gaya Pique, L. R. (2011). Ionospheric detection of the 25 May 2009 North Korean underground nuclear test. *Geophysical Research Letters, 38,* L22802. https://doi.org/10.1029/2011GL049430

Richmond, A. D. (1978). Gravity wave generation, propagation, and dissipation in the thermosphere. *Journal of Geophysical Research, 83,* 4131. https://doi.org/10.1029/JA083iA09p04131

Ridley, A. J., Deng, Y., & Toth, G. (2006).The global ionosphere thennosphere model. *Journal of Atmospheric and Solar Terrestrial Physics, 68(8),* 839-864. https://doi.org/10.1016/j .jastp.2006.01.008

Rieger, M., & Leitinger, R. (2002). Assessment of TID activity from GPS phase data collected in a dense network of GPS receivers. *Acta Geodaetica et Geophysica Hungarica, 37*(2-3), 327-341. https://doi.org/10.1556/AGeod. 37.2002.2 3.23

Roberts, D. H., Klobuchar, J. A., Fougere, P. F., & Hendrickson, D. H. (1982). A large amplitude traveling ionospheric disturbance produced by the May 18, 1980, explosion of Mount St. Helens. *Journal of Geophysical Research, 87,* 6291--6301. https://doi.org/10.1029/ JA087iA08p06291

Savastano, G., Komjathy, A., Verkhoglyadova, 0., Mazzoni, A., Crespi, M., Wei, Y., & Mannucci, A. J. (2017). Real time detection of tsunami ionospheric disturbances with a stand along GNSS receiver: A preliminary feasibility demonstration. *Scientific Reports,* 7(1), 46607. https://doi.org/10.103 8/srep46607

Seker, I., Livneh, D. J., & Mathews, J. D. (2009). A 3 D empirical model of Fregion medium scale traveling ionospheric disturbance bands using incoherent scatter radar and all sky imaging at Arecibo. *Journal of Geophysical Research, 114,* A06302. https://doi.org/10.1029/ 2008JAO 14019

Shiokawa, K., Lu, G., Otsuka, Y., Ogawa, T., Yamamoto, M., Nishitani, N., & Sato, N. (2005). Geomagnetic conjugate observation of nighttime medium scale and large scale traveling ionospheric disturbances: FRONT3 campaign. *Journal of Geophysical Research, 110,* A05303. https://doi.org/10.1029/2004JA010845

Yang, Y. M., Garrison, J. L., & Lee, S. C. (2012). Ionospheric disturbances observed coincident with the 2006 and 2009 North Korean underground nuclear tests. *Geophysical Research Letters, 39,* L02103. https://doi.org/10.1029/2011GL050428

Yeh, K. C., & Liu, C. H. (1974). Acoustic gravity waves in the upper atmosphere. *Reviews of Geophysics and Space Physics, 12,* 193-216. https://doi.org/10.1029/RG012i002p00193

Yuen, P. C., Weaver, P. F., Suzuki, R. K., & Furumoto, A. S. (1969). Continuous travelling coupling between seismic waves and the ionosphere evident in May 1968 Japan earthquake data. *Journal of Geophysical Research, 74,*2256-2264. https://doi.org/10.1029/ JA074i009p02256

Recommended Critical Infrastructure Security and Resilience Readings

Felix Kwamena, Ph.D.*
Email: felix.kwamena@carleton.ca

Kane, Joseph (2018) Recognizing Infrastructure's Role as a Local Economic Anchor, Brookings Institute, USA, August 10, https://www.brookings.edu/blog/the-avenue/2018/08/10/recognizing-infrastructures-role-as-a-local-economic-anchor/

Digital Threat in the Netherlands is Increasing, Cyber Security Assessment Netherlands, 2018 Ministry of Justice and Security (The Netherlands), https://english.nctv.nl/current_topics/news/2018/digital-threat-in-the-netherlands-is-increasing.aspx

Flournoy, M. Sulmeyer, M. (2018) Battlefield Internet: A Plan for Securing Cyberspace, Foreign Affairs, Vol. 97, No. 5, https://www.foreignaffairs.com/articles/world/2018-08-14/battlefield-internet?cid=int-fls&pgtype=hpg

Kahan, Jerome H, (2018) Understanding Resilience: The Blind Men and the Elephant, *Journal of Homeland Security Education*, Volume 7, pp 1-3.

Comiskey, John (2018) Theory for Homeland Security *Journal of Homeland Security Education*, Volume 7, pp 29-46.

Ulan, Elizabeth, Lockwood, Brian, and Comiskey, John (2018) Constitutional, Ethical, Both or Neither? An Investigation of Homeland Security Majors' Perceptions of National Security Agency Bulk Surveillance Programs, *Journal of Homeland Security Education*, Volume 7, pp 46-59.

Trverton, Gregory, Thvedt, Andrew, Chen, Alicia, Lee, Kathy, McCue, Madeline, Addressing Hybrid Threats, Swedish Defence University, Centre for Asymmetric Threat Studies, http://fhs.diva-portal.org/smash/record.jsf?pid=diva2%3A1219292&dswid=8378

Fischer, Severin (2019) Technological Innovation and the Geopolitics of Energy, Centre for Security Studies, April 5, http://www.css.ethz.ch/en/services/digital-library/articles/article.html/3d107f4c-298a-4c8d-a613-40fcb038d6d8

European Union Terrorism Situation and Trend Report 2018 (TESAT 2018) https://www.europol.europa.eu/activities-services/main-reports/european-union-terrorism-situation-and-trend-report-2018-tesat-2018

Forcese, Craig (2019) HUAWEI: Canada and the Rule of Law in the Meng Wanzhou Matter, LAWFARE, March 7, https://www.lawfareblog.com/canada-and-rule-law-meng-wanzhou-matter

Redmon, R. J., Denig, W. F., Loto'aniu, T. M., & Fuller-Rowell, D. (2018a). Recent geoeffective space weather events and technological system impacts in N. Buzulukova (Ed.), Extreme Events in Geospace (Chap. 24, pp. 587-609). Amsterdam, Netherlands: Elsevier.

Strain, D. (2018) A 1972 solar storm triggered a Vietnam War mystery, CU Boulder Today, https://www.colorado.edu/today/2018/11/12/1972-solar-storm-triggered-vietnam-war-mystery

Wachinger, G., Renn, O., Begg, C., & Kuhlicke, C. (2013). The risk perception paradox - implications for governance and communication of natural hazards. Risk Anal, 33(6), 1049–1065. https://doi.org/10.1111/j.1539-6924.2012.01942.x

Montibeller, G., and D. von Winterfeldt (2015), Cognitive and motivational biases in decision and risk analysis, Risk Analysis, 35(7), pp. 1230-1251, https://doi.org/10.1111/risa.12360.

Michailova, J., T. Tyszka, and K. Pfeifer (2016), Are people interested in probabilities of natural disasters? Risk Analysis, 37(5), pp. 1005-1017. http://dx.doi.org/10.1111/risa.12685.

Clemen, R. T. (1997). Making Hard Decisions: An Introduction to Decision Analysis (2nd ed.) Boston: Duxbury Press.

Hardy, R. D. (2019). A Sharing Meanings Approach for Interdisciplinary Hazards Research. Risk Anal, in press. https://doi.org/10.1111/risa.13216

Oughton, E. J., Hapgood, M., Richardson, G. S., Beggan, C. D., Thomson, A. W. P., Gibbs, M., … Horne, R. B. (2019). A Risk Assessment Framework for the Socioeconomic Impacts of Electricity Transmission Infrastructure Failure Due to Space Weather: An Application to the United Kingdom. Risk Anal, in press. https://doi.org/10.1111/risa.13229

Snyder, Jesse, How foreign companies use Canada's universities to steal away huge chunks of intellectual property.

Innovation Nation: Lax rules around university R&D programs are doing more to benefit foreign multinationals than Canada, National Post, March 6, https://business.financialpost.com/technology/how-foreign-companies-use-canadas-universities-to-steal-away-huge-chunks-of-intellectual-property

Tsafo, Nikos, (2019) Is Russia Winning the Race to Develop Arctic Energy? Center for Strategic and International Studies [USA], 22 March https://www.csis.org/analysis/russia-winning-race-develop-arctic-energy

Fast, Stewart, (2018) Who Decides? Balancing and Bridging Local, Indigenous and Broader Societal Interests in Canadian Energy Decision Making, Energy Regulation Quarterly, Vol. Issue 1, pp 37 – 46.

Bird, Stephen, (2018) Addressing the Policy Regulatory Nexus in Canada's Energy Decision Making, Energy Regulation Quarterly, Vol 6, Issue 3 pp 61 – 67.

Castro, Miguel (2019) Is Water Grid a Greener Grid? The Energy Journal, Vol. 40, No. 1, pp 213 – 246.

Dato, Prudence, (2019) Investment in Energy Efficiency, Adoption of Renewal Energy and Household Behavior: Evidence from OECD Countries, The Energy Journal, Vol 39, No 3, pp 213 – 244.

Linn, J. McConnell, V. and Leard, B. (2018) How Do Low Gas Prices Affect Costs and Benefits of U.S. New Vehicle Fuel Economy Standards? Economics of Energy & Environmental Policy, Vol. 7 No. 2, pp 51- 68.

Zakaria, Amro, "U.S. Energy Dominance from Whole Oil to Shale; how the New U.S. Energy Doctrine will Change the World", IAEE Energy Forum, Second Quarter 2019, pp 17-19.

Doshi, Tilak, K., "What Would Adam Smith Say about the Rush by Banks to Stop Funding Coal Power Plant?" IAEE Energy Forum, Second Quarter 2019, pp 21-22.

Hediger, Werner "Corporate Social Responsibility and Governance of Hydro Power – New Challenges in Energy Economics and Policy", IAEE Energy forum, Second Quarter 2019, pp 23-25.

Walker, Tom; Falvi, Suzanne; and Nelson, Tim "A New Approach to Valuing Reliability in Australia's National Electricity Market", IAEE Energy Forum Second Quarter 2019, pp 27-29.

Thompson, Philip, "What Do We Do When Energy is Free"? IAEE Energy Forum Second Quarter 2019, pp 31-33.

Warren, Peter, "Demand-Side Policy: Mechanisms for Success and Failure", Economics of Energy and Environmental Policy, Vol. 8, No. 1, March 2019, pp 119-144.

De Fatima, Maria, Arthur, S.R., and Cokerill, Andrew, "The Roles of Government and the Public Utility in Achieving Universal Access to Electricity", Economics of Energy and Environmental Policy, Vol. 8, No. 1, March 2019, pp. 103-118.

Fowlie, M., Khaitan, Y., Wolfrom, C., and Wolfson, D., "Solar Microgrid and Remote Energy Access: How Bleak Incentives Can Undermine Smart Technology", Economics of Energy and Environmental Policy, Vol. 8, Nov. 1, March 2019, pp 59-84.

Felix Kwamena, *Ph.D.*

Adjunct Professor/Director
Infrastructure Resilience Research Group (IR²G)
&
Director, Energy Infrastructure Security Division
Energy Sector, Natural Resources Canada

INFRASTRUCTURE RESILIENCE RESEARCH GROUP (IRRG)
UPCOMING EVENTS

SPRING / FALL 2019

EVENT	DATE / LINK
Spring / Fall 2019 Training Courses	January to December 2019 https://carleton.ca/irrg/training/
3rd International Urban Security and Resilience Symposium Jun 26, 2019 – Jun 27, 2019	https://carleton.ca/irrg/cu-events/3rd-international-urban-security-and-resilience-symposium/
2nd Economic Security, Resilience and De-Carbonization of Heavy Industries Workshop Theme: A Multi-stakeholder, -Multidisciplinary Approach to Addressing Challenges and Leveraging Opportunities for the De-Carbonization of Heavy Industries Quebec Suite, Fairmont Chateau Laurier Hotel, 1 Rideau Street, Ottawa, Ontario	November 27 - 28, 2019 https://carleton.ca/irrg/cu-events/economic-security-resilience-and-de-carbonization-of-heavy-industries-2/
2019 IRRG Dean's Lecture The Dean's Annual Lecture Series – Infrastructure Security and Resilience: Economic Security, Resilience and De-Carbonization of Heavy Industries Quebec Suite, Fairmont Chateau Laurier Hotel 1 Rideau Street, Ottawa, Ontario Ottawa, Ontario	November 28, 2019 (Evening 6:00 PM – 10:00 PM) https://carleton.ca/irrg/cu-events/2019-deans-lecture/

Check out IRRG's Website for:

Upcoming events

https://carleton.ca/irrg/events/

Professional Training / Development Courses

https://carleton.ca/irrg/training

Latest Issue of Online Journal ***Infrastructure Resilience Risk Reporter*** **(IR^3)**

https://carleton.ca/irrg/journal/