**VOL 1 ISSUE 3** **June 2015**

**Guest Editor**
Dr. Robyn Fiori

**IR3 Feature Articles**

## Editorial Corner

Dr. Robyn Fiori

### About the Editor

Dr. Robyn Fiori is a research scientist for the Canadian Hazards Information Service, 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. Her research has been published in numerous peer reviewed scientific journals including the Journal of Geophysical Research, the Journal of Atmospheric and Solar-Terrestrial Physics, and Space Weather. Dr. Fiori received her B.Sc., M.Sc., and Ph.D. from the University of Saskatchewan Department of Physics and Engineering Physics while studying in the Institute of Space and Atmospheric Studies.

### This Issue

The third issue of IR3 focuses on the 'Insider Threat' and comes from authors responsible for the security of critical infrastructure, who develop and implement resilience programs or are otherwise involved in the functionality, dependability, security, and resilience of critical assets and services.

Growing threats from cyber-attacks requires organizations to rely heavily on their incident response capabilities. According to authors Antoine Lemay and Tiago de Jesus, the first step toward development of an incident response program able to handle advanced persistent threat incidents is the creation and inclusion of indicators of compromise to be used by incident response teams to improve security.

Communication, both within an organization and between organizations, is the cornerstone to creating a strong resilience program nationwide. Ross Johnson discusses the importance of communication of threat information, best practices, and coordination on a local, national, and even international scale to best protect Canadian infrastructure. Mike Chemichen points out that security groups have an additional challenge in communicating the nature and significance of potential threats and the importance of resilience activities to executives. He highlights the importance of working with company leaders to develop an understanding of what resilience is and the role it plays in security.

Increasing awareness due in part to organizations such as the IRRG has brought increasing awareness to the impacts of space weather on critical infrastructure; an issue discussed in an article by the Canadian Space Weather Forecast Centre.

Raynald Lampron's article takes a step back from the development and implementation of resilience programs taking a more philosophical approach by looking at the role religion has played in conflicts throughout history and in terrorism.

### Next Issue

For Issue 4, we invite authors working in academia, industry or government to contribute articles and/or book reviews relating to their experience in the field of infrastructure resilience describing potential sources of compromise and lessons learned. Manuscripts of 3000-4000 words are requested by early October. You may not have much time or experience in writing 'academic' articles, but IR3's editorial board can provide guidance and help. Your experience is valuable and IR3 provides an ideal environment for sharing it.

# *Threat Actor Based Incident Response Process*

*Antoine Lemay*, PhD*
Département de génie informatique et génie logiciel
École Polytechnique de Montréal
Email: antoine.lemay@polymtl.ca

*Tiago de Jesus*, PhD*
Infrastructure Resilience Research Group (IR2G)
Faculty of Engineering and Design
Carleton University
Email: tiagodejesus@gmail.com

## I. INTRODUCTION

Today, we are facing an ever-growing number of cyber threats from various threat actors: cyber-criminals who seek personal information for fraud, advanced persistent threats to steal secrets for foreign governments, hacktivists to disrupt network operations for political causes, or just for fun. This increase in the threat landscape naturally leads to more cyber incidents, which in turn forces organizations to increasingly rely on their incident response capabilities.

Unfortunately, incident response is too often an ad-hoc affair with a process that is frequently dictated by the specifics of individual incidents. This is in part due to the diversity of threat actors and the risks each of them pose to an organization. While some frameworks exist to structure the incident response process, such as the SANS PICERL[1] model, they provide little guidance on the specific actions to undertake and don't take into account the nature of the threat. To address the increasing pressure on incident response teams from all the various cyber actors, there is a growing need for an efficient *threat actor based* incident response process.

Fortunately, there is a growing amount of available cyber intelligence that can be leveraged to produce an effective incident response process based on threat actor information. This intelligence is often codified in so-called *Indicators of Compromise*. These indicators provide actionable intelligence that can be used by incident response teams to select the optimal response procedure in order to increase operational efficiencies. The goal of this article is to present a methodology that integrates *Indicators of Compromise* into a threat actor based incident response process to maximize the effectiveness of the process.

This article starts by defining an *Indicator of Compromise*. We then discuss how to leverage *Indicators of Compromise* in order to produce an effective threat actor based incident response process. This is followed by a summary of the resulting process. Finally, a brief conclusion is offered to recapitulate key findings and show the way forward for incident response teams.

## II. WHAT IS AN INDICATOR OF COMPROMISE?

An *Indicator of Compromise* (IoC) is an observable element (called event in the context of incident response) that is strongly indicative of an attempt to compromise a system. For example, observing that your room has been tossed could be an indicator of a burglary. In the context of Information Technology (IT) systems, if a particular file associated with a piece of malware is present on your network this could be an IoC.

A number of organizations publish IoCs for IT systems. For example, the security firm Mandiant has published indicators for the threat actor they refer to as

[1] Ref: Mason Pokladnik, "An Incident Handling Process for Small and Medium Businesses", SANS Reading Room, 2007 [available online : http://www.sans.org/reading-room/whitepapers/incident/incident-handling-process-small-medium-businesses-1791]

APT1[2]. Another example is the Canadian Cyber Incident Response Center (CCIRC). Numerous indicators are available to critical infrastructure operators, and other stakeholders, on the CCIRC partners portal[3]. These indicators take numerous forms, such as the "fingerprints" of malicious files (i.e. hashes), IP addresses associated with malware hosting servers or command and control nodes, registry key entries used or created by malware, among many others.

## III. Integrating Indicators of Compromise into the Incident Response Process

A typical incident response process can be divided into the six steps of the SANS PICERL model[4]:

1. Preparation
2. Identification
3. Containment
4. Eradication
5. Recovery
6. Lessons Learned

In the preparation step, the incident response team puts in place the capabilities required to detect and respond to incidents. In the identification step, each event is analyzed to determine if it is an incident or not. In the containment step, active efforts are taken to prevent the spread of the threat. In the eradication step, the threat is eliminated / removed from the network. In the recovery phase, systems are restored to their "clean" state and operations are returned to normal. Finally, in the lessons learned step, the team meets to discuss if either the incident handling process can be improved and/or if steps can be taken to avoid such incidents from re-occurring in the future.

Unfortunately, the above process often fails at the identification phase. Modern IT systems produce a large volume of events, from operating systems logs, firewall logs, web proxy logs, intrusion detection system alerts, help desk reports, etc., which quickly reaches levels that are not humanly possible to analyze manually. To overcome this barrier some organizations turn to Security Information and Event Management (SIEM) systems to automate the event analysis process. Unfortunately, SIEMs are notoriously complicated to use and typically require dedicated experts to effectively operate them. Moreover, because of the speed at which cyber threats evolve, the detection rules that these systems must use to avoid missing incidents are so general that they produce a large number of false positives, which in turn have to be manually analyzed. IoCs offer a simple and effective approach to identify incidents in an ocean of events.

## IV. Incident Response Process: Generic Cyber-Criminal Versus Advanced Persistent Threats

For commodity malware, a reasonably well-documented process, which steps through each phase of PICERL models, can be followed to get a network back to normal operating conditions. After identifying malware, through anti-virus software or IoCs, infected hosts are isolated by unplugging them from the network or through firewall rules. The infected hosts are then "cleaned" by the anti-virus software or re-imaged by the incident response team in order to return the infected hosts to their pre-incident pristine state. Finally, once the malware has been eradicated from the network, the team discusses how the vector of infection could be blocked to avoid re-occurrence of such an incident. This recipe works well to combat commodity malware, but can have disastrous consequences when it comes to responding to state-sponsored threat actors running an espionage campaign.

The rise of so-called Advanced Persistent Threats (APTs) introduces new risk-based decision making

---

[2] Ref : http://intelreport.mandiant.com/Mandiant_APT1_Report_Appendix.zip

[3] Ref : Public Safety Canada, "CCIRC Community Portal," [available online : https://pc3p.ps-sp.gc.ca/_forms/PC3PLogin/Default.aspx?, partner status available by request.]

[4] Ref: Mason Pokladnik, "An Incident Handling Process for Small and Medium Businesses," in *SANS Reading Room*, 2007 [available online : http://www.sans.org/reading-room/whitepapers/incident/incident-handling-process-small-medium-businesses-1791]

into the incident response process. The first decision point is the selection of incident response activities that the team should pursue. Unlike common cyber-criminals, once an APT actor gains a "foothold" on a target network, they quickly introduce new tools (e.g. Remote Access Toolkits or RATs) and pursue various activities (e.g. steal passwords) in order to maintain a persistent access to the victim's network. The malware used to gain an initial point of presence on the target's network is just a single element that is part of a much more complex operation. If the commodity malware response process is used to respond to such a threat actor, precious clues, critical to understanding the extent of the APT operation, are irreversibly lost in the "cleaning" phase of the process (i.e. removal of malware or re-imaging of hosts).

Judicious use of IoCs can enable an incident response team to select the proper course of action without resorting to costly investigation for every single piece of malicious code found on the network. By leveraging the contextual information associated with IoCs, the incident response team could potentially determine whether they are responding to a simple commodity malware or a sophisticated espionage campaign being perpetrated by a state-sponsored threat actor. To effectively respond to an incident, the team must classify its IoC by the type of threat actor (e.g. cyber-criminal or APT) in the preparation phase. When an indicator triggers an alarm, the team can refer back to the classification to select the appropriate course of action. For example, if a file "fingerprint" matches an indicator extracted from Mandiants' APT1 list, the team needs to treat the incident as serious and investigate for further evidence of espionage activity. On the other hand, if a signature match is associated to a known criminal botnet, the team can just clean it up and move on. In the case of IoCs that are not specifically attributed to a type of threat actor, we can look at the specific tools, techniques and procedures used to compromise the network (e.g. spear-phising, Remote Access Toolkit, etc.) to determine the likelihood of an APT.

The second decision point relates to the urgency of the actions that must be taken by the incident response team. This depends critically on the current state of the incident. For example, it might be appropriate to run to a fire extinguisher at the start of a kitchen fire, but it might be too late when the house is a blazing inferno. Similarly, the actions that need to be taken when an APT has just established a presence in your network, and is performing internal reconnaissance, are very different than when they are in the process of extracting your crown jewels. We can leverage other contextual information provided with IoCs to help the team ascertain which phase of an operation the attackers have reached.

## V. Leveraging Contextual Information from Indicators of Compromise

Indicators of compromise are often tagged with additional contextual information in the form of keywords such as "pre-infection" or "post-infection." For example, let us consider the *www.evil.com* domain name as an IoC. The domain might have been flagged because it is known to be a malware hosting site for an APT actor. A computer that visits this site *might* get infected, but this is not a necessary consequence. The simple fact that an organization finds this indicator in its web proxy logs does not imply that its network has been compromised. For this reason this indicator can be tagged with the "pre-infection" keyword. On the other hand, if the *www.evil.com* domain is a known command and control (C&C) server used by an APT actor, a computer that connects to this domain is necessarily compromised. The presence of this domain indicator in an organization's logs is a definite sign that an APT actor has successfully breached its defenses and has gained presence onto its network. In this case the "post-infection" tag is appropriate for this IoC. Even in the case where no context is included with the indicators, it is often possible to extrapolate this type of contextual information. For example, an indicator that points to a new Windows Registry value is inherently a post-infection indicator because a program had to be run to create that effect.

Based on the presence of pre-infection or post-infection indicators, different paths must be followed. In the case of the presence of a post-infection indicator, a compromise has already occurred,

containment actions must be pursued more forcefully and an investigation of the extent of the compromise must be undertaken immediately. In the case where a pre-infection indicator is found, the most important action is to assess if the attempt to compromise the network was successful or not. If the attempt was successful, we can move on to the containment of affected hosts. However, if the attempt was not successful, we can either move on to lessons learned or investigate the root cause that allowed the attempt to occur in the first place. This is especially important in incidents related to APT actors where a failed attempt is only an indication of further attempts down the road.

## VI. Summary of the Incident Response Process

It is possible to effectively integrate IoCs into the incident handling process by introducing decision points between key steps in the PICERL model. The resulting process is illustrated in Figure 1. Between the preparation and identification phase, when events are analyzed to determine if they are incidents, we can use the database of IoCs to decide if an incident has occurred. If an IoC is triggered by one of the events, we can assume an incident has occurred and start the response process right away. After all, by their very definition, IoCs are events that are strongly correlated with the presence of compromise. Their very presence is a sign that something has gone wrong.

Once an incident has been declared, a risk-based decision for containment presents itself. If there are clear signs that a host has been successfully compromised, more haste is required than if only a potential vector of infection was observed. As such, if an indicator tagged with the "post-infection" keyword is triggered, immediate containment steps should be taken. If that is not the case, the incident response team should gather sufficient information to determine whether or not the incident has led to an actual compromise of the network before implementing containment actions.

Before moving on to eradication and recovery, the question of the intent of the threat actor needs to be addressed. If the attack was not targeted, it is most likely that the compromise was caused by a generic piece of commodity malware through a "drive-by download" set up by a cyber-criminal seeking to monetize *any* infected host. Once the commodity malware is cleaned off from the network, the likelihood of re-infection is relatively low since the organization was not intentionally infected by the cyber-criminal, but was simply one among many victims.

On the other hand, if the attack was specifically targeting an organization, the attacker will make (or has made) further attempts to compromise the target's network. In this case, we must pursue a more in-depth investigation to ascertain the full scale of the intrusion. For this case, context associated with the indicators (such as keywords of "target", "spear phishing", "Remote Access Tool/Trojan", etc.) can be leveraged to help with the identification of targeted attacks from an Advanced Persistent Threat.

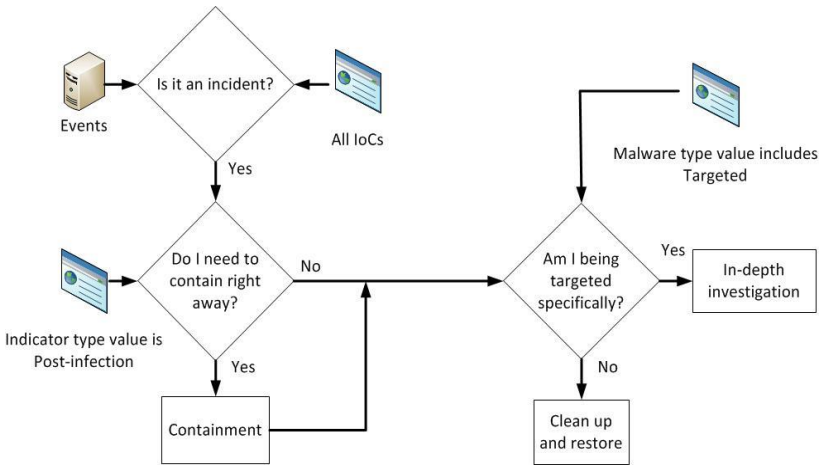


**Figure 1:** Integrating indicators of compromise into the PICERL process.

## VII. Conclusion

Indicators of compromise provide clear evidence of malicious activity. A judicious use of these indicators can significantly improve the effectiveness of the incident response process. They can be used on their own to help with the identification of events that should be considered incident. However, the leveraging of the additional contextual information can greatly help with critical risk-based decisions made in the containment step of the traditional incident response process. Using this additional data, incident responders can more accurately evaluate the risk associated with delaying containment activities. More importantly, incident responders can gauge the potential organizational risk given their knowledge of the threat actor.

In the first case, it will often be possible to classify indicators in pre-infection and post-infection indicators, which gives defenders a rough idea of the state of the incident. In the second case, keywords associated with particular tools, techniques and procedures of specific attackers can be used to identify the type of threat actors, i.e. an advanced persistent threat or a common cyber-criminal, and orient further incident response actions accordingly.

Ultimately, the inclusion of IoCs in the incident response process represents the first step toward an incident response program that is able to deal with advanced persistent threat incidents. It creates the proper framework to include the findings of in-depth investigations, in the form of new IoCs, in the incident response operations. The increased need for technical intelligence, again in the form of IoCs and the associated contextual information, may eventually lead to fully incorporating the intelligence lifecycle process for incident response operations.

*Dr. Lemay is a security researcher working on improving the safety, security and resilience of Supervisory Control and Data Acquisition (SCADA) networks against targeted cyber-attacks from Advanced Persistent Threats (APT). He received his Ph.D. from the computer engineering department from l'École Polytechnique de Montréal with a specializing in SCADA security. He has published papers in a number of venues, including the International Symposium for Industrial Control Systems (ICS) & SCADA Cyber Security Research and the Journal of Information Warfare. To complement his academic knowledge Dr. Lemay has worked as a telecommunications engineer consulting for Hydro Quebec's distribution division and as a security analyst at a large Quebec corporation. He has also obtained several professional certifications in the field of information security, such as CISSP, GSEC and GCIH.*

*Dr. Tiago de Jesus is a Senior Advisor for the Energy Infrastructure Security Division (EISD) at Natural Resources Canada. He is also the Deputy Project Manager for the National Energy Infrastructure Test Center (NEITC), which focuses on cyber threats to the Energy and Utilities sector. He previously worked for the RCMP National Security Criminal Investigation (NSCI) program as a Subject Matter Expert (SME) and was later in charge of their Cyber Unit. He holds an undergraduate degree in mathematics and physics from l'Université de Montréal, a Master's degree in physics from the University of British Columbia and obtained his PhD at McGill University in nano-electronics. He has also worked on Bay Street for Bank of Montreal as a risk analyst and co-founded two high-tech start-up companies, which developed computer simulation software for chipmakers. He is also a Civilian Expert for NATO's Rapid Response Team and a Research Associate at Carleton University's Infrastructure Resilience Research Group (IR2G).*

# *Electric Sector Security in Canada – A Strategic Approach*

*Ross Johnson*, CPP*
Senior Manager, Security and Contingency Planning
Capital Power Corporation

## I. CAN YOU LIVE WITHOUT ELECTRICITY?

In 2009, the book 'One Second After' examined that question. The story is about a (fictitious) electromagnetic pulse attack on the United States that knocks out the North American Interconnected Grid. The story, set in North Carolina, details the gruesome breakdown of modern society. Without giving too much away, it might be worthwhile to mention that a considerably drier treatment of the same subject by a Commission established by the US National Defense Authorization Act for Fiscal Year 2001, The Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack mentions the word 'catastrophic' thirty-three times in its fifty-seven page Critical National Infrastructure document, and in that regard, 'One Second After' doesn't disappoint.

In Canada ten sectors are considered critical. Electricity, a subset of the **Energy & Utilities** group, is considered to be the one critical interdependency that allows all of the others to exist. Without electricity, there is no banking, food distribution or sales, government, computers, phones, potable water, manufacturing, communications, or health care. In other words, you are into 'One Second After' territory.

Protection of the electricity sector in Canada is a complex task which requires the sharing of threat information, best practices, and coordination among electric utilities, government agencies, industry stakeholders, and other sectors. Central to this effort is the Canadian Electricity Association (CEA)'s Security and Infrastructure Protection Committee (SIPC).

Made up of members from electricity sector companies across Canada and reporting to the CEA Board of Directors, the SIPC is responsible for developing and delivering security programming and policy. The three areas of concern are policies related to physical security, IT security, and emergency preparedness.

To accomplish this mandate, the SIPC works with all stakeholders to ensure that Canadian federal activities on critical infrastructure protection meet the needs of the public, the industry, and our other North American industry partners. SIPC activities are coordinated at the national level to prevent problems from being pushed from one jurisdiction to another. We work closely with our partners at Natural Resources Canada, Public Safety Canada, sector networks, and in the law enforcement and intelligence communities.

In addition to our Canadian partners, the SIPC is also related to the North American Electric Reliability Corporation's (NERC) Critical Infrastructure Protection Committee (CIPC), where three SIPC members have voting member status, and one sits on the CIPC Executive Committee.

The CEA SIPC has undertaken a number of initiatives designed to reduce the threat to our sector, increase the professionalism of our security practitioners, promote resilience and share knowledge and best practices with our partners in Canada and internationally.

## II. COPPER THEFT CAMPAIGN

Copper theft has emerged as one of the greatest single security issues that electricity sectors face worldwide. Because of economic growth and electrification in the developing world, the world's production of copper falls far short of its annual consumption. According to the International Copper Study Group, in 2014 the world's copper mines produced 18.6 million tonnes, while the demand was 22.4 million tonnes. The shortfall of 3.8 million

tonnes is made up through recycling. This demand sets a high price for scrap copper, which in turn feeds a criminal industry that strips the electricity sector of exposed copper wherever it is found. As copper is valued for its conductive properties and its corrosion resistance, it is often used in substations and switchyards to ground equipment and fences, which makes it easy prey for copper thieves. The problem is particularly acute in a country as geographically expansive as Canada, where a significant amount of electricity infrastructure is located in remote locations.

The theft of copper in the electricity sector creates a considerable problem for both safety and reliability. Because of the widespread distribution of electric assets, it is extremely expensive to provide full security protection (guards, CCTV cameras, intrusion detection systems, etc.) at each substation, switchyard, or power pole that uses copper for grounding. Because full security comes at a price that electricity consumers wouldn't be able to afford or pay, the CEA SIPC has launched a multi-part copper theft campaign that involves four components:

1. Promotion of a national action plan to implement best practices and approaches across the country;
2. Coalitions to combat copper theft – communities working together to deter copper theft;
3. Tighter Provincial regulation of transactions at scrap metal recycling facilities; and
4. Amendments to the Criminal Code to add the definition of Critical Infrastructure and sentencing options more proportional to the impacts of these crimes.

An excellent example of a coalition to combat copper theft is the work that Dean Young, Security Manager for Altalink LP, has done in Alberta. Concerned about the constant erosion of their infrastructure through copper theft, Dean created a community of interested people – electric sector security professionals, police, prosecutors and parole officers, crime prevention and awareness personnel, metal recyclers, construction industry security, and wire producers. This group, called the Provincial Electricity Physical Security (PEPS) working group meets on a quarterly basis, and has a clear mandate: collaborate to identify problems, and develop solutions that they all can support. This group has managed to do something that eluded us in the past: it has changed perception. Before, copper theft was seen purely in financial terms, and largely ignored. Today it is seen for what it is – a danger to the safety of the public, First Responders, industry personnel, and the perpetrator, as well as a threat to critical infrastructure.

PEPS has pioneered many firsts:

- Stakeholder education programs on safety and reliability;
- Legislative change in Alberta to support the fight against metal theft;
- Standardized reporting formats and witness statements to ensure all germane information is fully captured;
- Victim impact statements to ensure the courts understand the impact of the crime;
- Working with the criminal justice system, the jeopardy to the offender has been increased through a charge of Mischief Endangering Life instead of a theft under $5,000 or property damage;
- The courts can order civil forfeiture of the culprit's assets;
- Law enforcement is now allocating resources to combat metal theft; and
- Intelligence sharing between all stakeholders, including the production of weekly police intelligence summaries and analysis.

Dean has been recognized by the Government of Alberta for his work in this area, and in 2014 he received the Alberta Justice and Solicitor General Community Justice Award. This award "acknowledges the efforts of individuals who make an extraordinary contribution in promoting community safety, preventing and addressing crime throughout the province."

The PEPS model is also being adopted in Ontario through the efforts of Ron Gentle, Chief Security Officer at Hydro One.

## III. Professional Development

The CEA SIPC has created a definition of a professional security management career path for the electric sector. It is reflected in two forms: an Excel spreadsheet that shows the experience, training, and certification needed for every security position in a typical electric sector company; and a skills and experience worksheet for security directors and Chief Security Officers. This latter document was developed as a single-page reference guide for human resources staff and recruiters to use to assess résumés of persons coming from diverse backgrounds who are competing for leadership positions.

## IV. Doctrine Development

The SIPC is involved in the development of doctrine for use in the sector. A number of guidelines are in progress or complete:

- Protection of Information;
- Security Management Programs;
- Conduct of Investigations ;
- Common Cyber and Physical Security Incident Reporting;
- Obtaining Security Clearances;
- Personnel Risk Assessments; and
- Comparative Analyses of Corporate Security in the Electricity Sector.

The SIPC also participates in the NERC guideline process, and recently contributed to physical security guidelines related to the protection of power plants, substations, and transmission stations.

## V. Standards

Canadian electricity sector companies are influenced by the activities of NERC, a not-for-profit international regulatory authority who works to assure the reliability of the North American bulk power system. NERC is North America's 'electric reliability organization,' and is regulated by the US Federal Energy Regulatory Commission (FERC) and governmental authorities in Canada.

A major contribution to the reliability of the bulk power system is NERC's critical infrastructure protection (CIP) reliability standards. These standards, which cover both cyber and physical security and evolve with the threat, ensure the adequate protection of those assets whose loss could destabilize the bulk power system. The latest version of the standards, Version 6, requires a minimum baseline of protection for all electric grid cyber assets and systems. All of Canada's major users, owners and operators of the interconnected North American grid comply with NERC CIP standards.

In response to the attack on the Metcalf Substation in Palo Alto, California in April 2013, FERC ordered NERC to create a physical security standard for large stations or substations whose loss could destabilize or render inoperable the bulk power system. This new standard, CIP-014-2 *Physical Security*, will have an impact on most of Canada's large utilities. The author is also an Executive Committee member of the NERC CIPC, and represented Canada on the CIP-014 Standards Drafting Team, ensuring that Canada's perspective was taken into consideration.

## VI. Promoting Resilience

Electric utilities on both sides of the border have mutual aid agreements to provide emergency repair support to each other in case a hurricane or ice storm damages distribution and transmission networks. For example, 2012's Hurricane Sandy saw more than 700 trucks and utility crew members from Canada travel to assist in recovery and restoration efforts in the US.

In the past, deployment of repair trucks has been slowed at the border, delaying response time. Lisa Hood, the former Business Continuity Manager at Hydro One, led development and implementation of a cross-border protocol with the United States that facilitates the passage of their repair trucks across the border, greatly reducing the amount of time it took for trucks to cross. The CEA SIPC adopted it as a protocol within the electricity sector, as did the Canadian Gas Association for gas distributors. Already adopted by the US Department of Homeland Security, we are awaiting information from the Canada Border Services Agency that will allow full, standardized deployment within Canada.

The protocol is simple – based on an Excel spreadsheet, all the vehicle, equipment and personnel information required for a border crossing is filled out for each vehicle and crew in advance of crossing. The spreadsheet containing this information is emailed to both the US and Canadian officials at the port of entry sides of the border crossing point where the utility will cross the border. The vehicles all collect in an assembly area near the border crossing, then are dispatched to the border in packets of several vehicles each. When they get to the border, the customs and immigration agents merely confirm that the vehicle matches the people inside as indicated on the spreadsheet, and then wave them on. A process that once could take hours has been reduced to minutes and seconds.

## VII. Information Sharing

The SIPC shares information with a number of stakeholders. If any CEA member is attacked, this information can be communicated quickly to other CEA members through a comprehensive incident response plan. For less critical incidents, a periodic Security Bulletin provides the information to CEA members. Threat information is shared within North America through attendance at classified briefings provided by Natural Resources Canada and the United States Department of Energy. We work closely with the Royal Canadian Mounted Police's (RCMP's) National Critical Infrastructure Team, and many of our members use the RCMP's Suspicious Incident Reporting System. Many also dial in to the monthly Electric Sector Information Sharing and Analysis Center teleconference, which discusses cyber and physical attacks on the electric sector in Canada and the United States.

A member of the CEA leads the NERC Physical Security Roundtable Group, which consists of over 130 electric sector security professionals across the continent. The Group meets by telephone once per month to discuss security issues, trends, and ideas.

## VII. Cyber Threat Reduction

The SIPC is engaged with several different organizations in an effort to reduce the threat from cyber space. These organizations include:

- NERC's Energy Sector Information Sharing and Analysis Center (ES-ISAC);
- Public Safety Canada's Canadian Cyber Incident Response Centre (CCIRC);
- Natural Resources Canada's National Energy Infrastructure Test Centre (NEITC); and
- US Industrial Control Systems – Computer Emergency Response Team (ICS-CERT).

We also recently sent a delegation to Israel at the invitation of the Israeli Prime Minister's Office to discuss cyber security issues in the electricity sector. We discovered that we have much to learn from Israel – they are years ahead of us in this area, and have transitioned from cyber *security* to cyber *defence*. We are in discussions now to see how we can help Israel implement some of this new technology in Canada and the United States.

We were also pleased that CEA's calls for additional resources at the federal level for preparedness, prevention and response to cyber events was included in the recent federal budget through increased funding and notice of coming legislation to heighten the protection of vital cyber systems. SIPC looks forward to contributing to the development of any new legislation by providing the electricity industry perspective.

## VIII. Alliances for Mutual Protection

We are considering an intelligence and information-sharing alliance with the finance and telecommunication sectors. Electricity is critical to both, and civil society requires resilience in all three sectors. By working together, we can help them understand the measures we have in place to protect their access to electricity while we learn of the wider cyber threat to critical infrastructure, and we can work with them to create contingency plans that will help them to ensure their continuity of operations in the event of an emergency or natural disaster.

At the beginning of this article, we talked about the movie 'One Second After' and the catastrophe that an EMP strike can cause. The EMP scenario has an analogue in nature, though – a geomagnetic disturbance (GMD) event. GMD events are caused by solar disturbances, and can lead to induced currents in power lines, overwhelming transformers and other equipment, and causing outages. An example of this occurred on March 13, 1989 when a GMD event blacked out the province of Quebec for over nine hours.

The best mitigation for a GMD event occurs prior to the event taking place. Learning from the 1989 incident, electric utilities adopted practices that would reduce the likelihood of a blackout in the event of another solar disturbance, through sound engineering practices and preparation; developed real-time alert systems that measure the impact of solar disturbances on the grid as they happen; and modified power system operating procedures to reduce power flow on lines and direct-current interconnections and suspend major switching operations during a disturbance.

## IX. CONCLUSION

The members of CEA's Security and Infrastructure Protection Committee take the business of protecting Canadians' access to reliable, affordable, and sustainable electricity very seriously. We work closely with governments, both federal and provincial, as well as with law enforcement and the intelligence community. We exchange ideas both nationally and internationally, and regularly challenge our members to find better ways of achieving our goals for less cost.

The owners and operators of Canada's critical electricity infrastructure understand the responsibility they have to provide clean and reliable electricity to Canadians, and through the CEA's SIPC, work hard to protect it. We look forward to combining our efforts with other critical infrastructure sectors so together we can ensure a sound and resilient base upon which Canada can grow and prosper. Hopefully, our combined efforts will ensure that a scenario like 'One Second After' remains firmly on the fiction shelf, where it belongs.

**Ross Johnson, CPP - is the Senior Manager of Security and Contingency Planning for Capital Power, based in Edmonton, Canada. He served in the Canadian Forces as an infantry and intelligence officer for 24 years. Since leaving the service in 2001, he has been employed in several security-related leadership positions in aviation security, the offshore oil industry, and the electricity sector.*

*Ross is the author of Antiterrorism Planning and Threat Response, a book on the prevention of terrorist attacks.*

*He is a member of the North American Electric Reliability Corporation's Critical Infrastructure Protection Committee, where he sits on the Executive Committee. He is also Chair of the Committee's Physical Security Working Group, and the leader of the Physical Security Roundtable Group.*

*He recently represented Canada on the Standards Drafting Team for the new critical infrastructure protection standard on physical security of large switchyards and substations.*

*Ross is also Chair of the Canadian Electricity Association's Security and Infrastructure Protection Committee, and Chair of ASIS International's Petrochemical, Chemical, and Extractive Industries Security Council.*

# *Resilience and Security for the Busy Executive*

*Mike Chernichen*, LLB*
Manager, Corporate Security

## I. OPENING THOUGHTS

Recently at an all employee meeting, a senior executive of our company jokingly referred to me as the "Director of Paranoia", in response to a question from one of my colleagues. I have known and worked with this executive for over 15 years and have had the privilege of earning his trust and respect. Like my colleagues I found his remark amusing, but also thought-provoking. As one of the top executives in our organization, this individual reviewed and approved the Security Management Plan that I created several years ago. In considering his remark I had to wonder whether I had adequately educated him regarding the primary purpose of our Security Management Plan.

Educating leaders in government or business regarding security for critical infrastructure, or simply convincing them of the need for their involvement in respect of the same is a challenging exercise. Very few of these individuals have any real experience or training relevant to the topic. Attempting to discuss complex aspects of security such as resilience tends to result in the executive shifting attention from the discussion to their smart phone. This is due in part to general misconceptions as to what resilience is and its role in respect to security.

Much has been written on the subject of resilience and critical infrastructure protection. Most are scholarly articles written in the language of techno-speak, in some cases waxing philosophically. Unfortunately the decision-makers who bear ultimate responsibility and accountability for the creation and implementation of effective security policies, protocols and plans, are rarely schooled in any field remotely related to the profession of security. These executives whether in industry and government, are charged with the responsibility for governance over the critical infrastructure that it is essential to the well-being of our nation. In their hands such articles are all too often dismissed as indecipherable, lacking clarity and thus failing to provide guidance which can be readily translated into effective action.

## II. THE NATURE OF RESILIENCE

Understanding resilience, like charity, begins at home. Corporate and government leaders relate best to the business they are responsible for. From their perspective, the responsibility they bear regarding security is focused on and usually limited to that business. Thus any discussion with them regarding resilience must begin with and relate back to that business.

The problem begins with the endless debate over definitions of resilience. In view of the target audience [the corporate or government leader], the most logical approach is to define resilience as the ability to:

- deter or, resist and repel the actions of a threat actor; and
- recover in an efficient and timely manner from such actions.

It is impossible to counter and prevent all threats. Resilience is the foundation of a security program. Creating and maintaining resilience is the "raison d'être" of having a security program.

In the case of resilience and its role in security, there are interesting parallels between the human body and an organization such as a nation state. Both are complex systems based on inter-reliance and support between individual elements of critical infrastructure. Both face a constantly evolving ecosystem of threats.
In the case of the human body, medical history has documented an evolutionary battle between health, well-being and longevity in the face of opposition from pathogens, environment, lifestyle and behaviour. Where once average lifespans ranged between 30 and

40 years, they now extend to 70 years and beyond with centenarians becoming common. The once short-lived hunter gatherer is the beneficiary of agriculture, the Industrial Revolution, urbanization and rapid advances in science and technology.

Our modern nation has seen a similar pattern of development. People spread across one of the largest contiguous landmasses in the world are united under a common flag and culture thanks to the evolution of transportation, communication and energy distribution systems.

However beneficial, the evolution of human society also brings new, and sometimes unexpected threats. For example, lack of genetic diversity among the human population, combined with modern global transportation systems exposes the human body in the modern world to pandemics that hitherto would have spread slowly or been contained in isolated corners of the world. In a parallel example, distant conflicts resulting from cultural extremism thousands of miles from our borders can generate direct threats to our national infrastructure via the very transportation and communication systems that form part of the network of global critical infrastructure.[5] [6]

Resilience may exist to a certain degree inherent in the natural characteristics of a site or system. For example a facility which is manned 24/7 has a degree of resilience against unauthorized access due to the continuous presence of personnel at the site.

However, native resilience is generally unable to address all potential threats to a site or system. Native resilience almost always lacks adaptability. For example a 14th century castle may have been state-of-the-art in providing resilience against human attackers, but would have fared poorly against the black plague. Ultimately this type of fixed fortification would have been unable to cope with the arrival of the gunpowder cannon on the battlefield without intervention by its owner to add additional countermeasures[7].

Returning to my analogy, the human body is equipped with its own automatic defences against infectious agents. However, without medical intervention, the human body is unable to defend itself against certain continuously evolving infectious agents, such as influenza without risk of sustaining temporary or permanent damage.

Thus effective resilience is a function of planning and continuous improvement. Using the example of the human body, receiving an annual flu shot which has been developed based on continuous monitoring of viral outbreaks and changes in viral strains globally is an attempt at effective resilience against infectious disease.

Effective resilience in the case of an organization also requires frequent testing of protective policies, procedures, designs and protocols in order to maintain a state of readiness and identify previously overlooked vulnerabilities. For example in the case of a cyber-system, this involves third-party penetration testing, system audits and system crash recovery drills. Finally effective resilience requires recognition:

- of the physical interdependencies between critical infrastructure and thus the need to work cooperatively on security with the owners/operators of other critical infrastructure;
- of the need to develop and maintain mutually supportive relationships with public agencies charged with identifying threats, countering threats, responding to emergencies, and legislating legal requirements for infrastructure protection; and
- that such interdependencies and mutually supportive relationships do and must extend

[5] Example: ISIS use of the Internet to carry out the radicalization of Canadian residents and redirection of domestic Canadian sympathizers to conduct terrorist attacks within our borders.

[6] Example: use of the Internet to carry out cyber attacks against Canadian critical infrastructure.

[7] Such as equipping the castle with its own long-range artillery and placing troops and forward positions away from the castle thus preventing an adversary from setting up its own artillery within range of the castle.

beyond borders, both provincial, state and international.

In terms of interdependencies, threats to one are threats to all. In terms of mutually supportive relationships and interdependencies, to paraphrase an old adage, no business, enterprise or undertaking in our modern world is an island. No single entity, whether the owner/operator of critical infrastructure or a government agency possesses sufficient resources to deal with threats to critical infrastructure on its own.

With respect to privately held critical infrastructure, day-to-day responsibility for security of such infrastructure is usually charged to an internal Corporate Security manager or group. However, Corporate Security is not a police force, nor a broad-based intelligence agency. Corporate Security is not considered a first responder. To access these resources the owner/operator of critical infrastructure must develop and maintain a relationship with the external entities that provide these resources. No single owner of critical infrastructure is capable on its own of effectively dealing with threats to its operations which may arise as an indirect result of an attack against the infrastructure owned by a third party supplying or providing essential services.[8] Mutual cooperation from the sharing of information to the conduct of joint security exercises is an essential resource multiplier in the creation of resilience for any single component of critical infrastructure, as well as the entire and interdependent network of such infrastructure. Viewed in these terms, security as a business function is a cooperative activity, not a competitive venture.

## III. THE INTELLIGENCE PROCESS

When developing and seeking executive approval to a security program, Security Managers may not take or be given the time to teach the executive the role and importance of information gathering, analysis and intelligence generation in developing and maintaining resilience.

It is a fundamental principle that all security measures, including the creation of resilience begins with a detailed understanding of the threat ecosystem and its evolution. Resilience must always face the threat. Anyone who has ever been in a bar fight can testify that looking the wrong way, usually ends badly. Developing and maintaining resilience, unlike theoretical physics, is not a thought exercise.

The intelligence process requires considerable and continuous dedication of resources. In addition to supporting the allocation of sufficient internal resources to this task, the executive ultimately responsible for security must understand the necessity of interdependence and cooperation with external parties, such as law enforcement and other infrastructure operators. Of all of the processes involved in creating and maintaining resilience, intelligence generation benefits the most from the afore-mentioned interdependence and cooperation.

## IV. THREATS AND INTERDEPENDENCIES

The threat environment is an ecosystem where interdependencies, connections or linkages may exist between elements within that environment. To make sense of complex systems, humans have a tendency to separate and compartmentalize the various elements of the system. In the case of the human body, we speak of the cardiovascular system at times overlooking its critical connection to the central nervous system, brainstem and endocrine system. A problem with any of these connections or interconnected systems can affect the whole. Treating a problem with one system without considering the whole interconnected network can result in ineffective treatment or worse.

Failing to understand and consider connections and interdependencies in the threat environment can lead to similar results. For example, illegal narcotics, theft and insider risks can be interconnected. An overwhelming majority of theft is driven by the use of illegal narcotics, with addicts desperately seeking to fund their

[8] The classic example is the electric generation and transmission system upon which most if not all other critical infrastructure relies upon as an essential service.

addiction. In the private sector drug programs are heavily focused on safety sensitive areas of the business. Rarely are areas critical to the business such as IT or finance considered for the application of such programs. However employees, contractors and service providers suffering from substance abuse problems may through error or intention expose the business to criminal activity such as theft of materials or information.

As our culture evolves more and more towards acceptance of recreational narcotic use, the risk of a compromised insider increases. In the case of government or the private sector, an insider compromised by substance abuse can cause as much or more damage as an external threat. Therefore, identifying and understanding elements of the threat environment which could cause or motivate an insider to compromise the business is essential to developing and implementing a security plan which will provide resilience in responding to the effects of interrelated threats.

Consider another example. Cyber security is frequently regarded as separate and apart from physical security. In many organizations cyber security is the responsibility of a group of IT specialists with limited or no connection/liaison with the individuals within the organization responsible for physical security. Cyber threats have generally been regarded as independent unrelated elements in the threat ecosystem, a creation of similarly specialized and siloed threat actors. However, as this aspect of the threat ecosystem has evolved, it has become irrevocably interconnected with threat actors seeking to use cyber attacks to cause damage in the physical world, as well as in cyberspace.

Cyber attacks have become a tool of warfare particularly valued in asymmetric conflicts. A weaker combatant, such as ISIS, will use [and indeed does use] cyber warfare to attack its enemies from afar. Attacks occurring between parties at war with one another in the physical world are not limited to military targets. Such is also the case with cyber attacks occurring as a result of such conflicts.

Closely linked with the use of cyber warfare by a remote attacker, is the use of Internet communications by a remote attacker to recruit, influence and in some cases direct the actions of domestic Lone Wolf Attackers (LWA) operating within the countries that the remote attacker is engaged in conflict with. The LWA is the ultimate insider threat. As has been the case in many LWA incidents, the individual influence to become an LWA is a vulnerable potentially unstable individual who otherwise blends into his home country's domestic society. The appearance and actions of an LWA are extremely difficult to predict and detect in advance. LWAs can appear in any organization, in either the private or public sectors [including branches of law enforcement and the military].

Ensuring resilience in a real-world security plan must accommodate and address threats that arise from linkages between multiple threat actors in the threat ecosystem. Rarely does a threat arise unconnected and distinct from other elements in this ecosystem. The leadership of an organization must be educated and helped to develop this perspective, if the corporate security manager is to receive the necessary support and resources to implement an effective security plan.

## V. CIRCLING THE WAGONS

A security plan exists to provide resilience. In its simplest terms, resilience is the ability to either with-stand or deter the actions of a threat actor or recover from/mitigate the effects of such actions. With few exceptions, security is merely one of many business functions within an organization whether in the private or public sector.

However, security is a critical function to the extent that failure to provide adequate and effective security for other critical aspects of the business can jeopardize the entire organization. This applies at both the macro and micro level. Private-sector businesses operating critical infrastructure lacking effective security risk the loss of infrastructure essential to the business. The effect of such failure, which results in a loss of critical infrastructure, can have a ripple effect negatively

impacting and damaging other private sector entities, the public locally, and possibly the nation as a whole.

The individuals charged with overseeing and managing the organization, are ultimately accountable for ensuring the security of the organization and its ability to carry out its functions. Rarely are these individuals schooled or experienced in regards to security matters. However, their approval and support is required to create and implement an effective security program. It, therefore, behooves those of us charged with responsibility to create the security plan and carry out the day-to-day implementation of the same to effectively and efficiently educate these individuals within our respective organizations regarding the essential aspects of the security plan.
This starts with the basics, with the concepts of resilience and dependencies/interdependencies with respect to critical infrastructure at the corporate, industry, regional, national and in some cases international levels. The critical role of intelligence with respect to information gathering and sharing, along with analysis to generate useful intelligence must also be stressed. The principal that security is a cooperative not a competitive activity should be emphasized. Last of all, the concept that threats exist as part of an interconnected ecosystem or threat environment must be taught.

Failing to properly educate key decision-makers regarding these foundational principles risks more than the manager of security acquiring a funny title such as "Director of Paranoia". Approval and support for the security plan and its implementation depends on the leadership of an organization having a working understanding of the principles and requirements for an effective security plan.

**Mike Chernichen is a graduate from the Faculty of Law, University of Calgary, with 38 years of experience in the Energy Sector. He is currently the Manager, Corporate Security, for a Canadian based multinational energy producer, and has been responsible for all aspects of his employer's security program since 2004.*

# *An Overview of Space Weather and Potential Impacts on Power Systems – A Canadian Perspective*

*R.A.D. Fiori, D.H. Boteler, L. Trichtchenko, L. Nikolic, H.-L. Lam, D. Danskin, L. McKee*
[1]Canadian Space Weather Forecast Centre, Natural Resources Canada, Ottawa, Ontario, Canada

*Abstract*

*Space weather, primarily due to activity on the Sun, can have impacts on Earth and space-based technologies and infrastructure including adverse effects on power systems. This is particularly true for Canada as effected regions are concentrated at Canadian latitudes. The potential threat to power systems is a driving force in developing forecasts to predict when systems are at risk. The Canadian Space Weather Forecast Centre[9] (CSWFC) of Natural Resources Canada (NRCan) is responsible for monitoring, forecasting, and reporting on space weather and space weather impacts in an effort to reduce the vulnerability of Canadian infrastructure to space weather.*

## I. Introduction

Space weather refers to a collection of physical processes resulting from solar disturbances which ultimately affect human activities on Earth and in space. Whenever severe solar disturbances occur, they have the potential to impact the Earth's magnetic field, also called the geomagnetic field, triggering geomagnetic disturbances. Geomagnetic disturbances are variations in the geomagnetic field that can last hours or days, and can directly affect activities that rely on the geomagnetic field. Geomagnetic field variations can also cause electric currents to flow in long conductors such as power systems, potentially causing damage (*Boteler*, 2001; *Boteler et al.*, 2008). Geomagnetic activity is strongest in bands called auroral ovals which surround the magnetic poles in both the northern and southern hemispheres. In the northern hemisphere the auroral oval extends across Canada. Due to Canada's location with respect to the north magnetic pole, Canada is the country most affected by space weather and geomagnetic disturbances.

[9] http://www.spaceweather.gc.ca

## II. The Sun and Solar Phenomena

To understand the space weather processes that affect power systems, it is first necessary to have a basic understanding of the Sun, which is the major source of space weather. Figure 1 shows the structures of the Sun and some of the features observed. The source of the Sun's energy is the hydrogen core which contains about half of the Sun's mass. Energy comes from the conversion of hydrogen to helium through the process of nuclear fusion. The core is surrounded by the radiation zone which emits radiation and diffuses it outward over a period of millions of years. Next is the convection zone where plasma circulates in turbulent cells. The photosphere is the visible layer of the Sun. It is only a few 100 km thick. The outermost region of the Sun, called the corona, extends millions of kilometers, but cannot be seen by the naked eye. The photosphere and corona are separated by a relatively thin layer called the chromosphere.

Like the Earth, the Sun has a magnetic field. The solar magnetic field can be very complicated, having loops and twists that vary on a wide range of time scales from seconds to hours. Figure 2a shows magnetic field lines looping out of the Sun from different active regions. These active regions appear as dark spots on the surface of the Sun called sunspots, see Figure 2b. Strong magnetic fields within the sunspot (~3000 time larger than the average solar magnetic field) inhibit convection of heat from the interior of the Sun causing the sunspot region to be about 2000K cooler than the surrounding solar photosphere. Sunspot groups are of interest because they are the source of solar eruptions and are used as an indication of solar activity.

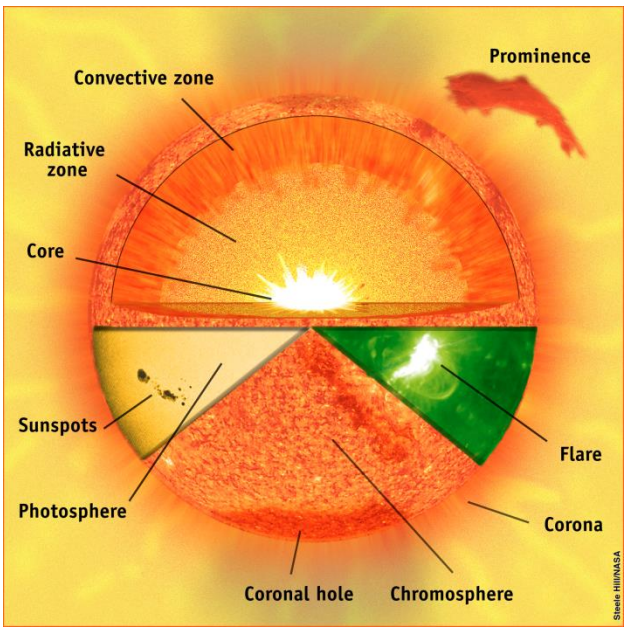


**Figure 1:** Parts of the Sun. Image courtesy of the Solar Heliospheric Observatory (SOHO). SOHO is a project of international cooperation between the U.S. National Aeronautics and Space Administration (NASA) and the European Space Agency (ESA).

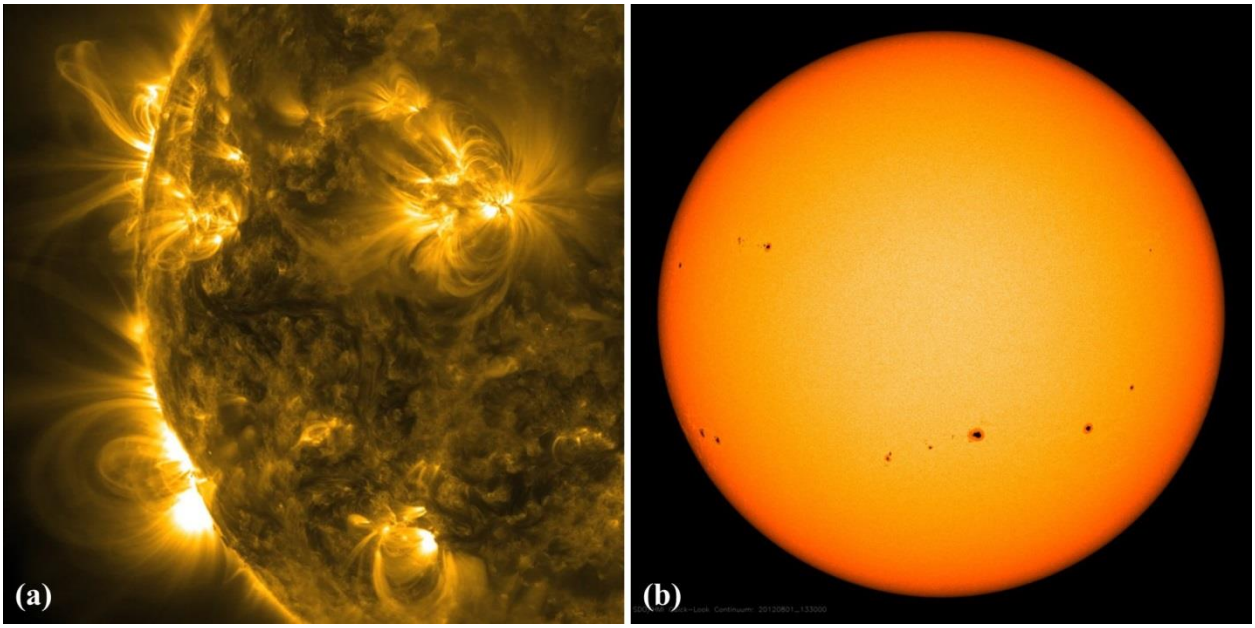


**Figure 2: (a)** Magnetic field lines looping out from active regions on the Sun viewed under ultraviolet light October, 2012. **(b)** Sunspots visible on the Sun August 1, 2012. Images courtesy of NASA and the Solar Dynamics Observatory (SDO).

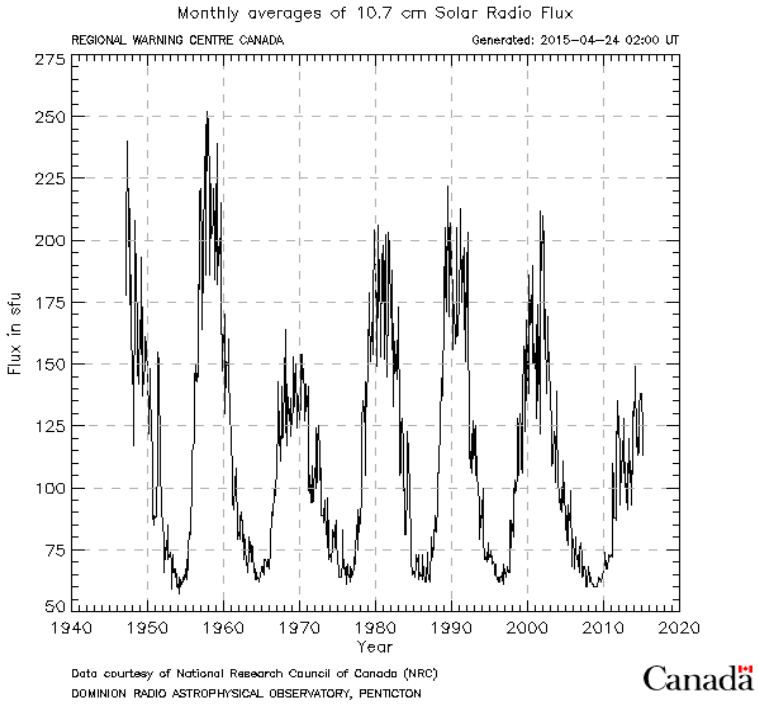


**Figure 3:** Monthly averages of the 10.7 cm solar radio flux in solar flux units (sfu). Data courtesy of the National Research Council's DRAO observatory.

The level of solar activity is monitored by counting the number of sunspots and sunspot groups on the visible solar disk (sunspot number) or by using the 10.7 cm Solar Flux index. Solar radio telescopes located at the National Research Council's Dominion Radio Astrophysical Observatory[10] (DRAO) measure the strength of 10.7cm wavelength radio emissions to create the 10.7 cm Solar Flux Index. Both the sunspot number and the 10.7 cm Solar Flux Index show that solar activity regularly varies over an 11 year cycle. (Figure 3)

Solar disturbances involve many different types of activity on the Sun. These include coronal mass ejections (CMEs), high speed solar wind streams from coronal holes, solar energetic particles (SEPs), eruptive prominences, and solar flares. Particles emanating continuously from the Sun are known as the solar wind, which carries part of the Sun's magnetic field called the interplanetary magnetic field (IMF). The solar wind and IMF interact with the geomagnetic field and outer atmosphere in complex ways, causing concentrations of energetic particles to collect and electric currents to flow in the magnetosphere[11] and ionosphere[12]. These different types of activity affect the Earth in a variety of ways, some of which lead to geomagnetic disturbances. The nature of these effects is determined by the type and strength of activity on the Sun.

Solar disturbances which have the greatest potential to create disturbances in the geomagnetic field include coronal mass ejections (CMEs) and high speed solar

[10] http://www.nrc-cnrc.gc.ca/eng/solutions/facilities/drao.html

[11] The magnetosphere is a highly dynamic region surrounding the Earth filled with various populations of charged particles, or plasma, whose motion is strongly controlled by a magnetic field.

[12] The ionosphere is a region of the Earth's upper atmosphere extending from ~60 km to 1000 km (or more) in altitude. The ionosphere is made up of ions and electrons which form a neutral plasma.

wind streams from coronal holes. CMEs have the ejections of plasma (sometimes ~10 billion tons of plasma) from the corona of the Sun. The ejected plasma carries a magnetic field. When the CME reaches the Earth 1 to 4 days after the eruption, the fast (~400 to 2000 km/s) moving dense region of particles compress the Earth's magnetosphere and the magnetic field associated with the CME particles may interconnect with the geomagnetic field leading to increased particle precipitation into the ionosphere and the production of electric currents in the magnetosphere and ionosphere. The magnetic fields associated with the ionospheric and magnetospheric currents lead to geomagnetic disturbances at the surface of the Earth. The interaction of a CME with the geomagnetic field is the main cause for large geomagnetic disturbances.

CMEs can be ejected from any part of the Sun, but only those directed toward the Earth will affect the Earth. Earth-directed CMEs (also called halo CMEs because the ejected plasma appears to form a halo around the Sun, Figure 4a) have the largest impact on most impact on the Earth because they involve huge the geomagnetic field. Partially Earth-directed CMEs (Figure 4b) deliver a partial or 'glancing' blow to the Earth and have a lesser affect. The speed of a CME is a rough indicator of how strong the effects on the Earth will be; a slow CME moving close to the background solar wind speed (300-400 km/s) will have less influence than a fast moving CME (>700 km/s).

Coronal holes are regions in the corona where magnetic field lines are open to space allowing high speed streams of plasma to escape from the Sun. These high speed streams of plasma sweep through space as the coronal holes are carried around by the rotation of the Sun. When the high speed streams arrive at the Earth they can cause long lasting (3 or 4 days) periods of disturbed geomagnetic activity, particularly in the auroral zone. High speed streams from coronal holes that are extended in solar longitude can interact with the Earth for longer periods of time. Figure 4c shows a large coronal hole located in the central visible disc.

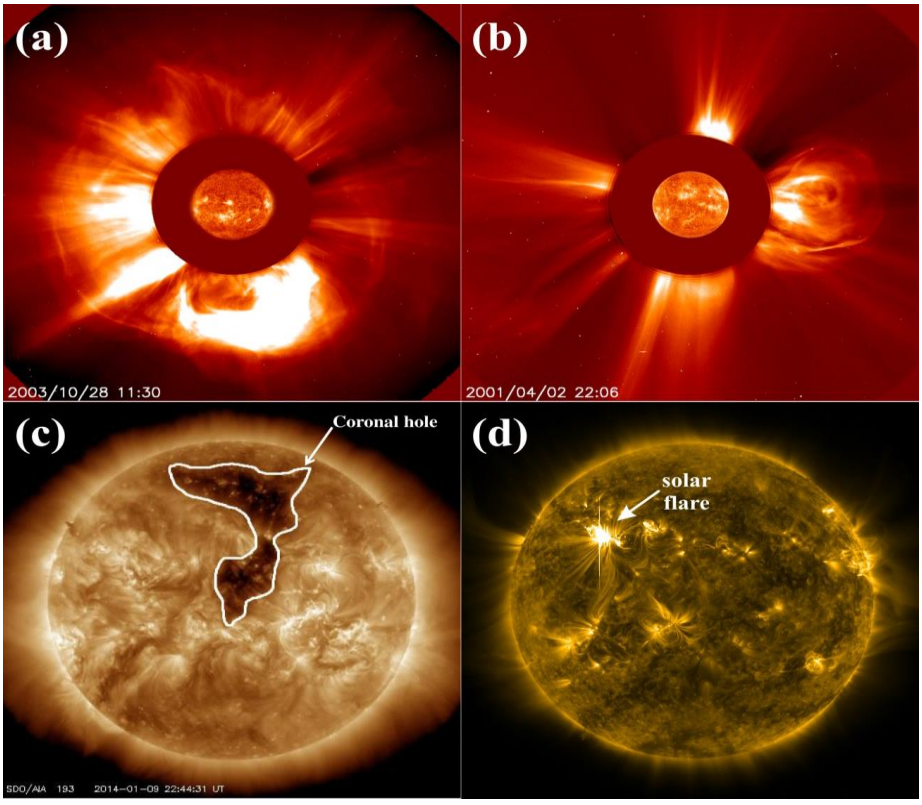


**Figure 4: (a)** Full halo CME having an Earth-directed trajectory. **(b)** CME ejected to the side of the Sun having a partially-Earth-directed trajectory. **(c)** Coronal hole. **(d)** Solar flare. Images courtesy of SOHO and SDO.

## III. Earth and the Geomagnetic Field

The geomagnetic field can be approximated by a simple bar magnet that passes through the center of the Earth at a slight inclination of 11° from the Earth's rotational axis (**Error! Reference source not found.**a). The geomagnetic field is dipolar, having two poles where the magnetic field strength is a maximum. Magnetic field lines can be thought of as coming out from the pole in the Earth's southern hemisphere, arcing around the Earth, and going into the pole in the Earth's northern hemisphere. In reality the geomagnetic field is more complex, but this description is convenient for basic understanding.

The geomagnetic field tends to shield the Earth from solar and interstellar particles. Unable to penetrate the geomagnetic field, the solar wind distorts it creating a protective magnetic cavity called the magnetosphere. The magnetosphere extends ~10 Earth radii on the dayside of the Earth and >50 Earth radii on the nightside (**Error! Reference source not found.**b). The IMF interacts with the geomagnetic field. Magnetic field lines pointing in opposite directions can interconnect in the front-side magnetosphere and be swept around into the magnetotail. When this happens, the solar wind particles can make their way into the magnetosphere. Energetic particles from the magnetosphere precipitate into the Earth's upper atmosphere to create the aurora.

Geomagnetic disturbances caused by sudden strong variations in the speed, density of the solar wind, the magnitude, or direction of the IMF result in variations of the geomagnetic field observed by magnetometers on the ground or onboard satellites orbiting the Earth. The background solar wind has a typical speed of 300-400 km/s. Speeds of >500 km/s typically indicate the arrival of CMEs or high speed solar wind streams from coronal holes. Geomagnetic disturbances are more likely when the solar wind speed is faster than background levels. Both the magnitude and polarity of the IMF influences the strength of the interaction between the IMF and the geomagnetic field which drives plasma flow both in the magnetosphere and closer to the Earth in the ionosphere. When the vertical component (perpendicular to the ecliptic plane) of the IMF (IMF $B_z$) is southward, there is a strong interaction with the geomagnetic field. Prolonged periods of southward IMF and sudden transitions from positive to negative IMF are likely to cause geomagnetic disturbances. The larger the magnitude of southward oriented IMF, the more likely geomagnetic activity will be enhanced.

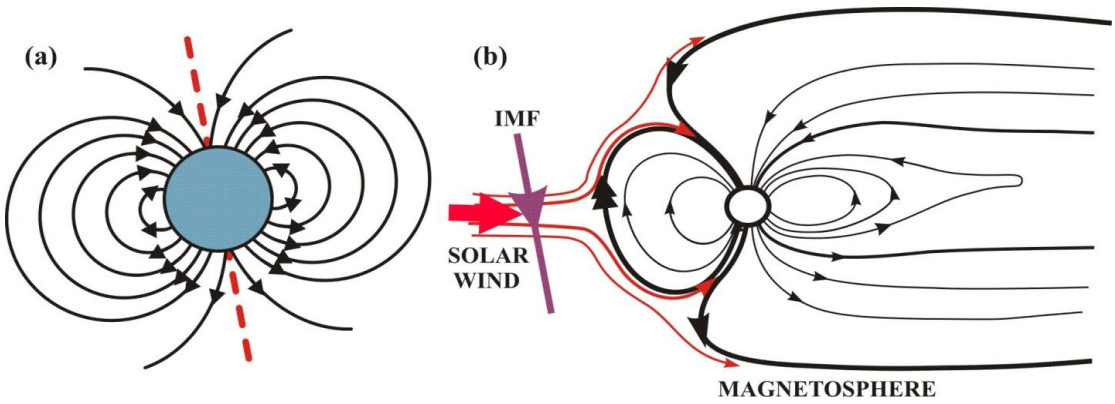


**Figure 5: (a)** The geomagnetic field can be approximated as a dipole field with magnetic field lines flowing into the Earth in the northern hemisphere and out of the Earth in the southern hemisphere. The dipole axis (red dashed line) is offset 11° from the vertical spin axis. **(b)** Cross-section of the Earth's magnetosphere. Also shown are the solar wind flow (red) and a southward oriented IMF line.

## IV. Geomagnetic Disturbances and Impacts on Power Systems

The fluctuating geomagnetic field associated with a geomagnetic disturbance causes currents to be induced in long conductors such as power transmission lines. These geomagnetically induced currents (GIC) can cause problems with the proper operation of power systems including transformer heating, tripping out of power lines, and, in worst case scenarios, even blackouts. Perhaps the most famous example is the 1989 Hydro-Québec blackout.

In March 1989, there was a series of space weather events which eventually led to a blackout of the Hydro-Québec power system. The space weather event began with an active group of sunspots that was visible from March 6-19, and was responsible for a series of X-class flares. CMEs associated with the flares that erupted on the 9$^{th}$ and 10$^{th}$ were Earth-directed and were responsible for triggering the geomagnetic activity that caused the Hydro-Québec blackout.

Geomagnetic disturbances began early in the morning of March 13, 1989. Rapid fluctuations in the geomagnetic field caused GIC in the Hydro-Québec power systems which culminated in a system-wide blackout beginning at 07:45 UT that lasted 9 hours affecting more than 6 million people (*Boteler*, 2003; *Boteler et al.*, 2008 and references therein). Many other power utilities in North America experienced problems ranging from minor voltage fluctuations to tripping out of lines and capacitors and damage to equipment.

Effective protection of power systems against potential impacts from geomagnetic disturbances requires reliable forecasting of space weather events allowing system operators time to make adjustment to mitigate adverse effects.

## V. Canadian Space Weather Forecast Centre

Space weather forecasts for Canada are provided by the Canadian Space Weather Forecast Centre (CSWFC) operated by Natural Resources Canada (*Trichtchenko et al.*, 2009; *Lam*, 2011). The CSWFC monitors, analyzes and forecasts geomagnetic activity and dispatches warnings and alerts across Canada (Figure 6). Geomagnetic activity is monitored and forecast based on data from NRCan's network of magnetometers, other ground-based and satellite-based instruments and data from other centres with instruments that monitor the Sun. Scientists look at patterns and clues in the data collected to produce a forecast. The centre also contributes to the International Space Environment Service (ISES) by providing geomagnetic data and space weather forecasts.

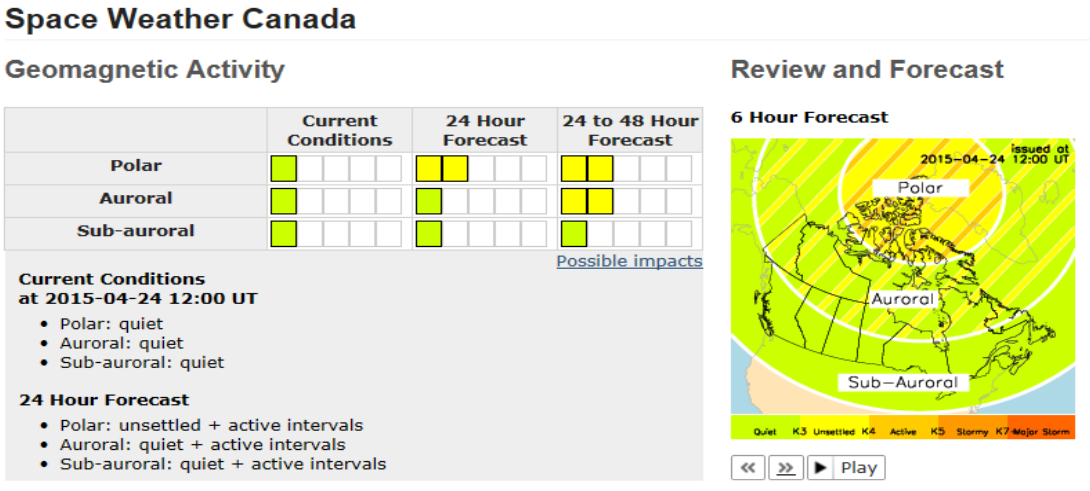


**Figure 6:** Geomagnetic activity levels are monitored and forecast by the CSWFC in three zones: polar cap, auroral, and sub-auroral.

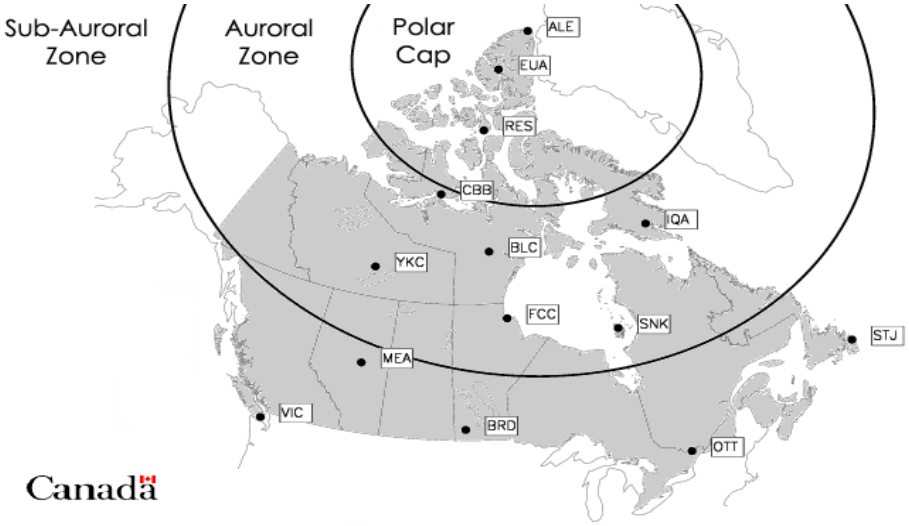


**Figure 7:** Location of NRCan magnetic observatories and the polar cap, auroral, and sub-auroral zones.

Due to the complexity of geomagnetic activity, forecasts for Canada are divided into three zones: the polar cap zone; the auroral zone; and the sub-auroral zone (Figure 6 and Figure 7). The auroral zone represents the typical location of the most frequent geomagnetic disturbances as compared to the surrounding polar and sub-auroral regions.

Geomagnetic activity level is derived from measurements made at magnetic observatories located in each zone (Figure 7). The data are processed to produce an hourly range index to characterize the range of magnetic field variations measured during one hour. Hourly range indices are divided into five activity levels classified as *quiet*, *unsettled*, *active*, *stormy*, and *major storm*[13]. Current geomagnetic activity levels and forecasted geomagnetic activity levels for the next 24 hours are provided individually for the polar cap, auroral, and sub-auroral zones in Canada.

The significance of each activity level to power systems is summarized by considering the possible impacts. *Quiet*, *unsettled*, and *active* geomagnetic activity levels are not expected to have notable impacts on power systems. Power systems in a region experiencing *stormy* geomagnetic activity levels risk the possibility of weak voltage fluctuations. Although these fluctuations are likely to be observed, they are, in general, within normal operating parameters and do not cause problems with the proper operation of the power system. It is possible that for some isolated cases, specific locations, or specific systems, fluctuations might move out of the range of what is acceptable. Power systems subject to *major storm* geomagnetic activity levels are at risk for GIC which may cause the mis-operation of protective relays and transformer heating and protective measures may be required to protect the system. Whether or not a system is impacted depends not only on the space weather conditions, but also on factors such as load level within the individual systems.

Particular attention should be paid to periods when geomagnetic activity levels are high enough to cause a *major storm watch*. A *major storm watch* is issued to indicate that *major storm* geomagnetic activity levels have been observed by multiple observatories during the same period. These conditions are likely to continue to be observed for at least the next few hours. The *major storm watch* is either limited to the auroral zone if such conditions have only been observed in that zone or applies to all of Canada if major storm

[13] Activity levels are assigned according to guidelines set by the CSWFC described at www.spaceweather.gc.ca.

conditions have been observed in both the auroral zone and the sub-auroral zone.

Geomagnetic activity conditions and forecasts and major storm watches are available at the CSWFC webpage www.spaceweather.gc.ca and on Twitter @SpaceWeatherCA.

Research at the Geomagnetic Laboratory is conducted, often in conjunction with industrial or academic partners, on a variety of topics related to geomagnetic and space weather hazards to technological systems. These include: modelling of geomagnetically induced currents in power systems; effects of telluric currents on cathodic protection of pipelines; high energy particle effects on satellites; the effects of ionospheric and geomagnetic disturbances on GNSS and radio communications, and geophysical exploration techniques.

## VI. SUMMARY

Space weather, which is ultimately driven by solar disturbances, has global impacts affecting a wide variety of technologies and critical infrastructure including power systems. Fluctuating geomagnetic fields can lead to the flow of GIC in power transmission networks. Depending on the strength of the fluctuation, GIC can cause transformer heating, the tripping out of power lines, and, in worst case scenarios, power blackouts. The Canadian Space Weather Forecast Centre (CSWFC) monitors, analyzes and forecasts geomagnetic activity in Canada for the purpose of mitigating space weather impacts on power systems.


## Acknowledgements

This work was supported by the Natural Resources Canada (Earth Sciences Sector), the Public Safety Geosciences program, and the Canadian Space Agency.


## References


Boteler, D. H. (2001), Assessment of geomagnetic hazard to power systems in Canada, Natural Hazards, 23, pp. 101-120.

Boteler, D. H. (2003), Geomagnetic hazards to conducting networks, Natural Hazards, 28, pp. 537-561.

Boteler, D. H., L. Trichtchenko, R. Pirjola, (2008), Geomagnetic effects on power systems, ASTRO 2008 conference proceedings.

Lam, H.-L. (2011), From Early Exploration to Space Weather Forecasts: Canada's Geomagnetic Odyssey, Space Weather, 9, S05004, doi:10.1029/2011SW000664.

Trichtchenko, L., H.-L. Lam, D. H. Boteler, R. L. Coles, J. Parmelee (2009), Canadian Space Weather Forecast Services, Canadian Aeronautics and Space Journal, 55 (2), pp. 107-113, doi:10.5589/q09-013.

# *Religion and Terrorism, an Association or a Requirement*

*Raynald J. Lampron* CD, MSM, RMC CPP*
Professional Security Practitioner
Associate, Infrastructure Resilience Research Group

*Abstract*

*Religion has played a role in many if not most world conflicts throughout history. During the Dark Ages and pre-Renaissance, Catholic popes were better known for their warring conquests than their religious speeches, waging cleansing wars upon the moors and other non-Christians. Religion was a founding principle of the crusades, used by both belligerents (Christian and Muslim alike) to great extent in order to rally and inspire the soldiers to fight with devotion and selflessness. Terrorism had been, and continues to be a non-conventional weapon of choice for small groups or factions, which is used in order to advance their cause. Religion has played a role in the history of terrorism, however does religion simply add value to a cause, or is it a fundamental ingredient to a successful recipe? This paper is not a dissertation on Muslim radicalism or a chronicle of current events in the Middle-East, but instead, it takes a look at the role that religion has historically played in terrorism and seeks to uncover if indeed it adds real value to a group cause or if it is simply another element in an arsenal of weapons that may be used in conjunction with the message and other violent actions of any given terrorist organization.*

## I. WHAT IS TERRORISM AND HOW IS IT DEFINED?

Terrorism has many-known faces over the ages and it keeps on evolving in its nature and the tactics it employs, even to this date. Because of the complexity associated with terrorism and the many facets it takes on, there has yet to be one overarching and fully endorsed definition. The fact that there is no universally understood and approved definition of terrorism has been a concern and a challenge for policy makers, law enforcement personnel and analysts. The definition that the Department of Defence has proposed and uses seems to offer the greatest appeal to most as it suggests a complete yet simple definition of the activities associated with terrorists their goals and intents. The Department of Defence describes terrorism as "The calculated use of unlawful violence or threat of unlawful violence to inculcate fear; intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological". The wording of this definition is of great interest to this paper as it reflects religious beliefs or goals associated with the pursuit of religious activities or ending.

The other imperative in the numerous descriptions proposed is the presence of a statement referring to the calculated violence or threats of violence, which is the means by which terrorism is conducted or delivered upon its target. Although such violence has taken many shapes and forms, which were principally driven by the available technology and delivery systems, the fundamentals of the activity remain unchanged, the use of fear and terror through death and destruction in the pursuit of a goal. The definitions of terrorism are almost as multiple as the causes, goals and "modus operandi" that defines them, therefore to properly understand and effectively fight terrorism, one must become closely acquainted with both the background and the cause of the group.

Persons and groups that are deeply dedicated to a cause will resort to great lengths and actions to advance their end, therefore the pursuit of terrorism is often, as demonstrated by the past actions of the Palestinian Liberation Organization (PLO), the Irish Republican Army (IRA) and others, set upon as a potent and definitive tool to bring their cause to the forefront. Although terrorism is often chosen as the approach of choice to bring a cause to light, is religion a mandatory element of a winning formula?

## II. EXPLORING THE ROLE THAT RELIGION PLAYS IN TERRORISM AND THE POTENTIAL VALUE ADDED IT BRINGS TO TERRORIST ORGANIZATIONS.

### *The Jewish Sacarii Sect*

During the mid-first century B.C.E., there existed a group, The Sicarii (led by descendents of Judas of

Galilee), who led a rebellious campaign against the Roman occupiers in Judea. The rebellion was ignited in great part by a census which was ordered by the Roman governor who intended to use its results to support taxation. Although the group's cause ultimately rested in the expression of freedom and self rule, a founding block of their rhetoric was anchored in a phrase by Judas who "famously proclaimed that the Jews should be ruled by God alone" (Answer.com, 2008). Following a campaign of terrorist activities by the Sicarii against the Romans that lasted several years, culminating in a full out war, the group ended its days in the mountain fortress of Masada, where at the brink of being conquered by the Roman legions, they chose to commit mass suicide instead of being captured and submitting to Roman rule and punishment. The example of the Sicarii demonstrates a commitment to a cause that was perceived to be greater than life itself. All members of the group, including their families, chose to live as outlaws, but within their faith without submitting to the tenet of an "unbeliever" ruler.

The Sicarii used the scriptures to set the tone for their movement. They claimed that the land of Judea had been given to them by God as "their promised land" after fleeing from Egypt. The scriptures were a powerful tool for the group's leadership who used their galvanizing virtue to bring together thousands of followers, including soldiers and fighters. The Sicarii's true goal was to secure independence from Roman rule; however the road they took was hampered by the refusal of the Romans to relinquish a portion of their conquest. The response of the Sicarii was to undertake a campaign of violence supported by terrorist acts, which was founded by the wish to be ruled solely by God and those who believed in God, the Jewish people. The depth of their faith was such that at the end every person ended their struggle against a foreign ruler by committing suicide.

*The Irish Republican Army*

The history of the Irish Republican Army (IRA) goes back as far as 1912 when the intent of the Third Home Rule Bill was to divide Ireland into two parts along religious boundaries. The north-east of Ireland was to be predominantly Protestant, whereas the remainder of the Island was to become a Catholic area. This partition was unacceptable for the Protestants who founded the Ulster Volunteer Force (UVF). The Catholics' reaction to this move by the Protestants was to create the Irish Volunteer Force (IVF), which would set the tone for a descendant, the IRA branches. In 1919, tired of the endless debates and discussions which were not bearing fruit or promising a United Ireland ruled by the Irish people, a group of "Irish Volunteers grew impatient and by ambushing a small army convoy near Soleheadbeg in County Tipperary, they initiated the War of Independence" (Triskelle, 2007). The tool used by the IRA and its predecessor movements was terrorism, which took the form of bombing of targets, kidnapping, assassination and numerous other violent measures.

The IRA is also known to have trained and developed many of its operatives in close connection with the Palestinian Liberation Organization (PLO), a move that solidified its knowledge of weaponry and tactics. The depth of the cross pollination between violent organizations of interest is reflected in an article proposed by Ehrenfeld (2002). Dr. R. Ehrenfeld related that **"**a British explosives expert working with the Red Cross, identified hundreds of explosive devices found there" and noted that "the pipe bombs found in Jenin are exact replicas of one's found in Northern Ireland". The incident came on the heels of a shooting spree of ten Israelis with a bolt-action rifle, perpetrated by a single sniper who left the rifle behind. This technique was also identified as an Irish Republican Army (IRA) trademark. The IRA's connections are not limited to the Middle East or the Palestinians, but extends to support of FARC activities in Colombia, for which the IRA has received at least $2 million in drug proceeds for training members of FARC" (Ehrenfeld, 2002).

The association and training reciprocity that appears to have occurred and may still be ongoing (PLO/IRA) is very interesting in itself because it involves two terrorist groups of two very different religions (Catholics and Muslims). These groups put aside

religious departure in order to support each other, most likely because they found a greater common denominator, the desire to create a nation that would be ruled by them or their representatives (Palestinians in Palestine and Irish for Ireland) without external influence. It is noteworthy to state at this juncture, that the IRA never used suicide bombers in its attacks, but there were occasions of "Proxy Bombs". During the Provisional IRA campaign 1969-1997, the IRA used the tactic it called the "proxy bomb". The proxy bomb was a sort of involuntary suicide bomb, where a victim was kidnapped and forced to drive a car bomb into its target. In one infamous operation in Derry in 1990, the IRA chained a Catholic civilian to a car laden with explosives, held his family hostage and forced him to drive to a British Army checkpoint as a "human bomb" where the bomb exploded, killing both him and five soldiers. This practice was stopped due to the revulsion it caused among the Irish nationalist community.

The IRA association with the Catholic religion is predominant and has been clearly recorded, both from outside sources, but moreover from the IRA`s own declarations and speeches. However, it is known that several active members and close associates of the group were Protestants and on rare occasions, there were also members of other creed. Although the practice has been to request that new members convert to Catholicism, this was not a firm rule and it did not prohibit joining the rank of the organization when a person has skills or attributes that are deemed necessary or valuable to the organization. The ability for non-Catholics to join the IRA and the evidence that the IRA has trained and exchanged with non-catholic terrorist organization proposes that religion is not at the heart of the cause, but instead other factors, such as politics and self-rule are more important. The case of the IRA proposes a considerable departure from religious sectarianism that is found in groups like Al Qaeda and Jihadist organizations.

Although religion was among the original factors in the conflict in Northern Ireland, it was not the definitive issue which precipitated the conflict. It could be successfully argued that the main factor behind the conflict was the fact that British settlers took over large areas of the Six Counties, dispossessing the native Irish inhabitants. The fact that the Irish were mostly Catholic and the English were Protestant probably did exacerbate the conflict, at least in the earlier years. Today, however, religion simply serves as yet another surface symbol of division that exists between the two opposing groups. Arguable, the British would in all likelihood not have been disliked any less by the Irish population if they had been Catholic, and vice versa.

*Maoist Leftist and Cuban inspired Terrorist Movements*

The next example is that of two South-American leftist terrorist groups, one a Maoist group, the Shining Path (*Sendero Luminoso*) and the other a Cuban-inspired leftist group named the Túpac Amaru Revolutionary Movement. The Shining Path's strategy "was to use violence to bring down Peru's democratic government, disrupt the economy, destroy the state's reputation among the peasantry and, ultimately, ruin its reputation among the population in general. Initially, Shining Path targeted local authorities, such as mayors, mid-level bureaucrats, police, and local political leaders. The Shining Path's momentum and remnants of the group now operate mainly in remote jungle areas. Shining Path is not sponsored by any state and has no known links to other terrorist groups. It considers itself the only remaining true communist revolutionary movement, its campaign has cost the Peruvian government over $10 billion to date" (Gregory, 2009). Neither the Shining Path nor the Túpac Amaru have any affiliation to any religious group or use religion as a motivator. Both groups are strict communists following Karl Marx's claim that religion is the opiate of the people. Neither chose to employ religion in their quest or to allow their followers to practice their faith. These two groups are purely social and political in belief and their goal is solely to overthrow the democratic government in place and replace it by a communist one in the pursuit of a socialist state.

*Osama Bin Laden and Al Qaeda*

Osama Bin Laden is a former Central Intelligence Agency (CIA) trained Mujahedeen who was recruited in the 1980s in order to fight the Russian occupation of Afghanistan. The Centre for research on Globalization (CRG) informs the reader that "In March 1985, President Reagan signed National Security Decision Directive 166,...[which] authorize[d] stepped-up covert military aid to the Mujahedeen, and it made clear that the secret Afghan war had a new goal: to defeat Soviet troops in Afghanistan through covert action and encourage a Soviet withdrawal. The new covert U.S. assistance began with a dramatic increase in arms supplies -- a steady rise to 65,000 tons annually by 1987, ... as well as a "ceaseless stream" of CIA and Pentagon specialists who traveled to the secret headquarters of Pakistan's ISI on the main road near Rawalpindi, Pakistan. There the CIA specialists met with Pakistani intelligence officers to help plan operations for the Afghan rebels" (CRG, 2001). The Mujahedeen were called upon to help fight the incursion of the Russian forces in Afghanistan, an invasion force lead by the Soviet Union and its Warsaw pact allies that threatened to increase of the span of the communist sphere of influence in the Middle-East, thus potentially creating an important shift in the geopolitics of the region. As part of the American counter communist strategy, some U.S. agencies under the direction of the leadership chose allies in countries of interest to foster democracy and align them to the political thinking and toward allegiance to the West. For those countries that had already fallen under the communist influence, greater efforts, including the use of force to a varying degree had to be used. The U.S. and its NATO allies had to be careful in their efforts depending on the Nation or Regions of interest, as this time was one of great peril as the world remained in the depth of the cold war. One prime example of a country that went from a democratic system to anarchy due to civil war, which once weakened by war and disorder was quickly invaded by the Soviet Union who wanted to expend their influence in the region. This move and shift in the balance of power could not be allowed and, therefore, much had to be done to reverse this communist tide.

The Central Intelligence Agency, through the Pakistani intelligence, service played a key role in training the Mujahedeen in the art of guerrilla warfare. However, psychology also played a role in radicalizing the fighters, by introducing the idea that "Islam was a complete socio-political ideology, that holy Islam was being violated by the atheistic Soviet troops, and that the Islamic people of Afghanistan should reassert their independence by overthrowing the leftist Afghan regime propped up by Moscow" (CRG, 2001). One must be fair, however, and state that the usage of religion as a reliable and inspirational tool is not a new phenomenon that was created by the CIA or its allies. They simply used an already proven and "winning" formula to advance their goal and cause, which is to reverse the tide of communism, in the same manner that many others had done before them. The usage of this militant strategy had unforeseen consequences, which beyond the empowerment of the Mujahedeen fighters in their quests to liberate Afghanistan from Russia, later transitioned into a liberation movement against all Christians and the Neo-Crusader invader, that is the radicalization of Muslims fighter against the presence or influence of all non-believers on Muslim soil.

Al-Qaeda is certainly the most active and lethal terrorist group of the 20th and 21st century, and it is possibly the worst throughout history. Al Qaeda has used, and continues to use propaganda, religion and sympathetic clerics to invigorate its fight against the West. The primary recruiting and support tool of Al-Qaeda is religious belief. The totality of their mission and drive is to make the world Muslim as God's anointed people and to destroy the Jewish State (Zion**)** and its people along with the West (Christian world), especially the United States as the great Satan they claim and possibly truly perceive it to be. For Osama Bin Laden, Al Qaeda and the Jihadist movement, religion is not only a motivator and a binding agent; it is the founding block of their quest and the sole purpose of their "raison d'être".

In the above cases, it is easy to correlate the importance that religion played in the cause of the Sicariis, the crucial role it plays for Al Qaeda and the Jihadist movement and, to an extent, the IRA. However, religion played no role in either the Túpac Amaru or the Shining Path movement or in the manner by which they advanced their cause and recruited their followers. Instead these latter two groups chose to irradiate religion from the movement and to base their strength on comradeship and brotherhood. Religion is certainly a powerful medium and a great cohesive agent that unites people; however, it is not an imperative as seen in the above example for the creation of a successful and lasting terrorist movement. This being said, there remains one important question to be asked: Is religion an imperative in suicide terrorism, or will followers kill themselves in the name of the cause alone?

## III. IS RELIGION AN IMPERATIVE FOR SUICIDE TERRORISM?

There are many reasons to go to war; most of us will willingly give up our life if the quest is deemed rightful, as was done in the First and Second World War and many others that our leaders have deemed necessary to fight. The western world used the principles of the *Right to wage war Cause* (Jus ad Bellum) and that of *Justice in war* (Just in Bello) to decide if our nation would go to war or not and what is permitted both as per the article of war and what is entered in the rules of engagement. This has not always been so, for example during the Antiquities and the Dark Ages and even Post Renaissance, the desire to enlarge one's empire or the quest for imperialism was often the basis for waging war. War was also waged for religious purposes such as the crusades or the wish to reclaim lost territory from the Muslims (Spain from the Moors). The conflicts that I have referred to so far have all been deemed to be just in their own way and interpretation, often with the support of the religious cleric, claiming them to be in support of the will of God. Even the American Revolution was a conflict where religion played a role, although minimalistic; John Witherspoon stated, in an effort to inspire, that for the revolution to work, it had to be blessed by God.

All soldiers accept that they may be called upon to make the ultimate sacrifice, however every soldier enters a conflict with the hope to survive and see peace being restored. Suicide bombing, however, guarantees that the perpetrator will make the ultimate sacrifice, and that in itself is an unnatural act for any person in their right frame of mind. Therefore, there has to be a great depth of belief and conviction, that it be a cause, religion or a code of ethics, in order for a person to accept certain death as part of their duty to the cause. There are two groups that immediately come to mind when one thinks of suicide bombers or soldiers, the Japanese Kamikaze and the Islamist suicide squads, however there are more examples.

The Japanese Kamikazes were members of a revered order who upon completing suicide attacks upon the enemy became instant heroes of the nation, while also making their family the envy of the community. Kamikazes followed an in-depth ritual before launching onto their quest; however the ritual was not religious in nature, but instead symbolic of their determination and devotion to the emperor. Although it could be debated that the devotion to the emperor was based on the fact that the emperor was divinely installed upon the throne of Japan, the honor code of the Japanese soldier (bushido) did not address religion, but addressed duties to the nation and the emperor instead. It is clear that religion was not a factor of importance in the decision of the Kamikazes to give their life for the cause and the emperor.

The other group of interest to this paper is the Islamist suicide squad. These people blow themselves up in the name of Jihad and therefore for the greatness of Islam as ordained by God. The Qur'an states suicide is a mortal sin. However, the interpretation of some clerics and Ayatollahs state that a soldier of Allah can, in the defense of the faith, commit suicide to kill infidels. Hoffman (2006) state there are "four essentials motivations that justify such attacks: seeking for Martyrdom, Hurting the enemy, Encouraging Muslims and Weakening the spirit of the enemy...

[which] clearly demonstrate that the Islamic-Bombing assault or the martyrdom is legitimate as it is within the framework of Islam" (p. 160 of Hoffman, 2006). There is a need for religion to play a crucial role in Islamic suicide terrorism. Otherwise, the action of killing oneself would become offensive to God and therefore a mortal sin. The indoctrination of Jihadist begins in some cases at a very young age whereby the children are taught to hate both Jews and Westerners (all infidels to say the least) and to desire to devote and even donate their lives to Jihad in the name and to the glory of Allah. Recruiting also takes place in refugee camps and other areas where people are poor, displaced and often orphaned by the actions of the Israeli or Western powers through conflict and therefore filled with anger and a desire for revenge. These recruits are willing to perform acts of violence, but to reach the threshold of suicide there needs to be a deep conviction which is addressed through religious zeal and teachings. The motivator for Muslim extremists to commit suicide while taking out a target chosen by their leader in religion, along with the promise of redemption for all sins committed on earth and the quasi "free" passage to heaven with associated benefits and the status of martyr.

There were also a number of other groups whose members committed suicide in order to achieve their aim. For example, Tsar Alexander II was killed by a member of Narodnaya Volya, Ignacy Hryniewiecki, who died while intentionally exploding a bomb during the attack. During the Second World War, Rudolf Christoph Freiherr von Gersdorff intended to assassinate Adolf Hitler by a suicide bomb in 1943, but was unable to complete the attack. Furthermore, following World War II, Viet Minh "death volunteers" fought against the French Colonial Forces in Vietnam by using a long stick-like explosive to destroy French tanks. All the above examples of suicide bombings were not inspired by religious belief, but instead by their great depth of conviction into their political cause.

## IV. Conclusion

Religion is a fundamental need of human beings. Religion helps us define who we are. It provides a moral compass for the masses and provides ethical guidance with regard to our daily encounter and exchanges with our fellow man and creature. Religion has also been used as a tool of war instead of the instrument of peace that it is arguably meant to be.

Many have used religion to entice other persons to follow them along a specific path, which for good or bad often leads to an obsession and surrendering of all power to the leader. Modern examples of such religious control could be found in the Davidian Sect of Waco, the new world of Jonestown, or the follower of the Aum sect. However, even though religion is a great galvanizer of people, all sects and leaders do not necessarily need religion. The followers of Mao Tse-Tung were fully organized, engaged and zealous, yet communism and comradeship was their cause and religion played no place; religion was abolished and banned by the party and by law.

Terrorism is an ancient tool of war. Terrorists, as for all other groups or sub-culture, have always needed a gelling element for recruitment. This gelling element validates their intent and approach in order to attract and maintain followers, and provides them with a cause to believe in and rally to. Conventional terrorism has often used religion as this gelling agent; this is reflected in History. However, there are many examples of zeal and dedication which are based in politics, leadership or culture rather than religion. This brings me to the point of suicide terrorism, which is a great departure from planting a bomb somewhere to kill the "enemy", it means killing oneself. Because killing oneself is seen in many religions as a sin against God, many have come to believe that the sin is justified if performed for the sake and protection of the religion and its people. There is no doubt that securing the help of a cleric or even a great religious leader, who will claim that death in the service of the deity they believe in is not a sin, but the ultimate sign of dedication will work wonders on people. However, is it really necessary?

The most prolific pre-Al Qaeda terrorist group and user of suicide bombers was the Liberation Tigers of Tamil Eelam, a Marxist-Leninist group that sought independence from Sri Lanka. This group used the desire for self-rule to recruit and indoctrinate followers; religion did not play any role for this organization. Instead the cause (self-rule in a country of their own) and the alleged harassment and abuse by the Sri Lankan government removed all fear and ethical barriers from the devotees who gave their lives so that others could leave in peace.

Nearly all recent suicide attacks are made by Islamists, and it would appear that religion and terrorism have created an almost symbiotic relationship, especially when it comes to radical jihadists, such as Al Qaeda, ISIS, Boko Haram and and other more radical and fundamentalist groups. However, I would like to state that although religion is a great motivator, I have proven that it is not a fundamental requirement to the formula. It is easily conceded that religion is an obvious choice for many Organizations and it readily galvanizes people while dividing others along its line, but to believe that it is the basis of terrorism would be a great mistake and lead to a potentially bloody conflict, once again waged on a misunderstanding of culture and history. Obviously, there has to exist a great motivator in order for someone to take another life, and an ever greater one to push someone to give their life in order to take other lives in return.

**Raynald J. Lampron is a member of the Federal Public Service Executive's Team at the Director level in Ottawa. Previously, he was Chief of Security and Emergency Operations, Natural Resources Canada with primary responsibilities for physical security, policies and governance, health and safety, facility emergency response. He spent over 27 years in the Canadian Armed Forces as team leader, Sensitive Investigations Unit, Human Intelligence Operations, and Force Protection both within Canada and Foreign theater of operations; with United Nations, NATO and Department of Foreign Affairs.*

*His final military duty was Wing Provost Marshal, 19 Wing, Comox, British Columbia.*

*He continues his military journey as a reservist, Brockville Rifles, Canadian Armed Forces, as Officer Commanding Administration, and legal and disciplinary Advisor to the Commanding Officer.*

*Mr. Lampron holds a Bachelor of Arts, Psychology and Political Science from the Royal Military College of Canada and a Masters in Security Managements (Hons.) from the American Military University. He is also a long standing member of the American Society of Industrial Security (ASIS International) and holds the prestigious ASIS Certified Security Professional Certification.*

## References

About.com. (2009). Department of defense definition of terrorism Retrieved 8 December 2010 from http://terrorism.about.com/od/whatisterroris1/ss/DefineTerrorism_4.htm

Answer.com. (2008). Is religion the only factor in the conflict in Ireland . Retrieved 8 December 2010 from http://wiki.answers.com/Q/Is_religion_the_only_factor_in_the_conflict_in_Ireland#ixzzl7ju5aVQc

CRG, (2001). Who is Osama Bin Laden. Retrieved 13 December 2010 from http://www.globalresearch.ca/articles/CHO109C.html

Ehrenfeld, R. (2002). IRA + PLO. Retrieved 11 December 2010 from http://www.analyst-network.com/article.php?art_id=637

Gregory. K. (2009). Shining Path and the Tupac Amaru, Peru leftist. Retrieved 20 December 2010 from CFR.org http://www.cfr.org/publication/9276/shining_path_tupac_amaru_peru_leftists.html

Hoffman, B. (2006). *Inside Terrorism*. Columbia University Press: New York.

Triskelle.eu. (2007). Irish republican Army. Retrieved 12 December 2010 from http://www.triskelle.eu/history/irishrepublicanarmy.php

Zalman. A. (2010) *Sacarii: first century terrorists*. Retrieved 7 December 2010 from http://terrorism.about.com/od/groupsleader1/p/Sicarii.htm

# *Recommended Critical Infrastructure Security and Resilience Readings*

*Felix Kwamena, Ph.D.**

**"An Obligation to Act: Holding Government Accountable for Critical Infrastructure Cyber Security"** by Jacques J.M. Shore, 11 March 2015, International Journal of Intelligence and CounterIntelligence 28: 236-251, 2015.

**"Measuring the Resilience of Energy Distribution Systems***"* by Willis, Henry H. and Kathleen Loa. Measuring the Resilience of Energy Distribution Systems. Santa Monica, CA: RAND Corporation, 2015.
http://www.rand.org/pubs/research_reports/RR883.html

**"Canadian Security Intelligence Service, Public Report 2013-2014**"
https://www.csis.gc.ca/pblctns/nnlrprt/2013-2014/index-en.php

**"The Saudi Connection: Wahhabism and Global Jihad"** by Carol E. B. Choksy & Jamsheed K. Choksy' World Affairs [USA], May/June 2015
http://www.worldaffairsjournal.org/article/saudi-connection-wahhabism-and-global-jihad

"**India to sign port deal with Iran, ignoring U.S. warning against haste"** by Nidhi Verma & Manoj Kumar, Reuters, 5 May 2015
http://www.reuters.com/article/2015/05/05/us-india-iran-port-idUSKBN0NQ0WT20150505

**"Saudi Aramco announces major shake-up, Nasser named acting CEO Deputy Crown Prince Mohammed Bin Salman named chairman of new supreme council of the Saudi state oil company"** by Wael Mahdi, Asharq Alawsat, 3 May 2015
http://www.aawsat.net/2015/05/article55343247/saudi-aramco-announces-major-shake-up-nasser-named-acting-ceo

**"The Growing Cyberthreat from Iran, the Initial Report of Projectpistachio Harvest"** by Frederick W. Kagan and Tommy Stiansen, April 2015
AMERICAN ENTERPRISE INSTITUTE
CRITICAL THREATS PROJECT AND NORSE CORPORATION

**"The Islamic State's Expansion in Libya"** by Andrew Engel . Policy Watch 2371
http://www.washingtoninstitute.org/policy-analysis/view/the-islamic-states-expansion-in-libya

**"Arab Futures. Three Scenarios for 2025"**
Edited by Florence Gaub & Alecandra Laban, European Union - Institute for Security Studies, Report # 22, February 2015

**"Has Successful Terror Gone to Ground?"** by **Arnold Barnett,** Risk Analysis, 2015, Society for Risk Analysis**, http://www.sra.org/**

**"Fact Sheet Iranian Regional Hegemony"**
Prepared by Clarion Project Research Fellow Elliot Friedland, April 2015
http://www.clarionproject.org/sites/default/files/Iranian-Regional-Hegemony.pdf

**"Assessing the educational needs of emergency management personnel"** by Kelly Brown, *Journal of Homeland Security Education, Vol. 4*, Issue 1 (2015)
http://www.journalhse.org/v4-brown.html

**“Solar Super-Storms “Inevitable”: Scientists”** Homeland Security News Wire, [USA}, 13 August 2014 http://www.homelandsecuritynewswire.com/dr20140813-solar-superstorms-inevitable-scientists

**“China's cyberpower: International and Domestic Priorities”** by James A. Lewis and Simon Hansen, Australian Strategic Policy Institute [Australia], 12November 2014 https://www.aspi.org.au/publications/chinas-cyberpower-international-and-domestic-priorities

**“Stuxnet-style malware 'developed by Western intelligence agency' uncovered in Russia and Saudi Arabia”** By Graeme Burton http://www.computing.co.uk/ctg/news/2383065/stuxnet-style-malware-developed-by-western-intelligence-agency-uncovered-in-russia-and-saudi-arabia

***“Regin - Top Tier Espionage Tool,* Enables Stealthy Surveillance, Symantec Security”** Response, Volume 1.0 November 24, 2014, http://symantec.com/security_response/

**"The Evolving U.S. Cybersecurity Doctrine"** by Derek Johanson *Security Index: A Russian Journal on International Security*, Vol. 19, Issue 4, (2013) http://www.tandfonline.com/doi/full/10.1080/19934270.2013.846072#.VFQLWVc08SU

**"Organised Crime and the Internet,"** by Peter Grabosky*The RUSI Journal*, Vol. 158, Issue 5 (2013 http://www.tandfonline.com/doi/full/10.1080/03071847.2013.847707#.VFQG41c08SU

**“Concerns About Risk Confronting Boards – Fifth Annual Board of Directors Survey 2014”** by Eisner Amper, www.eisneramper.com

**“Survey: Cybersecurity Is Keeping More Corporate Directors Up At Night”** by Jason Bramwell, Accounting Web [USA] 24 July 2014, http://www.accountingweb.com/article/survey-cybersecurity-keeping-more-corporate-directors-night/223660

**“After the Breach: Cybersecurity Liability Risk”** by Judith H. Germano and Zachary K. Goldman, The Centre On Law and Security, NYU School of Law 2014. http://www.lawandsecurity.org/Portals/0/Documents/CLS%20After%20the%20Breach%20Final.pdf

**“Critical Infrastructure: Security Preparedness and Maturity”** Sponsored by Unisys Independently conducted by Ponemon Institute LLC July 2014 http://www.unisys.com/unisys/news/spotlight.jsp?id=1120000970029010176

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