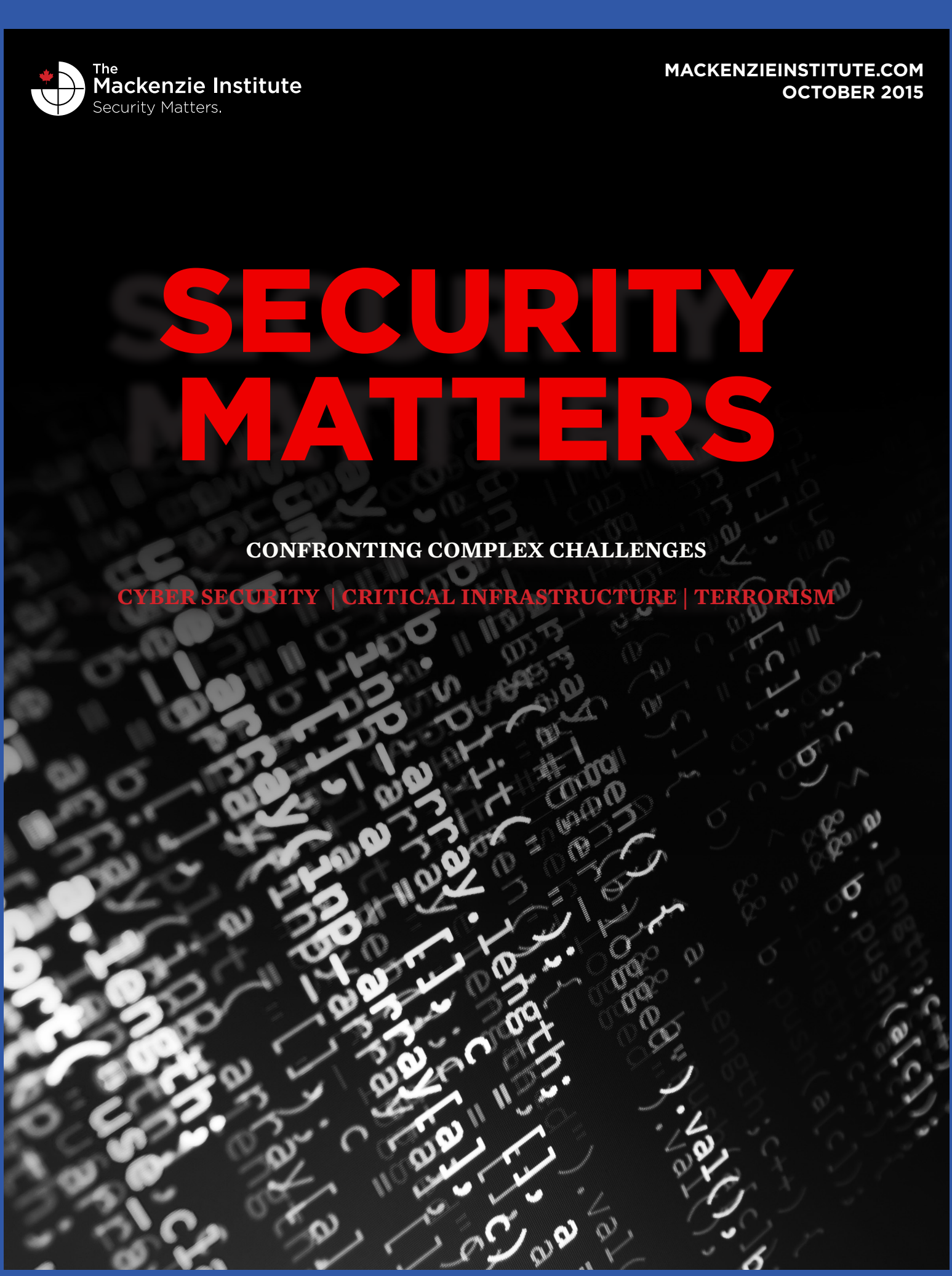
The Mackenzie Institute
Security Matters.

MACKENZIEINSTITUTE.COM
OCTOBER 2015

SECURITY MATTERS

CONFRONTING COMPLEX CHALLENGES

CYBER SECURITY | CRITICAL INFRASTRUCTURE | TERRORISM



The Mackenzie Institute works to be the conscience of the security field

The Mackenzie Institute, an independent think tank, brings a strategic and pragmatic approach to security matters that affect both domestic and global audiences. It is a globally recognized Canadian-based public policy institute for research and comment on issues impacting political and social stability, specifically terrorism, organized violence, and security.

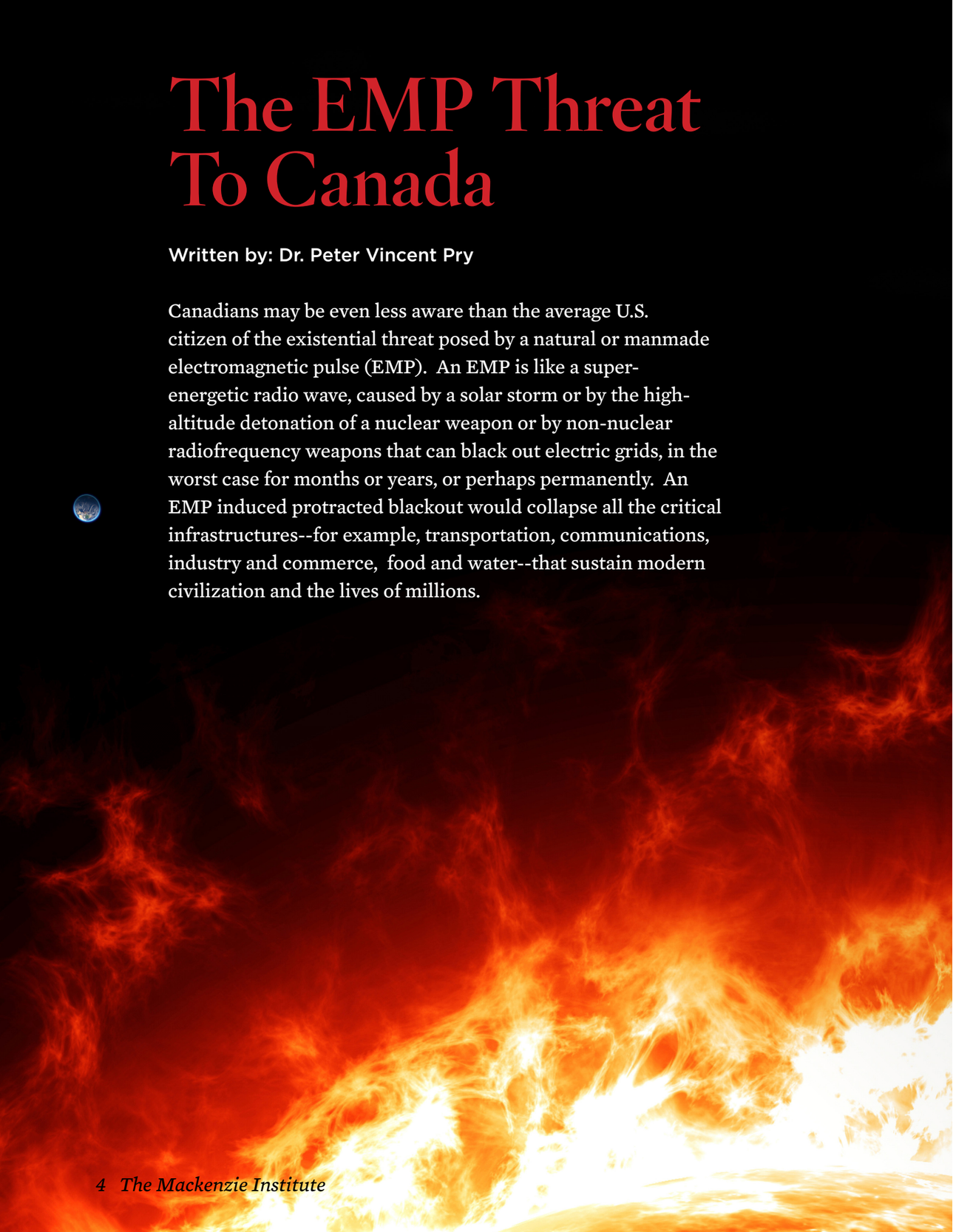
For more information or additional copies of this publication, please contact:
The Mackenzie Institute
PO Box 338, Adelaide Station
Toronto, ON M5C2J4
416-686-4063
www.mackenzieinstitute.com

Contents

The EMP Threat To Canada

Written by: Dr. Peter Vincent Pry

Canadians may be even less aware than the average U.S. citizen of the existential threat posed by a natural or manmade electromagnetic pulse (EMP). An EMP is like a super-energetic radio wave, caused by a solar storm or by the high-altitude detonation of a nuclear weapon or by non-nuclear radiofrequency weapons that can black out electric grids, in the worst case for months or years, or perhaps permanently. An EMP induced protracted blackout would collapse all the critical infrastructures--for example, transportation, communications, industry and commerce, food and water--that sustain modern civilization and the lives of millions.



The U.S. Congressional EMP Commission estimated that a nationwide blackout lasting one year could kill up to 9 of 10 Americans by starvation, disease and societal collapse. Canada, unlike the United States, is not usually thought of as the primary target for attack by terrorists, Iran, North Korea, China or Russia. But where EMP is concerned, Canada and the U.S. are in the same boat, because they are literally wired together, both nations living off of the North American Power Grid.

Moreover, Canada has some unique characteristics that make it potentially more vulnerable to EMP than the United States, yet also more easily protected.

Natural EMP

The sun can cause a natural EMP, called by electric utilities, a Geo-Magnetic Disturbance (GMD). Coronal mass ejections traveling over one million miles per hour strike the Earth's magnetosphere, generating geomagnetic storms every year. Usually these geo-storms are confined to nations at high northern latitudes and are not powerful enough to have catastrophic consequences.

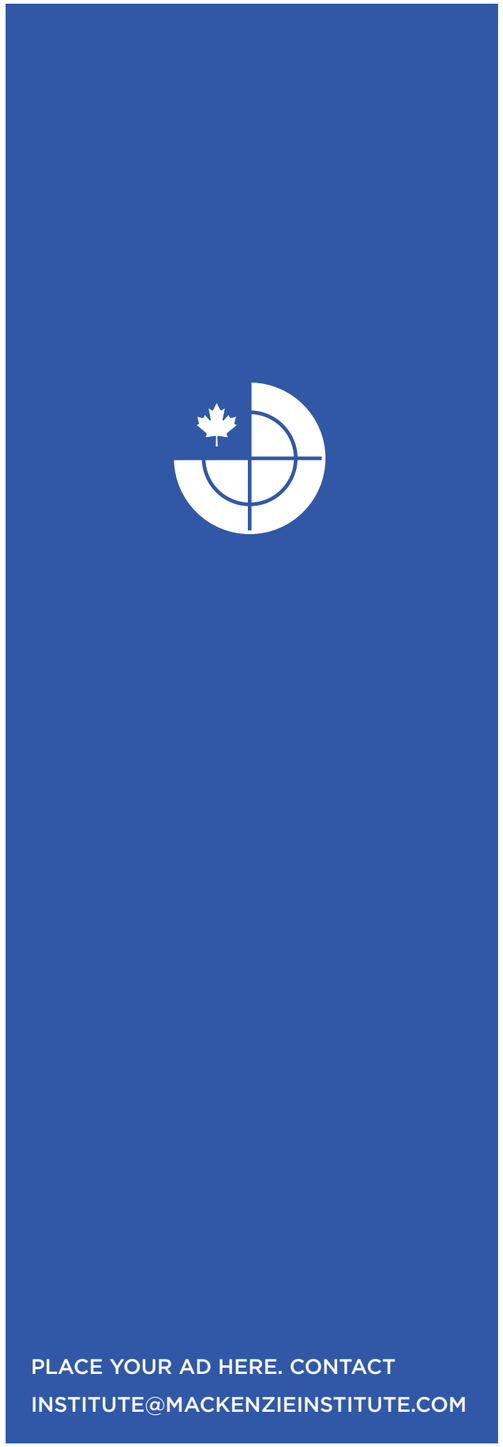
Canada is more susceptible than the United States to natural EMPs or GMDs because it is located at a higher northern latitude, where geomagnetic storms are more common. In 1989, natural EMP from the Hydro-Quebec Geo-Storm blacked-out half of Canada for a day causing economic losses amounting to billions of dollars.

Most worrisome is the rare solar super-storm, like the 1921 Railroad Storm, which happened before civilization became dependent for survival upon electricity. The U.S. National Academy of Sciences estimates that if the Railroad Storm were to recur today, there would be a blackout of the North American grid with recovery requiring 4-10 years, if recovery were possible at all.

The most powerful geomagnetic storm on record is the 1859 Carrington Event. Carrington was a worldwide phenomenon, causing forest fires from flaring telegraph lines, burning telegraph stations, and destroying the just laid intercontinental telegraph cable at the bottom of the Atlantic Ocean.

If a solar super-storm like the Carrington Event recurred today, it would collapse electric grids and life-sustaining critical infrastructures worldwide, putting at risk the lives of billions.

The U.S. National Aeronautics and Space Administration (NASA) in July 2014 reported that two years earlier, on July 23, 2012, the Earth narrowly escaped another Carrington Event. A Carrington-class coronal mass ejection crossed the path of the Earth, missing the planet



by just three days. NASA assesses that the resulting geomagnetic storm would have had catastrophic consequences worldwide.

Recurrence of another Carrington Event, expected roughly once every 100-200 years, is overdue. NASA estimates the likelihood of such a geomagnetic super-storm is 12 percent per decade. This virtually guarantees that Earth will experience a catastrophic geomagnetic super-storm within our lifetime or that of our children.

Radio-Frequency Weapons

Radio-Frequency Weapons (RFWs) are much less powerful than nuclear weapons and much more localized in their effects, usually having a range of one kilometer or less. Terrorists, criminals, and even disgruntled individuals have already made localized EMP attacks using RFWs in Europe and Asia. Probably sooner rather than later, the RFW threat will come to North America.

Reportedly, according to the Wall Street Journal (March 12, 2014), a study by the U.S. Federal Energy Regulatory Commission warns that a terrorist attack that destroys just 9 key extra-high voltage (EHV) transformer substations (out of a total of 2,000) could cause a nationwide blackout of the United States lasting 18 months.

Canada is probably more vulnerable than the U.S. to nationwide blackout by Radio-Frequency Weapons, because Canada has many fewer EHV transformer substations. Accordingly, an attack on fewer substations may more easily trigger a chain reaction of cascading failures that overwhelms all or most of the EHV transformers, causing a rolling blackout that engulfs the whole of Canada.

RFWs can also pose a significant threat to nuclear reactors by damaging control systems that could conceivably, in a worst case scenario, result in a meltdown of fuel rods in cooling ponds or within the nuclear reactor itself. Steam explosions and the release of radioactive contamination could result, as happened with the nuclear reactors in Fukushima, Japan, because they were blacked-out for several days, with no electricity to drive cooling pumps, following a tsunami.

Canada has 18 nuclear power reactors at three locations. All of these are in the east, located near major population centres.

Canada has 18 nuclear power reactors at three locations. All of these are in the east, located near major population centres. Radioactive contamination from fuel rods undergoing meltdown will follow prevailing winds and weather patterns--in the case of the Canadian reactors the weather moves eastward over populous areas--creating radioactive plumes covering potentially thousands of inhabited square miles.

According to the U.S. 9/11 Commission Report, one of the targets originally considered for attack by jetliner on September 11, 2001 was a U.S. nuclear reactor.

Canada is no stranger to terrorist plots against the power grid and nuclear reactors. In August 2003, the Royal Canadian Mounted Police arrested 19 suspected terrorists in Toronto, some of whom allegedly conducted ground reconnaissance against Canada's Pickering nuclear reactor and also conducted flight training, overflying Pickering.

Months before the Toronto arrests, a reliable source with information on Iran's support of international terrorism,

alleged there was a terror cell in Toronto planning to hijack a jet to crash into the Seabrook nuclear reactor, located about 40 miles north of Boston. The plotters allegedly hoped to create a radioactive plume that would contaminate New England. This alleged plot, that might have been part of a more ambitious "12th Imam Operation" meant to eclipse and surpass in destruction the 9/11 attacks, is detailed in the book "Countdown To Terror" by then Rep. Curt Weldon. Weldon was Vice Chairman of both the House Armed Services Committee and the House Homeland Security Committee in the U.S. Congress.

Canada's "homegrown" terrorists who might think about attacking the power grid could get help from their nearby U.S. counterparts in Minneapolis, Minnesota and Buffalo, New York that are known recruiting grounds for terrorists. Radio-frequency weapons might well become the weapon of choice for terrorists, instead of hijacked jetliners, for attacking nuclear reactors and power grids, if only because they are easier to obtain. They can be built by an individual with some knowledge of electronics, using design information available on the internet, and parts available from any electronics store. Powerful EMP generators, intended for industrial use as a diagnostic tool, but useable as a weapon of mass destruction, can be purchased mail order by anyone.

RFWs offer significant advantages over guns, bombs, or crashed jetliners for attacking electric grids. EMP fields can cause widespread damage of electronics, so precision targeting is much less necessary. And unlike damage from guns, bombs, or a crashed jet, an attack by RFWs is much less conspicuous, and may even be misconstrued as an unusual accident arising from faulty components and systemic failure.

Some documented examples of successful attacks using radio-frequency weapons, and accidents involving electromagnetic transients, are described in the U.S. Department of Defense "Pocket Guide for Security Procedures and Protocols for Mitigating Radio Frequency Threats" (Technical Support Working Group, Directed Energy Technical Office, Dahlgren Naval Surface Warfare Center):

"In the Netherlands, an individual disrupted a local bank's computer network because he was turned down for a loan. He constructed a Radio Frequency Weapon the size of a briefcase, which he learned how to build from the Internet. Bank officials did not even realize that they had been attacked or what had happened until long after the event."

"In Russia, Chechen rebels used a Radio Frequency Weapon to defeat a Russian security system and gain access to a controlled area."

"In the late 1980s, a large explosion occurred at a 36-inch diameter natural gas pipeline in the Netherlands. A SCADA system, located about one mile from the naval port of Den Helder, was affected by a naval radar. The RF energy from the radar caused the SCADA system to open and close a large gas flow-control valve at the radar scan frequency, resulting in pressure waves that traveled down the pipe and eventually caused the pipeline to explode."

"North Korea used a Radio-Frequency Weapon, purchased from Russia, to attack airliners and impose an "electromagnetic blockade" on air traffic to Seoul, South Korea's capitol. The repeated attacks by RFW also disrupted communications and the operation of automobiles in several South Korean cities in December 2010; March 9, 2011; and April-May 2012 as reported in "Massive GPS Jamming Attack By North Korea"
(GPSWORLD.COM, May 8, 2012).

Nuclear EMP

The EMP Commission found that virtually any nuclear weapon--even a primitive, low-yield atomic bomb such as terrorists might build--would suffice to make a catastrophic EMP attack. The electric grid and other civilian critical infrastructures have never been hardened to survive EMP.

The iconic EMP attack detonates a single warhead about 300-500 kilometres high over the centre of the U.S., generating an EMP field over all 48 contiguous United States. Such an EMP attack could be made by a missile or nuclear-armed satellite. North Korea and Iran have both apparently practiced this scenario, orbiting satellites on the optimum trajectories and altitudes to evade U.S. National Missile Defenses and, if the satellites carried a nuclear weapon, make an EMP attack.

Canada would also be affected by this iconic EMP scenario. A nuclear warhead burst 300-500 kilometres high over the centre of the U.S. will cover most of Canada with an EMP field too.

Another EMP scenario detonates a nuclear weapon 30 kilometres high anywhere over the eastern half of the U.S., which would collapse the Eastern Grid. The Eastern Grid generates 75 percent of U.S. electricity and supports most of the national population. Such an attack could be made by a short-range Scud missile launched off a freighter, by a jet fighter or small private jet doing a zoom climb, or even by a meteorological balloon.

North Korea and Iran have also apparently practiced making a nuclear EMP attack using a short-range missile launched off a freighter. Such an attack could be conducted anonymously to escape U.S. retaliation--thus defeating nuclear deterrence.

Canada would be affected by this scenario too. Collapse of the Eastern Grid would no doubt set in motion cascading failures, far beyond the EMP field that would reach into Canada, probably causing a protracted blackout of at least Ontario and Quebec, the most populous provinces.

In another scenario, an adversary makes an EMP attack on the U.S. National Missile Defenses in Alaska. In yet another scenario, U.S. missile defenses fail to intercept a nuclear warhead until it is near or over Canada, and then the warhead is salvage-fused for EMP attack. In these scenarios, Canada inadvertently becomes the focus of a nuclear EMP event.

In still another scenario, during some supreme international crisis between the U.S. and a nuclear-armed adversary, the adversary deliberately makes a nuclear EMP attack on Canada as a demonstration of its resolve, to deter the U.S. and "de-escalate" the crisis.

Protecting Canada

The EMP Commission recommended an "all hazards" strategy to protect North America by addressing the worst threat--nuclear EMP attack. Nuclear EMP is worse than natural EMP and the EMP from RFWs because it combines several threats in one. Nuclear EMP has a long-wavelength component like a geomagnetic super-storm, a short-wavelength component like radio-frequency weapons, a mid-wavelength component like lightning--and is potentially more powerful and can do deeper damage than all three. Protecting the electric grid and other critical infrastructures from nuclear EMP attack will also protect against a Carrington Event and RFWs. Moreover, protecting against nuclear EMP will also protect the grid and other critical infrastructures from the worst over-voltages that may be generated by severe weather, physical sabotage, or cyber-attacks.

Canada is fortunate in that it is, after China, the second largest generator of hydro-electricity in the world and depends for most of its electricity (64 percent in 2010) on hydro-power. Hydro-power is the most resilient means of generating electricity, least vulnerable to EMP. Thus, Canada should be able to relatively inexpensively protect most of its electric power by EMP hardening its hydro-electric plants.

Highest priority probably should be given to EMP hardening Canada's 18 nuclear power plants, which pose a potential radioactive hazard to populous Ontario. The CANDU nuclear reactors, designed in Canada, can also be re-wired to safely operate through a blackout, instead of shutting down, thereby keeping the lights on in Ontario.

Protecting Canada's hydro-power, which generates 64 percent of the nation's electricity, and nuclear power, which generates 15 percent, would secure 79 percent of Canada's electrical energy--more than enough to survive and rapidly recover from an EMP catastrophe. Nonetheless, it would be wise to protect the coal-fired plants (13 percent of Canada's electricity) so they will not explode from an EMP. Coal largely powers Alberta, Nova Scotia, and Saskatchewan.

Natural gas pipelines and power plants (6 percent of Canada's electricity) should be EMP hardened to avert gas explosions and firestorms.

Dr. Peter Vincent Pry is Executive Director of the EMP Task Force on National and Homeland Security, served in the EMP Commission, the House Armed Services Committee, and the CIA, and is author of "Electric Armageddon and Apocalypse Unknown: The Struggle To Protect America From An Electromagnetic Pulse Catastrophe".

Cyber Triggers And The First Strike Dilemma

Written by: Cynthia E. Ayers

"I think at the moment that there's not a significant price to pay [for cyber attacks] and so you see actors, nation states, individuals willing to do more."[1]
- Admiral Michael Rogers, Director, National Security Agency
Commander, U.S. Cyber Command

"Until we redefine warfare in the age of information, we will continue to be viciously and dangerously attacked with no consequences for those attackers." [2]
- Lieutenant General (Retired) Michael Flynn, Former Director, Defense Intelligence Agency

NATO Secretary-General Jens Stoltenberg, during a March 2015 public statement, declared: "NATO has made clear that cyber attacks can potentially trigger an Article 5 [allied military] response." The Secretary-General was reportedly reacting to recent Russian "hybrid" activities (cyber attacks perpetrated prior to and in conjunction with conventional military operations) in Crimea and Ukraine[3], but the implications of his statement are much broader. Is it possible that an adversarial cyber event could trigger the onset of a larger cyber and/or kinetic conflict? If so, what would it look like? Can such an event be identified in time for effective response? If not, is it possible that a "missed" cyber trigger in the form of a surprise cyber first strike could ultimately influence the fate of nations?

The potential for devastating cyber attacks against the United States has been the number one global threat listed within the 2013[4], 2014[5], and 2015[6] Worldwide Threat Assessments provided annually to Congress by the Director of National Intelligence (DNI). The DNI's 2013 assessment

followed a year of warnings, provided at unclassified venues by cabinet-level officials.

Former U.S. Secretary of Defense (SECDEF) Leon Panetta, during an interview with ABC News in May of 2012, identified examples of cyber attacks that could trigger a war. "There's no question," he stated, "that if a cyber attack . . . crippled our power grid in this country, took down our financial systems, took down our government systems, that that would constitute an act of war."[7] In a speech delivered to the Business Executives for National Security later the same year, SECDEF admitted: "We know that foreign cyber actors are probing America's critical infrastructure networks. They are targeting the computer control systems that operate chemical, electricity and water plants, and those that guide transportation throughout the country. We know of specific instances where intruders have successfully gained access to these control systems."[8]

Former Secretary of Homeland Security Janet Napolitano, in a January 2013 speech at the Wilson Center (Washington DC), warned of a "cyber 9/11" against critical infrastructure for which we should be preparing. "There are things we can and should be doing right now that, if not prevent, would mitigate the extent of damage," she said while noting the potential for a large-scale loss of electricity[9]. A few days later, during a PBS interview, she admitted that "cyber threats [have] moved to a new level," identifying Iran, Russia and China as the biggest perpetrators of cyber attacks. She specifically mentioned her concerns associated with "the nation's core critical infrastructure" – energy, telecommunications, and banking.[10] It is thus evident that a cyber trigger or first strike from an adversarial perspective, is expected to be an attack on critical infrastructure. The question, however, remains – how big and how effective does such an attack have to be to trigger a response?

The Department of Homeland Security's (DHS) Industrial Control System-Cyber Emergency Response Team (ICS-CERT), within their end-of-year (2012) statistical review, stated that 41% of the year's reported cyber attacks were aimed at the energy sector. Indications derived from the study pointed to a change in adversarial focus to the more vulnerable aspects of infrastructure – those that would be more devastating to the public if disrupted for long periods of time. The attackers "zeroed in on computer systems run by power grid operators and natural gas pipeline companies." Adding to the estimation of malicious intent, the 2012 statistics included "a successful attack against a key supplier of energy control systems."[11] Furthermore, in an announcement that was lacking in specifics, DHS confessed "that an American power station . . . was crippled for weeks by cyberattacks."[12]

Apparently while the ICS-CERT end of year report was being prepared, "a secret legal review" on America's use of "cyberweapons" was held. According to a February 2013 New York Times article, the legal assessment concluded that the authority to "order a pre-emptive strike" exists within the Office of the President -- provided there is "credible evidence of a [pending] major digital attack"[13] against U.S. equities. Executive Order 13636 Improving Critical Infrastructure Cybersecurity[14], and Presidential Policy Directive 21 (PPD-21) Critical Infrastructure Security and Resilience[15] were released on the heels of further press coverage of the "secret review." Both were signed on February 12th (2013) – the day of President Obama's State of the Union Address, which also contained warnings of enemy attacks against the financial sectors and the power grid.[16]

Executive Order 13636 was not without detractors. In response to its release, Brookings published "Bound to Fail: Why Cyber Security Risk Cannot Simply be 'Managed' Away". The authors criticized the Executive Order as insufficient because of its reliance on risk management and voluntary participation. "Business logic ultimately gives the private sector every reason to argue the always hypothetical risk away, rather than solving the factual problem of insanely vulnerable cyber systems that control the nation's most critical installations."[17] The same could be said for government. Mitigation against catastrophic critical infrastructure collapse – a "worst case" scenario, yet entirely achievable and desirable by adversaries[18]-- must not depend on risk management. History tells us that worst case does happen; and in the context of conflict, worst case is usually intentional.

Passive and patchy cyber defense is no longer enough to thwart major cyber attacks.[19] "We won't succeed in preventing a cyber attack through improved defenses alone."[20] Reliance on cyber security professionals to locate, identify, and keep up with cyber threats is an increasingly expensive and "unsustainable" option.[21] Additionally, cyber defense models can't catch everything. The threat to the energy sector alone can be seen in the level of support provided by ICS-CERT, which, as reported in their Year In Review for 2014, was more than double that of the previous year. Also, the report noted with "great concern" the ICS-CERT response to "multiple newly discovered cyber campaigns that had been ongoing for several years."[22]

Detection of imminent threat cannot depend on the chance finding of ongoing "cyber campaigns." As former SECDEF Panetta said, "If we detect an imminent threat of attack that will cause significant

physical destruction or kill American citizens, we need to have the option to take action to defend the nation when directed by the President."[23] If the "secret legal review" did indeed examine and acknowledge that the President had such authority, is the United States now well protected in the cyber realm?

Some might say yes. In January 2015, President Obama imposed new sanctions on North Korea as a result of the "hack" on Sony Pictures[24] after vowing: "We will respond proportionately and in a space, time and manner that we choose."[25] He later signed an Executive Order, authorizing sanctions on those "responsible for or complicit in malicious cyber-enabled activities" that can pose "significant threat to the national security, foreign policy, economic health, or financial stability of the United States."[26]

Others might disagree. In addition to the 2014 discoveries of long-term malware insertions,[27] cumulative attacks and delayed attribution continue to be a problem. The DNI's testimony for the 2015 Worldwide Threat Assessment[28] included this admonition:

"The muted response by most victims to cyber attacks has created a permissive environment in which low-level attacks can be used as a coercive tool short of war, with relatively low risk of retaliation. Additionally, even when a cyber attack can be attributed to a specific actor, the forensic attribution often requires a significant amount of time to complete. Long delays between the cyber attack and determination of attribution likewise reinforce a permissive environment."

Lieutenant General Flynn's comment (at the beginning of this article) about hackers being encouraged because there are "no consequences"[29] reveals similar frustration.

Although increases in cyber intrusions have been noted in open-source for years, little (to the public's knowledge) has been done offensively in the cyber or physical realms by the West (with the possible exception of Stuxnet[30]). Even with the most recent revelations of data theft,[31] the public remains unaware of the extent to which any counterattack has been attempted.

From hacker groups like "Anonymous" to actors (officially recognized or not) of nation-states, cyber attackers have been waging unofficial cyberwar at rising levels across the network. There has, however, been no definitive "line in the sand" – a point at which response is assured.

It is understood that regardless of attacker intent, there can be unintended consequences of adverse activities, especially if attacks have been sequential and cumulative. Unpredictability in adversarial attack modes and capabilities is something that must always be considered. Similarly, a consequence of response is the possibility of introducing or reacting to an event that might trigger a larger, less controlled cyber conflict – one that could lead to a full-scale kinetic war. This is no doubt a possibility that the White House is trying to avoid.

Yet, the process of verifying a Presidential pre-emptive authority against impending cyber attacks would also indicate an understanding that a "worst case" cyber scenario has been considered, if not yet conceived, by potential adversaries. As indicated by SECDEF Panetta, an attack against the electric grid,[32] if well-coordinated and sufficiently resourced, could have catastrophic effects on the population. Long-term regional or national power-outages might mean large numbers lost to malnutrition, disease, and chaos. A year without power could result in the death of over two-thirds of the population within the affected area.[33] Such an attack is worthy of being labeled a trigger event in what would probably be a "cyber first strike."

Counterattack under this type of scenario would be difficult and probably too late to be relevant. Similar to the "not fully successful" 2008 Russian invasion of Georgia[34], a cyber first strike is intended to leave victims vulnerable for a kinetic follow-on attack. Theoretically, a successful cyber first strike would leave a nation without hope of allied assistance and ultimately, unable to maintain sovereignty. The leaders of NATO have reason to be concerned. The U.S. is already seeing adversaries in its critical infrastructure. These infiltrators have been allowed the opportunity to test their capabilities with the mere realization that sanctions may eventually be applied.

Cyber triggers have already been "missed." What's next? Will sanctions be applied? Will pre-emptive action be taken? Or will the enemies' cyber first strike (or cyber "take down") spell the demise of U.S. national sovereignty in an inevitable – albeit short -- cyber war?

Cynthia Ayers is currently a consultant working with the Mission Command and Cyber Division of the Center for Strategic Leadership & Development, U.S. Army War College. She retired from the National Security Agency (NSA) in 2011 with over 38 years of government service. Her intelligence community career included a position as an NSA Representative to the DCI's Counterterrorism Center at CIA headquarters. Post-retirement, Ms. Ayers was employed as Vice President of EMPact America, a bipartisan, not-for-profit group, and is currently a Director (Deputy to the Executive Director) of a congressionally-sponsored task force working on critical infrastructure issues.

Restoring Accountability for Telecommunications Surveillance in Canada

Written by: Dr. Christopher Parsons

Originally published August 11, 2015

Canadian federal, provincial, and municipal authorities routinely request access to data that are either stored or processed by telecommunications service providers. A slew of laws authorize such requests including recently passed legislation expanding security intelligence activities[1] and establishing new data preservation and production powers. Furthermore these laws have authorized government agencies' use of malware, and legalized the voluntary sharing of telecommunications data between corporations and government.[2] Surveillance-enabling laws are well-used by authorities, to the point that hundreds of thousands of requests for telecommunications data are made each year and affect hundreds of thousands of Canadians.[3] And as discussed in this article, few government requests for access to telecommunications data are disclosed to the Canadian public. In essence, governments of Canada conduct a massive volume of telecommunications surveillance with limited public accountability.

This article will first examine corporations' involvement in government surveillance activities: how much surveillance are companies compelled to conduct and how effective are companies' efforts to explain their government-compelled surveillance practices. Next, the paper will discuss how Canada's surveillance oversight, review, and reporting infrastructures have fallen into disrepair and the significance of these infrastructures' failures. The paper concludes by discussing how improving statutory electronic surveillance reports, empowering oversight and accountability bodies, and establishing a parliamentary oversight committee for national security could restore trust in contemporary surveillance activities while identifying — and defraying — bad actions.

Corporate Disclosures of Telecommunications Information

Canadian telecommunications service providers (TSPs) are routinely compelled to provide telecommunications data to government authorities. In 2010, the Royal Canadian Mounted Police (RCMP) made at least 28,143 requests for subscriber data; such information includes subscribers' names, addresses, and possibly information about the devices they use, electronic identifiers, and billing information. Of these requests, 93.6% were fulfilled without authorities first acquiring a court order.[4] In 2011 the Office of the Privacy Commissioner of Canada learned government authorities had made at least 1,193,630 requests for subscriber data over the year, and that the requests affected at least 784,756 subscribers.[5] In 2013, six of Canada's telecommunications providers asserted that they had received a combined 140,457 requests for subscriber data between them and a grand total of 372,825 requests by government authorities for telecommunications information. This latter total reflects all of authorities' requests for telecommunications data, thus including subscriber data requests as well as those based on subpoenas and warrants, on emergency grounds, and other legal grounds. These latter kinds of requests can include any kind of electronically communicated data, from wiretaps to text messages to emails or Internet logs.[6]

At present, few Canadians will ever learn that their telecommunications information has been disclosed to government authorities. Only when individuals have their communications intercepted, recorded using a hidden camera, or other real-time acoustic recording, are they notified of the government's surveillance regardless of whether charges are brought against the monitored person.[7] More specifically, government authorities do not have to notify Canadians when authorities have collected persons' subscriber data, stored email, or other modes of telecommunications surveillance.

The only way for Canadians to learn they are affected by these latter modes of surveillance is if the collected information is used against them in a legal proceeding. Consequently, most Canadians remain oblivious when their TSP discloses their personal information or monitors their telecommunications on behalf of government authorities.

No Canadian TSP has publicly committed to notifying their subscribers of government surveillance or taken public policy positions that Canadians ought to know when their TSP has been compelled to share subscribers' information with authorities.[8] Although Canadian TSPs have begun releasing transparency reports to disclose the number of times government authorities compel data from the companies, the reports do not explain data retention periods or disclosure practices. The former is needed for Canadians to understand just how much data a given government order might elicit from a company, and the latter for Canadians to understand what authorities must do to force companies to disclose information. These additional categories are needed to contextualize existing transparency reports if those reports are to be useful public policy documents.

At present the only parties who are guaranteed to know about the surveillance — the government authorities and TSPs — tend not to, or are disinclined to, inform the victims of such surveillance when charges are not brought against the targets of the government's attentions. In light of these limitations, Canadians are forced to rely on accountability processes as well as oversight and review bodies to ensure that inappropriate surveillance does not take place.

Accountability Deficits

Canada has a federal oversight system that was largely developed for the 1970s and 1980s, which has fallen into disrepair as successive federal governments have prioritized the expansion of surveillance powers at the expense of equivalent oversight and accountability for the use of these powers. Specifically, annual electronic surveillance reports and federal review, oversight, and accountability offices do not effectively monitor or report on the extent of government surveillance powers. Consequently, the public and parliamentarians are hindered in holding the government accountable for its use of telecommunications surveillance powers.

The federal and provincial governments of Canada are obligated under s.195 of the Criminal Code to produce annual reports that detail the regularity with which they intercept Canadians' communications. The actual number of federal intercepts has declined since the 1970s, though the average number of persons affected by

each interception warrant has risen.[9] Moreover, while the federal government of Canada publishes its annual report on the Public Safety Canada website, few of its provincial counterparts make their reports publicly accessible. This has the effect of masking the extent of interception-related surveillance; whereas federal government agencies conducted 845 telecommunications interceptions in 2011,[10] Canadian telecommunications service providers received at least 6,000 interception orders in the same year.[11]

The annual electronic surveillance reports do not account for the range of contemporary telecommunications surveillance practices undertaken by government agencies. They do not, for example, account for government requests for subscriber records, for access to content stored on computer servers, for access to metadata pertaining to telecommunications activities, or uses of computer malware to collect or extract information from computer devices. These non-interception modes of surveillance account for the majority of government telecommunications surveillance; whereas the Canadian Border Services Agency made 18,849 requests for telecommunications information in 2012 and 2013, none of those requests involved intercepting communications.[12] The RCMP made at least 28,143 requests for subscriber information in 2010,[13] whereas there were a total of 535 requests for telecommunications interceptions across the entire federal government for the same year.[14]

Canadians might expect federal review, oversight, or complaints officers to ensure government authorities do not inappropriately access telecommunications information.

These officers and their associated offices, however, cannot provide high-levels of assurance that authorities only appropriately access telecommunications information. In the case of the Security Intelligence Review Committee (SIRC), which conducts annual reviews of some of the Canadian Security Intelligence Service's (CSIS) activities, its review functions have been challenged by not having a full complement of committee members to oversee the SIRC.[15] Only recently has the government appointed two new members to fill the committee. Both of them possess strong national security backgrounds. However, the SIRC was never meant to include such persons on its committee[16] and so even in fully staffing the committee, its composure of not including members of the intelligence committee has been compromised.[17] Moreover, CSIS delays providing information to the SIRC and thus inhibits the SIRC's abilities to conduct reviews.[18] And the SIRC cannot identify how CSIS-gathered information is used after it is shared outside of CSIS,[19] preventing the review body from assuring parliamentarians that CSIS-related telecommunications surveillance is conducted in accordance with CSIS', and associated agencies' mandates or legal authorities.

The Office of the Privacy Commissioner of Canada (OPC) is limited in its ability to investigate government telecommunications surveillance. Critically, the Privacy Act limits the OPC to only examining the collection and use of Canadians' personal information; the OPC "does not have jurisdiction to examine in general the lawfulness of the activities of national security agencies."[20] Moreover, even when the OPC discovers that a federal agency is conducting, or has conducted, an inappropriate mode of telecommunications surveillance it cannot stop the activity using its powers under the Privacy Act, nor can it compel federal agencies to modify their practices under the OPC's present legal powers. The result is that while government agencies may implement the OPC's recommendations there are no hard legal consequences for failing to act on those recommendations.

Oversight deficits carry over to the Office of the Communications Security Establishment Commissions (OCSEC), which oversees Canada's foreign signals intelligence agency, the Communications Security Establishment (CSE). The OCSEC tables an annual report that accounts for some of the CSE's activities in the prior year. While the OCSEC has always asserted that CSE has behaved lawfully, the Commissioner warned in 2004 that the assessment "should not be taken to mean that I am certifying that all CSE's activities in 2003-2004 were lawful. I cannot make this assertion, because I did not review all their activities—and no independent review could."[21] Moreover, this assertion of lawfulness is based on the federal government's classified and privileged interpretation of CSE's own national security mandates; the OCSEC has warned that, given this basis of lawfulness, they have applied an "interim" solution of relying on the Department of Justice's interpretations of CSE's mandate since CSE's formal independence in 2001.[22] The result is that CSE's lawful telecommunications surveillance that has occurred since 2001 is predicated on a stopgap interpretation, one which has never been publicized. Moreover, the OCSEC, like the SIRC and OPC, cannot work with other governmental review, oversight, or accountability bodies. The consequence is that the OCSEC cannot track information that CSE collects and then distributes to other agencies. As a result, the OCSEC does not fully understand how CSE-

The CBSA, as an example, possesses neither an inspector general nor an independent review organization, despite the regularity that CBSA conducts.

collected telecommunications information pertaining to Canadians is used by other domestic and foreign government agencies.

Making matters worse is the absence of dedicated review or oversight bodies for most government agencies that receive or compel access to telecommunications information. The CBSA, as an example, possesses neither an inspector general nor an independent review organization, despite the regularity that CBSA conducts telecommunications surveillance. The same is true of the majority of government agencies that will be authorized to receive and share information, including telecommunications-derived data from private firms and between government agencies as a result of provisions in Bill C-13: Protecting Canadians from Online Crime Act and Bill C-51: Anti-terrorism Act, 2015.

Restoring Accountability to Government Surveillance

Bringing government practices to account requires reforming the annual electronic surveillance reports, empowering review and oversight bodies to 'follow the data' beyond the borders of their own agencies, and expanding parliamentary oversight. Without such reforms Canadians and their political representatives, as well as independent officers to parliament meant to oversee and review government surveillance activities, cannot effectively detect or reform inappropriate, overzealous, or otherwise concerning government surveillance activities.

Annual electronic surveillance reports provide useful information about government telecommunications surveillance, but fail to account for the majority of contemporary surveillance practices. Given the shift in government agencies' investigation techniques towards those favouring access to stored records and to non-content aspects of communications, these annual reports should be expanded to account for today's government surveillance practices. Legislative amendments could explicitly require government agencies to account for their access to subscriber and customer name and address records, use of malware and tracking warrants, along with other (lesser known) modes of contemporary surveillance. Moreover, such reports should be published online by all Canadian governments. Such reforms would let Canadians and parliamentarians understand the full extent of government authorities' contemporary surveillance powers, how regularly those powers are used, and the effectiveness of those powers in generating criminal prosecutions.

Government agencies increasingly work with one another in the course of investigations and these collaborations will increase and deepen in light of information sharing provisions included in Bill C-51: Anti-Terrorism Act, 2015. While such collaborations amplify information sharing, the organizations responsible for ensuring that government agencies do not inappropriately collect or exchange telecommunications-related data have not kept pace. Canada's oversight, review, and privacy bodies are not legislatively permitted to collaborate or coordinate with one another. Consequently, they cannot ensure that information is collected and shared responsibly. Moreover, when these bodies do find inappropriate behaviours their abilities to legally force changes to organizational practices are limited: the OPC cannot enforce its decisions, SIRC cannot compel changes in CSIS, and the OCSEC is largely barred from identifying unlawfulness because of how its mandate and terms of reference have been secretly established. These limitations must be rectified for these bodies to assure Canadians that telecommunications surveillance is lawful and appropriate given the crimes being investigated.

In addition to improved annual reporting, and coordination and enforcement capabilities provided to independent review and oversight bodies, parliament must establish a committee to oversee security and intelligence activities. A committee that was focused on overseeing and reporting on the adequacy, efficiency, and efficacy of policing, security, and intelligence agencies' budgetary practices would let parliamentarians hold the government to account for its spending of government monies. The committee should also, paralleling similar committees in the United States and United Kingdom, be notified of significant changes to national security policies or novel practices so that member of parliament could genuinely represent their constituents' interests and be able to task review and oversight bodies to provide special reports as

needed. Such a committee would ensure that government telecommunications surveillance activities provide good value for the tax dollars invested and that the agencies conducting the surveillance are behaving appropriately.

Were the aforementioned recommendations adopted then Canadians could at least know that their parliamentarians possessed the information and capabilities needed to hold government to account for its telecommunications surveillance. Elected representatives would be able to ask about the appropriateness of contemporary surveillance, whether new powers are genuinely required in light of the extent and regularity of contemporary surveillance, and better understand how proposed powers might fit amongst those currently enjoyed by government authorities. Without adopting these sorts of reforms, or ones like them, then Canadians will effectively continue to live in a country where extensive amounts of entirely secret telecommunications surveillance is conducted without the knowledge or meaningful approval of Canadians or their representatives. Successive federal governments have expanded government authorities' surveillance capabilities: it is well past time for equivalent accountability capabilities to also be expanded.

Dr. Christopher Parsons is a Postdoctoral Fellow at the Citizen Lab in the Munk School of Global Affairs at the University of Toronto and a Principal at Block G Privacy and Security Consulting. His research focuses on how privacy (particularly informational privacy, expressive privacy and accessibility privacy) is affected by digitally mediated surveillance and the normative implications that such surveillance has in (and on) contemporary Western political systems. He is currently looking at Deep Packet Inspection (DPI), behavioural advertising, and mobile device security. Broadly, his academic and personal interests attend to privacy, citizenship, technology, surveillance, globalization, copyright, and cosmopolitanism.

Organizational Resilience

Written by: Peter Power

Summary

Organizational Resilience (OR) refers to a united approach in the face of growing risks, threats and opportunities, rather than applying separate functions (e.g. security, disaster recovery, risk management, business continuity etc.), each trying to cope at different levels. OR moves beyond defensive security and what might be called a 'protection posture', by applying a more cohesive yet flexible approach that far from downgrading key functions such as security, both elevates and integrates such tasks by uniting policies, objectives and a shared purpose. In short, synergy replaces silos.

The objective is to enable any organization, including structures that supply it and otherwise depend on it, to absorb shocks, learn from them and be better equipped for future events. Functions such as business continuity, information security, IT disaster recovery, crisis management, physical security, environment management and operational risk management, become part of a broad corporate framework in a world that is becoming turbulent faster than organizations are becoming resilient.

An organization's resilience, properly understood, has critical implications for its stability, competitiveness, profitability and shareholder value. One reason why Governments such as the UK(1) , Australia(2) and the US (10) are already committed to promoting OR.

Organizational Resilience Defined

The UK Government standard on OR(1) (as one example) states that it is the "capability of an organization to anticipate and respond and adapt to, incremental change and sudden disruptions in order to survive and prosper". A succinct explanation and not that dissimilar, for example, from the definition stated by the Australian Government (2): "a business's ability to adapt and evolve as the global market is evolving, to respond to short-term shocks, be they natural disasters or significant changes in market dynamics and to shape itself to respond to long-term challenges".

Perhaps the most relevant definition of OR in Canada is one put forward by IBM(3) Canada: "Resiliency is your company's ability to protect people, assets, data and technology through proactive measures that help mitigate risk".

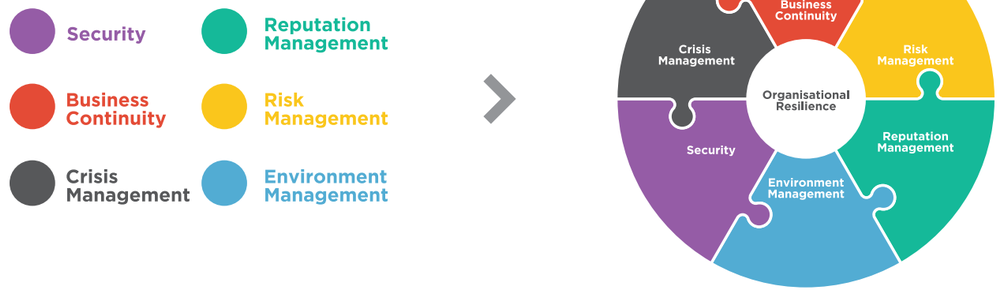
For the purpose of this article I have assumed that OR is broadly the same as Business Resilience as well as Corporate Resilience. It does not equate with fusion centres where the purpose is simply to share and better manage the flow of data and intelligence across different levels and sectors. OR has a significantly broader remit to unite policies, objectives and a shared purpose with a function to absorb shocks, learn from them and be better equipped for future events.

Comments from the UK OR standard (which draws on other standards, such as Crisis Management(4)) include:

- Resilience is not a choice between continuity and adaptability. Rather, it is a synthesis of both: continuity in the face of disruptive challenges, and long-term viability against a backdrop of strategic change.
- A more resilient organization cultivates a culture of shared purpose.
- Organizations should create the means, incentives and imperatives to share information about risks, incidents, near misses, vulnerabilities and opportunities, across the organization and with partners and other interested parties, including competitors where this could realise mutual benefit.

OR therefore moves from a more usual/traditional collection of silos, towards the integration of key disciplines, as shown in this diagram.

This enables a 360-degree connected capability to better detect, mitigate, respond, recover, learn and adapt to any disruptive challenge that might impact either, or every layer in the organization. It can also reduce overheads by having one overall coordinator, albeit with managers at key positions, all sharing the some purpose:



It does this by integrating all those aspects of each discipline that have a common shared theme (or connection) of anticipating, responding and adapting to slow or sudden disruptions or shocks wherever, or however they might occur.

Why Organizational Resilience

In today's increasingly interconnected world where communication is both global and instant, disasters can have a wave effect that resonates throughout the supply chain, already made fragile by cut backs and 'Just in Time' work practice. For example, when a disaster destroys a manufacturing plant on another continent, a supplier 1000's of miles away is unable to meet production goals. Therefore, a crisis in one part of the world can bring economic activity to a grinding halt in another country or region. No surprise then that several governments are already signed up to the principles of OR.

On which point, the approach of any government to OR has to rely on more than just politics. It is possible that the long-term vision required to plan and create true OR could be in conflict with relatively short 4/5 year political terms of office. Such a situation offers little incentive

for politicians to take a long-term rather than a short-term view as acute or short-term risks are more likely to gain attention over longer-term chronic risks. Consequently, organizations and governments alike can often be focussed on specific risks which may not in fact, be the greatest threat to them.

Whether it is the public or private sector, all this prompts the need for real change in crisis mitigation, security, preparedness and response from both sectors as many countries' vital parts of critical national infrastructure (e.g. power, transport, communication etc.) are in the hands of commercial organizations, sometimes with a head office in a country distant from where the service is actually provided. All this matters in a world that is constantly changing, where crises don't fit into precise boxes with a neat beginning and end.

Organizations (and professions) make distinctions of expertise but so far, rarely promote OR as a feature to share common doctrine and procedures, each others' infrastructure and bases, and to be able to easily communicate with each other. This is sometimes referred to as 'interoperability' that has the following benefits:

- Understanding interfaces
- Collaborative work practice
- Present and future focus
- Share everything - no restrictions
- Pooling resources
- Synergy

In 2013 PricewaterhouseCoopers (PwC), a global business support organization with 13 offices across Canada, published a report on 'Rebuilding for Resilience'(5). This contained a series of observations, including some of the challenges that organizations might have to consider when reforming their in-house disciplines towards OR. For example, taking higher risks for the same rewards and recognizing that failures and disruptions still happen, despite heavy investments in risk management.

Case Studies

- JP Morgan Chase & Co, a successful global bank, has long applied a 'Global Resiliency' program designed to provide integrated firm-wide resiliency aligned to its business strategy and principles. It does this by engaging senior management on all aspects of the program, including determining the resiliency risk appetite, strategy, leadership and program oversight. Also, helping employees understand their roles and undertake validation tests and exercises for all critical functions and locations.

- In 2014 Cranfield School of Management (www.som.cranfield.ac.uk) looked at the following specimen/successful organizations who already apply OR in their report 'Roads to Resilience' (6): InterContinental Hotels Group, Jaguar Land Rover, UK Olympic Delivery Authority, Virgin Atlantic and Zurich Insurance. They found that resilient companies do not just happen. They have cultural and behavioural traits that encourage all employees to be flexible, customer focused and alert to danger. In particular (a) the ability to anticipate problems before they develop, (b) flexibility to respond, (c) risk information flowed freely, (d) people and processes were in place to restore things to normal as quickly as possible and (e) the ability to learn from experience and make the necessary changes so that every event is analyzed. At Virgin Atlantic, for example, senior executives work in one corner of an open-plan office on the second floor. Colleagues can come to them with their thoughts and, of vital importance, there is a no-blame culture. To quote the head of internal audit (coincidentally on secondment from another firm): "There is an executive team who do not really have egos. They are happy for you to go and have an honest conversation with them." As a result, vital risk and security information travels around the company and the board make well-informed decisions. This contrasts with the risk blindness evident in virtually every corporate failure identified in an earlier report by Cranfield.

- In 2010 the Australian government set out to measure and compare OR in that country. The Australian Journal of Emergency Management Volume 25 2010(7) states that 'effective resilience management for any one organization must look beyond that single organization and consider the resilience of other organizations that it depends on.....threats can exceed the scale foreseen and planned for by an organization. The ability to survive and take advantage of these events depends on the resilience capacity of the organization. An organization wishing to survive and prosper from adversity could optimise its opportunity by enhancing its resilience attributes in preparation for such events'.

- In 2011, President Obama issued Presidential Policy Directive Eight (8) 'to develop (ongoing) a national preparedness system with the objective of strengthening resilience in the face of terrorism, cyber attacks, pandemics, and catastrophic natural disasters'. The directive defined resilience as 'the ability to adapt to changing conditions and withstand and rapidly recover from disruption due to emergencies.'

- In 2012 Aon Global Risk Management services published a 'Reputation Review'(9) which found that 'there is an 80% chance of a company losing at least 20% of its value (over and above the market) in any single month, in a given five-year period'. They conclude that 'in an age of instant and global communications, it is more important than ever to identify emerging threats'.

Conclusions

OR offers two practical concepts of responsiveness: the first might be considered a buffer. That is a collective process to hopefully anticipate any form of shock and prepare a reaction to allow some breathing space before the organization learns and adapts.

The second might be described as adaptive capacity that combines organizational agility to adapt, along with strategic flexibility. Buffers might be important for survival, but adaptive capacity is an indicator of longer-term resilience.

In a world where the extraordinary has become commonplace and the unexpected is now regularly anticipated, predictability takes on a different meaning, so the need to anticipate and allow for adaptive capacity has never been greater.

Present attitudes on trying to carry on operating through any disruption, damage or any other challenge tend to be rooted to the world of business continuity (which seldom has enough links to physical security), being dependant on historical data, and therefore might be described as "Bouncebackability" (a word invented by football coach Iain Dowie).

However, successful organizations in the future might benefit from taking a slightly different approach if they consider the comment attributed to Charles Darwin in his 1859 book 'The Origin of Species' that changed forever global thinking on evolution: "It is not the strongest of the species that survives, but rather, that which is most adaptable to change". Successful organizations might therefore adapt to change, rather than follow the Latin origin of Resilience (resalire - to spring or jump back) by going forward instead. In other words, OR with collaborative work practice, forward looking, synergy and adaptive capacity - "Bounceforward"

In 2017 the International Standards Organization (ISO) is due to publish an international standard on OR - ISO 22316(10). This global standard will set out (1) a series of principles that govern resilience as an outcome, a state of being achieved by an organization, rather than a discipline, function or process and (2), a series of attributes of a more resilient organization, e.g. purpose, leadership, behaviours, innovation and potential strategies to enhance resilience.

There is no 'one size fits all' approach to OR. Sometimes there are no right answers to the questions raised. However, an organization that considers different views and opinions as an asset, is willing to learn from near misses and failures (without rushing to blame people) and enables a high level of synergy rather than silos, is likely to be well placed to demonstrate effective OR.

With today's pervasive change and uncertainty it is no longer adequate to simply rely on security, risk and business continuity that often applies historical data to try and predict future shocks, catastrophes and crises along with their consequences. Big or small, an organization needs to anticipate, respond and adapt to incremental change and sudden disruptions, in every direction and at all levels, in order to learn, survive and prosper.

"Change will not come if we wait for some other person, or if we wait for some other time. We are the ones we've been waiting for. We are the change that we seek".

- U.S. President Barack Obama(11).

Peter Power is MD of Visor Consultants (UK) Ltd and co-author of the UK Standard on Crisis Management (BS 11200) as well as a past member of the (IPPR) UK National Security Commission. He has considerable experience of several real time catastrophes and is an international speaker, writer and a Fellow of the Institute of Risk Management and the BC Institute. He has been a Special Advisor to the Toronto based World Conference on Disaster Management since 2001 and has previously given presentations to CSIS in Ottawa and the Attorney General's Office in Australia, as well as the United Nations (WTO). He is on the Advisory Board of The Mackenzie Institute.

The Need for Effective Intervention Programs to Prevent Islamic Extremists and Terrorist Recruitment in Western Countries with Special Emphasis on Canada

Written by: Dr. Wagdy Loza

Originally published July 2, 2015

Increasingly over the last decade the world has witnessed more frequent acts of terrorism, reaching a crescendo since Islamic State of Iraq and the Levant (ISIL; also known as the Islamic State of Iraq and Syria [ISIS], or the Islamic State [IS]) appeared on the scene. ISIL engages in "direct marketing techniques" with social media videos soliciting participants among local citizenry. Many non-Western countries, such as Iraq, Syria, Nigeria, and Israel have been most dramatically affected. However, terrorist attacks targeting Western nations are now also being commissioned by ISIL. It has been reported that there were approximately 10,000 fatalities from 2,800 attacks in 2013 alone (Pipes, 2015). Refugees are now counted in the millions. It would be reasonable to suggest that the 2014 tally will be much higher. These attacks have a far reaching impact extending well beyond the victims of the attacks and their families. Many people from all around the world could be diagnosed with Post Traumatic Stress Disorder (PTSD) just from watching the news footage of these attacks. Indeed, a French pharmacist reported that the consumption of anxiety medication rose by 20% nationwide (Gurfinkiel, 2015) since France's 9/11 (the terrorists who murdered journalists, police, and civilians in France in January 2015).

Australia, Canada, and other European countries have been targeted for terrorists' attacks too. On October 20, 2014 in Quebec, Canada, Martin Couture-Rouleau drove his car into two military men, killing a Warrant Officer and wounding his colleague. Police stated that the terrorist, who perpetrated this act, was radicalized after converting to Islam (Waugh & Douglas, 2014). A few days later, Michael Zehaf-Bibeau, another

"It has been reported that there were approximately 10,000 fatalities from 2,800 attacks in 2013 alone"

convert to Islam, shot an unarmed soldier at the National War Memorial and stormed the parliament buildings. This act could have resulted in the killing of government officials and several parliamentarians, but was averted by the heroic actions of brave staff. In between these two incidents, two Canadians were convicted for terrorist related crimes.

Also around this period, more disturbing is the news that intelligence officials estimate around 130 Canadians have traveled abroad to fight with groups like ISIL; of this group, 80 individuals have returned home (Valdmanis, 2014). One of these young men, who was a convert to Islam, had threatened Canadians and invited other young Canadians to convert to Islam and join ISIL in its fight. Similarly, many young converts from western countries have joined ISIL. In addition to these disturbing facts, previous research indicated that the extreme Middle Eastern religious ideologies are prevalent and growing among the Muslim communities in Europe (Bawer, 2006; Wicker, 2007; Yaseen, 2007) and other western countries. Other examples of the prevalence of the extreme ideologies among first or second generation Middle Eastern emigrants are drawn from several sources. For example, Leuprecht, Hataley, Moskalenko, and McCauley (2009) reported a 2005 UK poll of Muslims shows 5% agreed that further attacks by British suicide bombers in the UK are justified. This report also indicated that there were about 80 people actually involved in violent jihad. Other surveys showed that the British Muslims reported their primary identity as being Muslims (rather than reporting their dominant identity as British); they held more positive views toward jihad and martyrdom than their fellow citizens (Ansari et al., 2006); 13% of British Muslims believed that the persons who bombed the London subway system in July 2005 were Martyrs for Islam; and 49% believed that the U.S. military actions in Iraq were an attack against Islam (Wicker, 2007). Consistent with these research findings, Canadian research indicates the prevalence of Middle Eastern extremist ideologies among samples from western and non-western countries (Ahmed, Audu, Loza, & Maximenco, 2013; Loza, 2010a; Loza, 2010b; Loza, El-Fatah, Prinsloo, Hesslink, & Seidler, 2011). More recently, results of a Canadian study conducted by Loza, Bhawanie, Nussbaum, & Maximenco (2013) indicated significant differences between new Muslim immigrants to Canada from Pakistan and their Christian countrymen on all subscales that measure extremist ideologies, political, religious beliefs. Particularly unsettling was the finding that the highest difference occurred on the subscale reflecting the condoning of jihad. Consistent with these figures, Fatah (2014a) reported that the problem of radicalization is widely entrenched and embedded among Somali, Bangladeshi, and Pakistani Canadians. Unfortunately, the prevalence of these ideologies may have contributed to the home grown terrorism that we have seen of late.

Research also indicates the prevalence of extreme Middle Eastern ideologies among incarcerated offenders (Loza, 2010b) and support the concerns expressed by several Western prison administrators regarding the trend of radicalizing offenders while they are serving sentences in Western prisons. The results of this study are reinforced by the recent terrorist attacks in Paris. Said Kouachi, Cherif Kouachi, and Amedy Coulibaly, the radicalized Islamic terrorists who murdered journalists, police, and civilians in Paris spent time in jails. Similarly, other terrorists such as Mohammed Merah (Toulouse, France Massacre 2012) Alton Nolen (the

Oklahoma beheading), Michael Zehaf Bibeau (attack on Canadian Parliament) and Carlos Bledsoe (Arkansas Army Recruiting Station) were released from prison before committing their ideologically-motivated and heinous acts. Indeed, the entire ISIL command and control structure was formulated by its leaders, including its emir, Abu Bakr al-Baghdadi, while incarcerated in Camp Bucca prison in Iraq. All were subsequently released when the prison was turned over to Iraqi officials (Dunleavy, 2015).

The above information demonstrates that Canada, and other Western countries, are in need of a comprehensive plan, which includes two components: one for preventing extremism/terrorism and the other for intervening/rehabilitating convicted terrorists. However, a review of the available information indicates that Canada lacks effective plans and strategies for designing and implementing meaningful prevention and rehabilitative intervention for potential extremists/terrorists and convicted terrorists.

Current Prevention Programs In Canada

There are two known programs in existence in Canada today. One program was designed by Muhammed Robert Heft, a convert to Islam, as a 3-step de-radicalization program for radical Muslim Canadians. Through this program Heft has, "helped many youth who have turned towards radicalization and brought them away from that destructive state." Commentators have also noted that, "The R.C.M.P. and other Canadian policing agencies acknowledge and recognize his work in de-radicalization and counter terrorism." Heft is also responsible for starting, "the development of CAN-Bridge, whose goal is to facilitate a more formal and successful relationship between Western governments and Muslim communities," and, "Amongst many of its services, CAN-Bridge will help with outreach; develop de-radicalization programs, training, workshops and seminars for both Muslim communities and government agencies alike." It is also reported that he developed the, "'12-Step Extremist Detox Program' that is being offered at a Toronto mosques for young Islamic radicals who are sympathetic to the terrorist group al Qaeda [sic]."

The second program was developed by Sayyid Ahmed Amiruddin as a 12-step radicalization prevention program.2 Further to this, Amiruddin has appeared before the special senate committee on anti-terrorism (Parliament of Canada, Ottawa, October 4, 2010) on a method of psycho-spiritual rehabilitation therapy that he developed based on the Sufi approach, and applied his methodology to create a twelve-step radicalization prevention program. He reported that over 50 mosques and Islamic organizations throughout Canada have since privately endorsed his de-radicalization program to their congregations. Amiruddin claimed that a number of his clients underwent a radicalization process and were successfully recruited for the "jihad against Canada." He reported that his program utilizes the services of psychologists and psychiatrists, and that his program deals with: "hyper-religiousity, which is a diagnosed system of bi-polar disorder treated with prescription drugs"; decreasing in anti-Semitism (which they found to be a main driver in radicalization); and in reducing anti-Western attitude and "increase participation in our democratic process." Amiruddin also reported that his program works, and that they are confident it will save lives and is of benefit to all Canadians.

Amiruddin further stated that one of the "primary signatures of those individuals who are receptive to extremist manipulation, is their rejection, for example, of Sufism as a discipline within Islam altogether. Those groups within, generally, the Sunni group that may have literature available to their congregations, which may actually be conducive to radicalization, they of course would reject our arguments [sic]."

He also stated that, "by the time an individual completes the 12 steps of our program, the traces and vestiges of extremism are wholly uprooted from them."

Amiruddin believes one way of measuring the success of his program, "would be definitely the media and occurrences of terrorist or home-grown terrorist cases [sic]." He stated that another would be, "by working closely with partners and the police, any reports or complaints they want to share with us as a community-

based organization. Another way is through surveys and different privately obtained data that we would carry out within the community." During the senate hearing, one of the senators hailed this program as "an excellent program" and that, "the program is a logical solution to preventing radicalization."

From the available information there are many questions to be asked about the above mentioned Canadian programs prior to judging them as "excellent" or as presenting, "a logical solution to preventing radicalization." For example, it is not clear how the candidates are identified, or what the referral and selection process is. Additional questions include: what is the program content?; What is being delivered?; What are the methods of delivery?; What are the qualifications of the program designer(s) and delivery staff beside being a convert to Islam or an Imam?; How is the program designed?; What are the program components?; and, Is every participant diagnosed as suffering from bi-polar disorder and treated with prescription drugs? In the absence of an independent content evaluation and objective outcome data, it is hard to evaluate the efficacy of these programs as all of these questions and more are left unanswered. It is also concerning that the staff administering these programs are not from the Middle East, and have no firsthand information about the Middle Eastern culture, values, and political systems. In addition, the second program is administered by an Imam who is — according to him — a Sunni Sufi Muslim authority in the Naqshbandi Sufi Order (personal communication). This explains the Imam's testimony that the radicalized Sunni's, "of course would reject our arguments."

New Prevention Programs

Recently it was reported that the Royal Canadian Mounted Police (RCMP) is planning to implement a program called "Prevent" that is currently used in England (a brief description of this program is sited below). Beside the shaky history and numerous serious criticisms of this program, it is entirely premature to predict how effective this program would be in Canada, given the different profile for extremists between the two countries and the different socioeconomic backgrounds (Valdmanis, 2014).

Availability Of Rehabilitation Programs For Convicted Terrorists In Canada

From personal experience and from available information, it is evident that the Correctional Service of Canada (CSC; the Canadian federal penitentiary system) does not have a program specifically designed to rehabilitate incarcerated terrorists. It is worth noting that Ali Mohamed Dirie—one of the Toronto 18 who served a total of seven years for his part in the plot to blow up Parliament and attack politicians—managed to leave Canada while on conditional release, joined ISIL, and was reportedly killed there.

The Consulting Body For The Decision Makers Of The Government Of Canada

The Cross-Cultural Roundtable on Security (CCRS)3 consists of 15 citizens appointed by the Ministers of Public Safety and Justice to advise the Government of Canada on matters relating to national security. The members of the CCRS are community leaders who have extensive experience in social and cultural matters, but are members of the CCRS as individuals. Members of this committee have outstanding credentials and expertise; however, it seems that the majority of them are not originally from the Middle East and their hands-on knowledge of Middle Eastern politics, culture, values, language, and history is minimal. None of them could be considered a religious authority in Sunni Islam or expert on extremism/terrorism.

"The members of the CCRS are community leaders who have extensive experience in social and cultural matters, but are members of the CCRS as individuals."

Examples Of Available Prevention And Rehabilitation Programs In Other Countries

England: The "Prevent" program is one of the four "P's" that make up the government's post 9/11 counter-terrorism strategy: Prepare for attacks, Protect the public, Pursue the attackers and Prevent their radicalization in the first place. The "Prevent" program has been widely criticized as ineffective, and despite millions of pounds spent, the strategy remains deeply controversial and the program is virtually impossible to fully assess and incapable of achieving its goals. Recent reports indicate that this program has failed to stop the flow of British fighters joining Islamic State. The program was overhauled in 2011 after it found some of its projects unwittingly funded by groups that supported

extremist ideologies. The efforts have failed to stop the flow of British fighters joining the Islamic State (Valdmanis, 2014).

Egypt: Since 1928 Egypt has witnessed many terror attacks committed by Muslim extremist Jema'a Islamia, and Jihad's group. Egypt is probably the first in the world to develop methods of dealing with terrorism. In the 1990s the government adopted two strategies for dealing with these groups. The first was harsh and included military courts, hanging, lengthy detention of members of Muslim extremists' groups. The second was a soft approach, which included religious leaders, where some leaders of the ex-members visited detainees and inmates to convince them to abandon violence and build peace. In 1997, Egypt's two fiercest Islamic terrorist groups renounced the use of violence (Rashwan, 2009, Blaydes and Rubin, 2008; Zena, 2002). The Egypt program died with the passing of time. However, the events of July 2013 followed the Brotherhood being ousted from power. Unprecedented violence followed subsequently at the hands of Muslim Brotherhood, with thousands killed and maimed, with government and other properties destroyed, and 60-80 churches burned. All of this indicate that Egypt's strategies for combating extreme Islamic terrorism were not effective.

Saudi Arabia: Riyadh's Care Rehabilitation Center is an institution that integrates convicted terrorists into Saudi society through religious re-education, psychological counseling, and assistance in finding a job, vocational training, art therapy, sports, and religious re-education. The program aims to address underlying factors that led the individual to choose terrorism. Beneficiaries—those participating in the program—live in dorm-style housing. There is a pool, soccer field, volleyball court, PlayStation, television, and an art therapy facility. Participants' families are also recruited as a source for their recovery. The guiding philosophy, the leaders of the program explain, is that jihadist are victims, not villains, and they need tailored assistance (El-Saeed, 2010; Gunaratna 2011; Stern, 2009.) It is reported that a former Guantanamo detainee who was enrolled in the program took off for Yemen and became the deputy leader of Al Qaeda in Yemen. Furthermore, the Saudi government reported that eleven of the Riyadh's "graduates" returned to terror, and are now on the Saudi list of most-wanted terrorists. (Gunaratna, 2011, Stern, 2009). Fatah (2014a) reported that everyone released from Guantanamo under Saudi Arabia guarantee is now fighting with ISIS.

Singapore: Singapore's program offer their detainees a combination of psychological, vocational, counselling and rehabilitation programs. "The most powerful is religious rehabilitation. Religious rehabilitation has the power to unlock the mind of a detainee or an inmate. It has the power to make a beneficiary of rehabilitation repent, become remorseful and re-enter the mainstream".

The wives also receive counselling and the whole family is provided with social and community assistance (Gunaratna, 2011).

Indonesia: The Indonesians utilize ex-terrorists as a central part of their disengagement process. They utilize former leaders to prevent radicalization of Indonesian youth. One of the former leaders explains to captured terrorists how they have "misunderstood" the Islamic struggle and "the meaning of Jihad." Also, he challenges detainees' Islamic justifications for armed action against civilians. The lack of transparency surrounding official statistics about program success call their statistics into question (Horgan & Braddock, 2010)

Yemen: Yemen's program is administered by the Religious Dialogue Committee (RDC). To achieve attitude change, the RDC debates with those captured and imprisoned. The RDC challenge militants on their understanding of the verses of the Quran. Discussion includes: the place of jihad in Islam and its justifications; the relations of the Muslims and others; and the concept of the State, government, and ruler rights within Islam. The head of the RDC claims that after weeks of debate, if the prisoners renounce violence, and if applicable, the terror groups they were part of, they are released and offered vocational training and help finding employment. Most claims of success—if not all—come directly from the RDC. Most skepticism of the RDC's success rates is surrounding their highly subjective views about what constitutes terrorism as opposed to "legitimate resistance," which can skew program results. Recent years have seen the RDC's achievements called into question. An attack on the U.S. Embassy in Sana'a, with two or three of the attackers allegedly graduates of RDC's program, is not a good indication of this program's reported success (Hogan & Braddock, 2010).

Observations

Although all programs claim success, the main focus among all of these programs is commonly on religion. They are not adhering to the principles of effective correctional programming, not designed and deliver by experts in human behaviour, and have no proper or systematic evaluation.

After 9/11 Canadian professionals (mostly non-clinicians) ventured into the complex field of Middle Eastern extremism despite their most important credential only being an Imam, a Sheekh, or a convert to Islam. Having a superficial knowledge of this

topic has hindered progress towards designing and delivering effective programs. For the last decade, they have presented themselves as experts and even developed intervention programs. Unfortunately, very few of these so-called experts possess the necessary background to undertake these tasks. The majority have acquired their knowledge through news media and books. The involvement of these pseudo-experts has been causing—and will continue to cause—more harm than good. Many salient issues related to Middle Eastern extremism are alien to western culture and, consequently, not easily grasped by westerners through theoretical means. Most of these experts are at the disadvantage of not having in-depth, first hand understanding or knowledge of the history, culture, ideologies, values, language, religion, history, ethnicity, regions, customs, and political and social backgrounds of the dominant or minority Middle East populations (Loza, 2012). Political correctness and over sensitivity regarding addressing religious issues are factors that hamper serious contribution from concerned and credible researchers (Loza, 2007).

To build a global regime to rehabilitate terrorists, governments with the expertise and resources need to pave the way and create a path for other nations to follow. Every successful program requires a long-term investment of intellectual and other resources. The Correctional Service of Canada (CSC) is a world leader in the development and implementation of correctional programming. All CSC programs are designed using the principles of risk, need, and responsivity, and have demonstrated effectiveness. Therefore, it is opined that the CSC have the knowledge, resources, and commitment needed to develop programming to combat terrorism that is not heavily loaded with religious components. It should be noted that the content of terrorism programming is different from other current CSC programs; indeed, our expertise and resources make the CSC qualified to take on this ambitious endeavor.

Program Design And Important Characteristics:

Prior to implementation, the programs must be subject to rigorous studies and must be peer reviewed to ensure their efficacy. These programs must include strong periodic and end-of-program evaluation components for each participant to measure progress against program targets. In addition, there must be follow-up components so progress of participants can be tracked over time. Programs must be sensitive to the Canadian culture, values, beliefs, and community characteristics.
Prior to commencing any form of programming, each individual must complete an assessment process. This assessment will include information gathering regarding psychosocial history and an estimated level of risk for recidivism should the individual not receive treatment. This assessment is vital to the success of any program as it will allow the clinicians to tailor the program to each individual terrorist/extremist as each of their circumstances will differ. The makeup of terrorists'/extremists' personalities, backgrounds, and circumstances differ and, as such, no specific program will fit for all. Therefore, it is vital that programs used with this population have two components: a group component (that will benefit all participants) and an individual counselling component (that is designed to cover the terrorist's specific needs).

In order to fully address the growing issue of terrorism in Canada and the west, two programs are needed: one to prevent new recruitments into terrorist organizations, and a second to rehabilitate convicted terrorists.

Prevention Programs:

The internet has been playing an important role in the recruitment of new terrorists. Counter-recruitment/prevention programs need to be proactive. There may be a need to initiate internet sites to expose and challenge the extreme ideologies, and to help with early identification of possible terrorists to engage with them or intervene. To my knowledge, no country has yet to

implement a counter-attack policy using the same methods as terrorist organizations use to entice youth to join their cause. The conjoined interactivity of electronic and visual media seems to be the most compelling combination of conversion tools utilized by terrorist organizations. For example, Jack Roche of Australia made a conversion decision to follow jihad after viewing a video of alleged atrocities suffered by Muslims, similar to what occurred in Indonesia (Hairgrove & Mcleod, 2008). Identical methods are used in Canada and other parts of the world, including websites, chat boards, games, hip-hop bands, and blogs. These could be extremely effective components of a prevention program by helping expose and challenge extreme ideologies, provide early identification of possible terrorists, and intervene with them.

In addition, program designers must pay attention to the importance of developing group cohesion. This has been utilized by terrorist recruiters through small groups, as they provide mutual emotional and social support, development of common identity, and encourage members to adopt new faith positions (Hairgrove and McLeod, 2008; Sageman, 2004). Government and nongovernment agencies could support the development of small groups' teaching materials by using credible teachers and multiple languages made available through Muslim book distributors, or free for online download (a similar recommendation was offered by Rabasa, Benard, Schwartz, and Sickle (2007)). It is important that such materials be made simple enough to produce small-sized files, which can be efficiently transmitted over limited-capacity internet channels Those who are at risk for adopting a new faith usually do so because they are looking to try new things, are looking for change, are bored, want a way out of their routine life, are looking for acceptance, want to be different, looking for fulfillment or status, camaraderie, and self-actualization. Something about the new religion resonated within them. The precipitating "need state" is often preceded by some disturbing or troubling event such as loss of a job, loss of a relationship, or other personal problems (Loza, 2007). Some of these individuals could be prevented from joining violent terrorist organizations if these needs were fulfilled through prevention programs that include counselling. Additionally, Horgan and Braddock (2010) suggested encouraging youth-at-risk for joining violent groups to join a non-violent Islamic network could allow them to achieve the benefits they were seeking from group membership without the requirements to engage in jihad.

Rehabilitation Programs:

The most successful offender rehabilitation models focus on the individual offender, with intervention based on an assessment of what caused the offender to commit the crime. The ideal model includes prison-based rehabilitation programs, followed in turn by transitional services, and community after-care services (Stern, 2009). Rehabilitation programs must deal with the motivation, risk, needs, and responsivity of each individual convicted terrorist (Andrews, 2001). Loza (2007) warned that extremism and terrorism are increasing and there is an urgent need for a multifaceted research and rehabilitation programs that utilize several disciplines to help with possible solutions to the problem. As well, offering correctional staff training on Middle Eastern extremist ideologies could help with the rehabilitations efforts. De-radicalization efforts are complicated endeavors. There must be appropriate intervention for offenders who have been convicted for Islamist extremism/terrorism one that focuses on targeting extremist beliefs and ideologies, attitudes, attributions, behavior, thinking with follow up/ maintenance programs.

Regarding staffing, there is a need for a team of professionals including a Muslim cleric (Imam/Sheik) who is qualified to offer religious counselling and is well-versed in the issues related to Middle Eastern extremism/terrorism (M.E.T). As well, the team should include a psychologist with expertise in the culture, language, ideologies, religious background of the offenders, and someone who has a good understanding of issues related to M.E.T. Not every Imam or psychologist will be able to provide the required counselling. Since the majority of religious programing did not produce the desired results, new programs are needed with a good portion of these programs focusing on psychological intervention.

Program Content: Programs must address extremists' Middle Eastern ideologies that promote Jihad, establishing Kalifat political system, superiority, the general negative feelings, thinking, beliefs, motivations, and cognitions about the groups of people whom terrorists/extremists are against, as well, individualized counselling that covers the specific needs of each terrorist/extremist.

Program Staff: It is imperative that appropriate staff be selected to deliver the two programs. Appropriate staff include those who understand the Middle Eastern culture and values. Imams may not be the best option for taking a leading role in rehabilitation programs as they may not be a good option to deal with those who have already become radicalized (Fatah, 2014a); indeed, sometimes those who are radicalized reject anti-jihadi Imams as heretics. In Egypt the Muslim Brotherhood rejected counselling from religious leaders and Imams. They accused them of being much too close to the authority.

However, interventions operated by former members of the group may have a greater chance of successful engagement with current members. The former members have credibility and have detailed knowledge of the motivations and aims of the group. All program staff should be thoroughly trained, and clinical supervision should be provided. According to Andrews (2001), the most important element in a successful program is the qualification and training of the people delivering the programs.

It is suggested that staff designing and delivering programs be thoroughly knowledgeable about ideological contexts, the history, culture, ideology, values, language, religions, ethnicity, region customs, and political and social backgrounds of the population in question prior to undertaking assessments or designing interventions for extremists/terrorists. This would involve physically spending years of living in different countries of the Middle East. Not every Muslim or converted Muslim is expert in assessing and providing interventions for terrorists. Besides acquiring the necessary knowledge about terrorism, it takes years of studies and learning about program designs and counselling to become a qualified expert. Many programs look good on paper because they utilize an Imam or converted Imam with little or no training in psychology or program design and implementation; however, they yield questionable results as they do not utilize the expertise of qualified staff.

Program components should include countering extreme ideologies with other ideologies that are not religiously based. These may make terrorists interests and views more balanced and promote more loyalty to their current countries and their democratic political system. Perhaps most fundamentally, we need to educate western populations and politicians about the ideologies of extremists and their dangerous consequences, counter the extremist strategy of isolation, and the notion of "them" vs. "us" by increasing and strengthening integration and assimilation policies. In practice, this will involve avoiding the notion of cultural uniqueness as a means to isolate groups through separate and exclusive school systems, cultural neighbourhoods, and the monitoring of teachings in religious institutions. Politically unpopular, it will be necessary to rethink immigration and refugee policies with the goal of balancing the ratio of immigrants according to religion, mandating total loyalty to their newly adopted countries, countering the extremists' long-term strategy of overwhelming the Western countries through increasing their numbers while using the democratic process to impose their views, and educating the public and policy makers about the issue of abusing freedom of expression and democracy that extremists use to promote their ideas and ideologies in the West (Loza, 2007).

Perhaps most fundamentally, we need to educate western populations and politicians about the ideologies of extremists and their dangerous consequences, counter the extremist strategy of isolation, and the notion of "them" vs. "us" by increasing and strengthening integration and assimilation policies.

Dr. Wagdy Loza is an Adjunct Assistant Professor of Psychiatry at Queen's University, a Member of the Ontario Review Board (Ontario), Chief Psychologist, a retired member of Correctional Service of Canada, former Adjunct Professor of Psychology at Carleton University, and former Chair of the Extremism/ Terrorism section of the Canadian Psychological Association (CPA).

The Rising Threat of Lone Wolf Terrorism

This interview with Andrew Majoran, Former General Manager of The Mackenzie Institute was originally published by CMS Strategic in April 2015.

1. Is lone wolf terrorism a new phenomenon? If so, why has it come about?

Terrorism is not a new concept at all, but as time goes on, terror tactics evolve. The "lone wolf" or "solo-terrorist" was popularized by American white supremacists Tom Metzger and Alex Curtis of the Anti-Defamation League in the early 1990s. They believed that underground activity at the individual level is the most effective means of promoting an agenda. According to Metzger and Curtis' model, lone wolf operations leave behind the least evidence for law enforcement authorities, which dramatically decrease the chances that terrorists will get caught. The tactics described by Metzger and Curtis have increased in popularity, with lone wolf tactics gradually ushering in a new era in terrorism.

This evolving trend in terror tactics is evident in recent events wherein individual terrorists have produced more frequent and deadly outcomes. In 1995, Timothy McVeigh killed over 150 people and injured over 500 hundred more in a lone wolf bomb attack on a Federal building in Oklahoma City. In November 2009, Nadal Hasan, a U.S. Army Major and Psychiatrist, killed 13 and injured dozens more in an attack on the Fort Hood military base in Texas. More recently, in August 2011, Anders Breivik killed 77 individuals in a bombing and mass shooting attack in Norway. These incidents are just a small sample of the many lone wolf style terrorist attacks that have occurred in the western world in the last 30 years. It is becoming more and more evident that operating at the individual level directly correlates with the successful completion of terrorists' goals.

2. How has terrorism evolved in recent years?

The standard view of a terrorist being a young, naive, impoverished male is no longer accurate. Terrorists today are highly educated individuals who come from every community you can imagine. Many of the individuals currently orchestrating ISIL's strategy come from good families and have high-level western education. Radicalization is something that differs from case to case, and must be understood from a psychological standpoint. To answer the question, terrorism has evolved dramatically in recent years. Terrorist groups like ISIL have gained sympathizers and foreign fighters from across the globe, and they have effectively used social media to promote violent jihad against their enemies. The social reach that modern terrorist groups have displayed in recent years correlates directly with the subsequent rise in lone wolf style attacks, as sympathizers have been inspired to plan and commit terrorist acts in isolation, instead of joining the ranks of a larger traditional terrorist group.

3. Is there a common trend in lone wolf terrorists?

If history is any indication, lone wolf terrorists come in many forms. Religion, race, sex, and ethnic background have proven to be irrelevant factors. The primary danger associated with lone wolf terrorists is that they act in isolation, severely limiting the chances of them being discovered. Although Islamic extremism is the largest of the terrorist threats at present, there have been a large amount of lone wolf attacks committed by individuals who do not fit that description. For example, the worst lone wolf attack committed on Western soil to date was actually committed by a white, Christian male, Anders Breivik, in Norway, which draws into question the typical belief that terrorists sympathize Islamic fundamentalism. The only trend that is evident with lone wolf style terrorists is that they sympathize with a particular cause to the point of violent radicalization, and they choose to commit terrorist acts in isolation.

4. Is there a requirement for civil and military powers to work together?

Yes, cooperation at all levels is paramount to the success of countering all forms of violent extremism. Governments must use the tools they have available to them to ensure that their public are safe. The private sector must ensure that the promotion of security and well-being are held in the highest regard. Both civil society and government must cooperate to ensure violent extremism and radicalization are being combatted from all directions, be it at the law enforcement and intelligence level, or the grassroots and educational level. When it comes to security, civil society and government operating on different levels would be counter-intuitive, and would likely have disastrous results. Cooperation is integral.

References

Cyber Triggers and The First Strike Dilemma, Page 12

1 Walter Isaacson, David Sanger, & Michael Rogers, Beyond the Build: Leveraging the Cyber Mission Force, A Presentation before a Conference at the Aspen Institute, July 23, 2015, http://aspen-securityforum.org/wp-content/uploads/2015/07/Beyond-the-Build-Leveraging-the-Cyber-Mission-Force.pdf.
2 Bill Gertz, "US Intelligence Community Report: America's Weak Response to Cyber Attacks Will Encourage More Breaches," Business Insider, July 28, 2015, http://www.businessinsider.com/us-response-to-cyber-attacks-will-encourage-more-2015-7.
3 Paul McLeary, "NATO Chief: Cyber Can Trigger Article 5," DefenseNews, March 25, 2015, http://www.defensenews.com/story/defense/policy-budget/warfare/2015/03/25/nato-cyber-russia-exercises/70427930/ .
4 James R. Clapper, Statement for the Record, Worldwide Threat Assessment of the US Intelligence Community, Senate Select Committee on Intelligence, March 12, 2013, http://www.dni.gov/files/documents/Intelligence%20Reports/2013%20ATA%20SFR%20for%20SSCI%2012%20Mar%202013.pdf.
5 James R. Clapper, Statement for the Record, Worldwide Threat Assessment of the US Intelligence Community, Senate Select Committee on Intelligence, January 29, 2014, http://www.dni.gov/files/documents/Intelligence%20Reports/2014%20WWTA%20%20SFR_SSCI_29_Jan.pdf
6 James R. Clapper, Statement for the Record, Worldwide Threat Assessment of the US Intelligence Community, Senate Select Committee on Intelligence, February 26, 2015, http://www.dni.gov/files/documents/Unclassified_2015_ATA_SFR_-_SASC_FINAL.pdf.
7Jake Tapper, "Leon Panetta: A Crippling Cyber Attack Would Be 'Act of War'," ABC News, May 27, 2012, http://abcnews.go.com/blogs/politics/2012/05/leon-panetta-a-crippling-cyber-attack-would-be-act-of-war/.
8 Leon E. Panetta, Defending the Nation from Cyber Attack, Speech Presented to Business Executives for National Security, Washington D.C.: U.S. Department of Defense, Office of the Assistant Secretary of Defense (Public Affairs), October 12, 2012.
9 Deborah Charles, "U.S. homeland chief: cyber 9/11 could happen 'imminently'," Reuters, January 24, 2013 http://www.reuters.com/article/2013/01/24/us-usa-cyber-threat-idUSBRE90N1A320130124.
10 Ray Suarez, "Examining Cyber Security With Homeland Security Secretary Janet Napolitano," PBS Newshour, February 15, 2013 http://www.pbs.org/newshour/bb/science/jan-june13/cybersecurity_02-15.html.
11 Mark Clayton, "Energy sector cyberattacks jumped in 2012. Were utilities prepared?" Christian Science Monitor, January 7, 2013, http://www.csmonitor.com/Environment/Energy-Voices/2013/0107/Energy-sector-cyberattacks-jumped-in-2012.-Were-utilities-prepared?nav=627893-csm_article-leftColRelated.
12 David E. Sanger and Thom Shanker, "Broad Powers Seen for Obama in Cyberstrikes," The New York Times, February 3, 2013, http://www.nytimes.com/2013/02/04/us/broad-powers-seen-for-obama-in-cyberstrikes.html?_r=2&.
13 Ibid.
14 Barak Obama, Executive Order: Improving Critical Infrastructure Cybersecurity, February 12, 2013 http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.
15 The White House, Presidential Policy Directive/PPD-21: Critical Infrastructure Security and Resilience, February 12, 2013, http://www.fas.org/irp/offdocs/ppd/ppd-21.pdf.
16 The White House, Remarks by the President in the State of the Union Address, February 12, 2013, http://www.whitehouse.gov/the-press-office/2013/02/12/remarks-president-state-union-address.
17 Ralph Langner and Perry Pederson, Bound to Fail: Why Cyber Security Risk Cannot Simply Be 'Managed' Away, February 2013, http://www.brookings.edu/research/papers/2013/02/cyber-security-langner-pederson.
18 Cynthia E. Ayers, "EMP Effects and Cyber Warfare (Parts I and II)," The Jewish Voice, February 26, 2014 and March 6, 2014, http://jewish-voiceny.com/index.php?option=com_content&id=6777:emp-effects-and-cyber-warfare--part-i&Itemid=301 and http://jewishvoiceny.com/index.php?option=com_content&id=6882:emp-effects-and-cyber-warfare--part-ii&Itemid=301.
19 Verizon, 2013 Data Breach Investigations Report, 2013, http://www.secretservice.gov/Verizon_Data_Breach_2013.pdf, p. 59
20 Leon Panetta, "Defending the Nation from Cyber Attack."
21 Prescott E. Small and Pedro Bueno, Defense-in-Depth: An Impractical Strategy for a Cyber World, SANS Institute, November 14, 2011, http://www.sans.org/reading-room/whitepapers/warfare/defense-depth-impractical-strategy-cyber-world-33896.
22 Department of Homeland Security and the National Cybersecurity and Communications Integration Center, ICS-CERT Year in Review, 2014, https://ics-cert.us-cert.gov/sites/default/files/documents/Year_in_Review_FY2014_Final.pdf, p. 4.
23 Leon Panetta, "Defending the Nation from Cyber Attack."
24 Warwick Ashford, "Obama Threatens Foreign Cyber Attackers With Sanctions," Computer Weekly, February 13, 2015, http://www.computerweekly.com/news/4500243644/Obama-threatens-foreign-cyber-attackers-with-sanctions.
25BBC News, "Sony Hack: Obama Vows Response as FBI Blames North Korea," BBC.com, December 19, 2014, http://www.bbc.com/news/world-us-canada-30555997.
26 Michael Daniel, Our Latest Tool to Combat Cyber Attacks: What You Need to Know, April 1, 2015, https://www.whitehouse.gov/blog/2015/04/01/our-latest-tool-combat-cyber-attacks-what-you-need-know.
27Anya Litvak and Deborah M. Todd, "BlackEnergy Malware Threat Has Some Uneasy," Pittsburg Post-Gazette, November 11, 2014, http://powersource.post-gazette.com/powersource/companies/2014/11/11/Black-Energy-spooks-nation/stories/201411110080; Lucian Constantin, "New Havex Malware Variants Target Industrial Control Systems and SCADA Users," IDG News Service, June 24, 2014, http://www.pcworld.com/article/2367240/new-havex-malware-variants-target-industrial-control-system-and-scada-users.html.
28James R. Clapper, Statement for the Record, Worldwide Threat Assessment of the US Intelligence Community, Senate Select Committee on Intelligence, February 26, 2015.
29 Bill Gertz, "US Intelligence Community Report: America's Weak Response to Cyber Attacks Will Encourage More Breaches."
30 Ralph Langner, To Kill A Centrifuge: A Technical Analysis of What Stuxnet's Creators Tried to Achieve, The Langner Group, November 2013, http://www.langner.com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge.pdf.
31Hal Schwartz, "6 Times U.S. Agencies Were Hacked Before the Pentagon," DCInno, August 8, 2015, http://dcinno.streetwise.co/2015/08/08/federal-cybersecurity-hacks-opm-pentagon-irs-white-house/.
32Jake Tapper, "Leon Panetta: A Crippling Cyber Attack Would Be 'Act of War'."
33 Congressional EMP Commission, Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack: Critical National Infrastructures, Washington, DC, 2008; and The Committee on the Societal and Economic Impacts of Severe Space Weather Events, Severe Space Weather Events: Understanding Societal and Economic Impacts, The National Research Council of the National Academies, Washington, DC: The National Academies Press, 2008.
34 David J. Smith, "Russian Cyber Strategy and the War Against Georgia," Infocus Quarterly, January 17, 2014, http://www.atlanticcouncil.org/blogs/natosource/russian-cyber-policy-and-the-war-against-georgia

Restoring Accountability for Telecommunications Surveillance in Canada, Page 19

1 Dr. Christopher Parsons received his Bachelor's and Master's degrees from the University of Guelph, and his Ph.D. from the University of Victoria.
2 Bill C-51: An Act to enact the Security of Canada Information Sharing Act and the Secure Air Travel Act, to amend the Criminal Code, the Canadian Security Intelligence Service Act and the Immigration and Refugee Protection Act and to make related and consequential amendments to other Acts.
3 Bill C-13: An Act to amend the Criminal Code, the Canada Evidence Act, the Competition Act and the Mutual Legal Assistance in Criminal Matters Act.
4 See: Christopher Parsons. (2015). "Stuck on the Agenda: Drawing lessons from the stagnation of 'lawful access' legislation in Canada," Michael Geist (ed.), Law, Privacy and Surveillance in Canada in the Post-Snowden Era (Ottawa University Press).
5 See Access to Information and Privacy document released by Public Safety Canada, A-2011-00220.
6 Gowlings, for the Canadian Wireless Telecommunications Association. (2011). "Re: Response to Request for General Information From Canadian Wireless Telecommunications Association (the "CWTA") Members," Gowlings. December 11, 2011.
7 Christopher Parsons. (2015). "The Governance of Telecommunications Surveillance: How Opaque and Unaccountable Practices and Policies Threaten Canadians," Telecom Transparency Project, http://www.telecomtransparency.org/wp-content/uploads/2015/05/Governance-of-Telecommunications-Surveillance-Final.pdf.
8 Criminal Code, 1985, s.195.
9 Christopher Parsons. (2015). "The Governance of Telecommunications Surveillance: How Opaque and Unaccountable Practices and Policies Threaten Canadians," Telecom Transparency Project, http://www.telecomtransparency.org/wp-content/uploads/2015/05/Governance-of-Telecommunications-Surveillance-Final.pdf.
10 Nicholas Koutros and Julien Demers. (2013). "In Big Brother's Shadow: Historical Decline of Electronic surveillance by Canadian Federal Law Enforcement," Social Sciences Research Network, last revised March 15, 2013, retrieved December 2, 2014, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2220740.
11 Public Safety Canada. (2014). "Annual report on the use of electronic surveillance - 2013," Government of Canada, last modified August 27, 2014, retrieved June 30, 2015, http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/lctrnc-srvllnc-2013/index-eng.aspx
12 Public Safety Canada. (2014). "Annual report on the use of electronic surveillance - 2013," Government of Canada, last modified August 27, 2014, retrieved June 30, 2015, http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/lctrnc-srvllnc-2013/index-eng.aspx; Matthew Braga. (2014). "New Documents Show Thousands of Unreported Wiretaps by Canadian Cops," Motherboard, November 20, 14, retrieved November 26, 2014, http://motherboard.vice.com/en_ca/read/new-documents-show-thousands-of-unreported-wiretaps- by-canadian-cops.
13 Minister of Public Safety and Emergency Preparedness's Responses to MP Charmane Borg's Q-233 Order Paper Questions, March 24, 2014, retrieved January 17, 2015, https://www.christopher- parsons.com/Main/wp-content/uploads/2014/03/8555-412-233.pdf.
14 See Access to Information and Privacy document released by Public Safety Canada, A-2011-00220.
15 Public Safety Canada. (2013). "Annual report on the use of electronic surveillance - 2013," Government of Canada, last modified August 27, 2014, retrieved June 30, 2015, http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/lctrnc-srvllnc-2013/index-eng.aspx;
16 Security Intelligence Review Committee. (2014). "2013-14 Department Performance Report," Government of Canada, October 24, 2014, retrieved October 30, 2014, http://www.sirc- csars.gc.ca/opbapb/dprrmr/2013-2014/index-eng.html.
17 Peter Gill. (2989). "Symbolic or Real? The Impact of the Canadian Security Intelligence Review Committee, 1984-1988," Intelligence and National Security 4:3.
18Security Intelligence Review Committee. (2014). "2013-14 Department Performance Report," Government of Canada, October 24, 2014, retrieved October 30, 2014, http://www.sirc- csars.gc.ca/opbapb/dprrmr/2013-2014/index-eng.html.
19 Chuck Stahl. (2013). "The Standing Committee on National Security and Defence: Evidence," Parliament of Canada, December 9, 2013, retrieved March 15, 2015, http://www.parl.gc.ca/content/sen/committee/412%5CSECD/51109-E.HTM
20 Christopher Parsons. (2015). "Capturing the Security Intelligence Review Committee," Telecom Transparency Project, June 24, 2015, retrieved June 25, 2015, http://www.telecomtransparency.org/capturing-security-intelligence-review-committee/.
21 Office of the Privacy Commissioner of Canada. (2015). "Bill C-51, the Anti-Terrorism Act, 2015: Submission to the Standing Committee on Public Safety and National security of the House of Commons," Government of Canada, March 5, 2015, retrieved March 15, 2015, https://www.priv.gc.ca/parl/2015/parl_sub_150305_e.asp.
22 Office of the Communications Security Establishment Commissioner. (2004). "Communications Security Establishment Commissioner Annual Report, 2003 – 2004," Government of Canada, retrieved March 15, 2015, http://www.ocsec-bccst.gc.ca/ann-rpt/2003-2004/activit_e.php#4.
23 Bill Robinson. (2015). "Does CSE comply with the law?," Lux Ex Umbra: Monitoring Canadian Signals Intelligence (SIGINT) Activities Past and Present, March 14, 2015, retrieved March 15, 2015, http://luxexumbra.blogspot.ca/2015/03/does-cse-comply-with-law.html.

Organizational Resilience, Page 27

1 British Standard BS6500 'Organizational Resilience' 2014.
2Australian Government. Attorney-General's Department 2015
3 IBM 'Smarter continuity and resiliency' Canada 2015
4 British Standard BS11200 'Crisis Management' 2014
5 PwC. Rebuilding for resilience. Fortifying Infrastructure to withstand Disaster 2013
6 Roads to Resilience - Cranfield School of Management 2014
7 Measuring and Comparing Organizational Resilience. Australian Journal of Emergency Management Volume 25 2010
8 U.S. Homeland Security. Presidential Policy Directive / PPD-8: National Preparedness 2011
9 Aon 'Reputation Review' 2012
10 ISO 22316. Draft. Standard due April 2017
11 U.S. President Barack Obama. Chicago Illinois 5 February 2008

The Need for Effective Intervention Programs to Prevent Islamic Extremists and Terrorist Recruitment in Western Countries with Special Emphasis on Canada, Page 35

Ahmed, A.G., Audu, M.D., Loza, W. Maximenco, A. (2013). The Prevalence of Extreme Middle- Eastern Ideologies among Some Nigerians. International Journal of Social Science Studies
Andrews, D. A. (2001). Principles of effective correctional programs. In L. L. Motiuk & R. C. Serin (Eds.), Compendium 2000 on effective correctional programming (pp. 9-17). Ottawa: Correctional Services of Canada.
Ansari, H., Cinnirella, M., Rogers, M. B., Loewenthal, K. M., & Lewis, C. A. (2006). Perceptions of martyrdom and terrorism amongst British Muslims. In M. B. Rogers,
C. A. Lewis, K. M. Loewenthal, M. Cinnirella, R. Amlot, & H. Ansari (Eds.), Proceedings of the British Psychological Society Seminar Series Aspects of Terrorism and Martyrdom, eCOMMUNITY (pp. 1-5). International Journal of Mental Health & Addiction.
Arafa, M. G. (2015). ةعامجلا نيبنس مسخلا داصحو فنخلا فقو ترادابم ةيرصملا ةيمسلا :قوعو فنخو قوعو... ؟. Initiative of stopping violence and the fruits of five years of the Egyptian Islamic group, El-Islam El-Youm. Retrieved (2015-01-10), from http://www.islamtoday.net/bohooth/services/saveart-55-1151.htm
Bawer, B. (2006). While Europe slept: How radical Islam is destroying the West from within. New York: Doubleday.
Blaydes, L, Rubin, L (2008). "Ideological Reorientation and Counterterrorism: Confronting Militant Islam in Egypt," Terrorism and Political Violence, 20, 4, 461 – 479
Dunleavy, P. Special to IPT News (January 9, 2015). Another Ex-Con, Another Terrorist Attack – The Danger in Closing Gitmo: retrieved from http://www.investigativeproject.org/4729/guest-column-another-ex-con-another-terrorist
El-Saeed, N. M (2010). ألما ريبان فيي وجو يف نطول غرد ءارما باو ليطتسا فرطت: Prince Naief a shield in front of extremism and terrorism, Al Jazirah News Paper 09/06/2010 G Issue13768. Retrieved (2011/05/10) from: http://www.al-jazirah.com/2010/20100609/qr27.htm

Fatah, T (2014a; senate committee on terrorism: Nov 24). Retrieved (2014-11-26): https://themuslimissue.wordpress.com/2014/12/12/video-canada-senate-committee-on-national-security-nov-24-2014-opening-statement/
Fatah, T (November, 25, 2014b). The myth of 'de-radicalization' of Islamic radicals. Toronto sun. Retrieved (2014-11-26): http://www.torontosun.com/2014/11/25/the-myth-of-de-radicalization-of-islamic-radicals
Gunaratna, R (2011) Terrorist rehabilitation: a global imperative, Journal of Policing, Intelligence and Counter Terrorism, 6:1, 65-82,
Gunaratna, R, BIN ALI, M (2009). De-Radicalization Initiatives in Egypt: A Preliminary Insight: A Preliminary Insight. Studies in Conflict & Terrorism, 32:277–291, 2009
Gurfinkiel, M, (2015). France's moment of truth. Middle East Forum. Retrieved (2015-01-16). www.meforum.org/4980/france-moment-of-truth
Hairgrove, F., & McLeod, D. (2008). "Circles Drawing Toward High Risk Activism: The Use of Usroh and Halaqa in Islamist Radical Movements." Studies in Conflict & Terrorism (May): 399-411
Horgan, J., & Braddock, K. (2010).Rehabilitating the Terrorists?: Challenges in Assessing the Effectiveness of De-radicalization Programs. Terrorism and Political Violence, 22, 24.
Kareema, A.M (2015): . جماعة الاخوان المسلمين. رؤية نقدية شرعية. عام 2014 مصر _ الجيزة _ العياط وجزيرة الدهب. The group of Muslim Brothers: A critical view. El-Gizera, Cairo, El-Aiat.
Loza, W. (2010a).The prevalence of Middle-Eastern extreme ideologies among some Canadians. JIV, 26, 1388-1400.
Loza, W. (2010b).The prevalence of Middle-Eastern extreme ideologies among some Canadian offenders, JIPV, 25, 919-928.
Loza, W. (2007). The psychology of extremism and terrorism: A Middle-Eastern perspective. Aggression and Violent Behavior,12, 141–155
Loza, W (2012-May). Issues regarding the assessment and intervention with Middle-Eastern radicalization, extremism and its operational manifestation: terrorism. Crime Scene, Volume 19, Number 1: Canadian Psychological Association, Canada.
Loza, W. Abd-El-Fatah, Prinsloo, J., Hesselink, A., Seidler, K. (2010). The Prevalence of Extreme Middle-Eastern Ideologies Around the World. Journal of Interpersonal Violence, 2011 Feb; 26 (3):522-38
Loza, W., Bhawanie, S., Nussbaum, D., & Maximenco, A. (2013). Assessing the Prevalence of Extreme Middle-Eastern Ideologies among Some New Immigrants to Canada. International Journal of Social Science Studies, Vol. 1, number 2.
Leuprecht, C., Hataley, T., Moskalenko, S., & McCauley, C. (2009). Winning the Battle but Losing the War? Narrative and Counter-Narratives Strategy. Perspectives on Terrorism, 3(2). Retrieved from http://terrorismanalysts.com/pt/articles/issues/PTv3i2.pdf Long, D. (2004). Ecoterrorism. New York: Facts on File, Inc. Maslow, A. H. (1943). A Theory of Human Motivation. Psychological R
National Post (October 27, 2014). Michael Zehaf-Bibeau Threatened To Act 'In The Name Of Allah In Response To Canadian Foreign Policy': Source. http://news.nationalpost.com/2014/10/27/police-investigating-whether-michael-zehaf-bibeau-told-anyone-about-his-plans-before-ottawa-shooting/
Parliament of Canada, Ottawa (October 4, 2010): Proceedings of the Special Senate Committee on Anti-terrorism, Issue 7 – Evidence. Retrieved (2014-10-11) from: http://www.parl.gc.ca/Content/SEN/Committee/403/anti/07eva-e.htm?Language=E
Pipes, D. (2015). How terrorism harms radical Islam. Retrieved (2015-01-10) http://www.washingtontimes.com/news/2015/jan/9/daniel-pipes-how-terrorism-harms-radical-islam/print/).
Rabasa, A., Benard, C., Schwartz, L.H., Sickle, P (2007). Building Moderate Muslim Networks. Arlington, VA:Rand Center for Middle East Public Policy.
Rashwan, D. (2009). The renunciation of violence by Egyptian jihadi organizations. In Bojorgo and Horgan (Eds.) Leaving Terrorism Behind: Individual and collective disengagement. Routledge, London and New York.
Sageman, M. (2004). Understanding terror networks. Philadelphia: University of Pennsylvania Press.
Stern, J. (2009). How to Deradicalize Islamist Extremists, Mind Over Martyr, Foreign affairs, 89 No. 1, 98-108.
Valdmanis, R (Reuter, Ottawa Wed Oct 29, 2014 1:11pm EDT). Canada's plan to defang would-be jihadists at home. Retrieved from http://www.reuters.com/article/2014/10/29/us-canada-attacks-deradicalization-idUSKBN0II1WG20141029
Waugh, C., & Douglas, J. (Oct 21, 2014). CBC News. As it happened. Retrieved (2014-10-22) from http://www.cbc.ca/player/Radio/As+It+Happens/ID/2565724715/
Wicker, C. (2007). International lessons learned and recommendations for combating domestic Islamic terrorism. Carlisle, PA: U.S. Army War College, Carlisle Barracks.
Yaseen, E. (2007, September 28). Dawla dinia or islam dimokrati? [Religious country or Democratic Islam?]. Cairo, Egypt: Al-Ahram Newspaper.
Zena, A (June 21, 2002). جدل ساخن داخل أوساط الإسلاميين بعد مبادرة قادة «الجماعة» بتقديم اعتذار للشعب المصري. Hot debate inside Islamic communities after the initiative of the leaders of the group for apologizing to the Egyptians. El-Sharq El-Awsat News. Retrived (2015-01-10) from http://classic.aawsat.com/details.asp?section=4&article=109340&issueno=8606#.VK7bP405Ck

The
Mackenzie Institute
Security Matters.

MACKENZIEINSTITUTE.COM | OCTOBER 2015