CASE STUDY ANALYSIS:

ISLAMIC STATE (IS)-INSPIRED TERRORIST ATTACK IN OTTAWA, CANADA

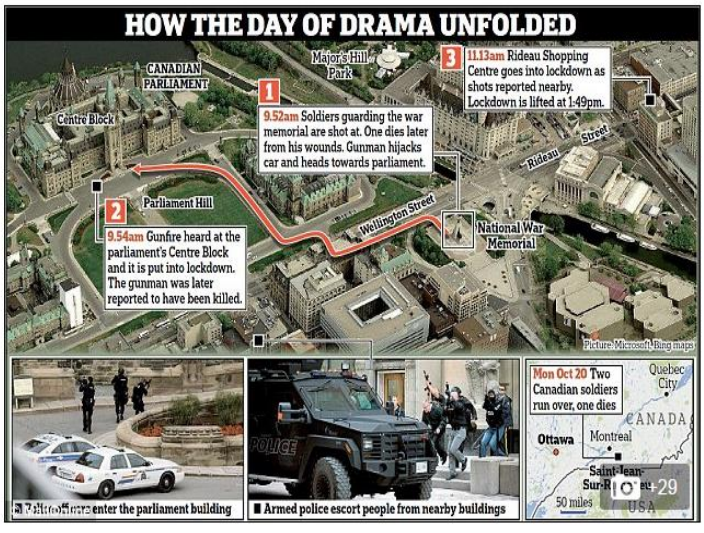
This report is based on information collected from open sources and the professional insight of ASERO's team of experts. This analysis focuses mainly on the anti-terrorism / protective security aspects of the event and less on the intelligence perspective.

DESCRIPTION OF EVENTS

On October 22, 2014, Canadian citizen Michael Zehaf-Bibeau (age 32) went on a shooting spree in Ottawa, Canada at the National War Memorial and the Parliament building. Cpl. Nathan Cirillo, a soldier at the war memorial was killed and two others wounded, one of which was identified as a security guard at Parliament's Centre Block. Zehaf-Bibeau was eventually shot and killed by Kevin Vickers, the sergeant-at-arms for the House of Commons, during a gunfight with police and guards. After arriving in Ottawa, where he stayed in a local shelter, Zehaf-Bibeau purchased a rifle and a vehicle in order to carry out the attack.

1st attack at the Centotaph National War Memorial

- Zehaf-Bibeau parked his car facing east on Wellington Street behind Cenotaph, walked about 100 meters before shooting Cpl. Nathan Cirillo in the back.
- The deployment of the soldier outside the war memorial is a ceremonial one and according to media reports the weapon that the soldier was carrying was not in fact loaded.
- It is unclear whether the security guards injured in the Cenotaph attack were there for protective duties or were there coincidentally.



2nd attack at the Parliament building

- Zehaf-Bibeau returned to his vehicle where he then made a U-turn on Wellington, parking the car at the vehicle entrance for members of parliament.
- He then ran past the bollards towards the East Block.
- Seizing a Minister's vehicle parked on the street, he proceeded to drive to the Center Block of Parliament Hill followed by three RCMP vehicles in pursuit. **This part of the**

attack lasted 1 minute and 23 seconds.

- Zehaf-Bibeau proceeded down the corridor where many senior politicians including the Prime Minister and members of Parliament were sitting in meeting rooms. According to reports, there are no access control measures in place for the rooms in this corridor.

THE ASSAILANT

Just prior to the attack, Zehaf-Bibeau prepared a video message where he spoke about his ideology and political motives. Local authorities have since declared Zehaf-Bibeau a homegrown radical terrorist, with no further elaboration on the matter.

Zehaf-Bibeau had applied for a passport in order to travel to Syria and travelled to Ottawa on October 2nd in an attempt to speed up the approval process. It was also stated that the shooter had a criminal record for mainly drug- and violence-related offences.

THE ENVIRONMENT

Western intelligence services have been warning for some time now about the developing threat from IS. These countries are faced with a major challenge of monitoring the large number of individuals affiliated with ISIS both at home and abroad. Authorities are being stretched in order to address the increasing numbers of radicalized individuals and determine means of tracking those fighters trained in Iraq and Syria seeking to return to their native countries to carry out an attack.

Canada, like other western countries, continues to combat new terror plots developing within its borders. In 2013, authorities thwarted two terror-related attacks: (1) a bomb plot in April to derail a VIA Rail Canada train and (2) a plot in July to carry out an attack against the Victoria British Columbia legislature building.

Then, just **two days** prior to the attack in Ottawa, the threat level was raised from low to medium after 25-year-old Martin Couture-Rouleau rammed a vehicle into two soldiers in Quebec, killing one and injuring a second.

In addition, a leaked FBI-DHS intelligence bulletin, "Islamic State of Iraq and the Levant and Its Supporters Encouraging Attacks against Law Enforcement and Government Personnel," dated October 11, 2014, warned of the homegrown threat from ISIS. Although the document made

note of the fact that the FBI is currently unaware of any specific immediate threats, it does address ISIS statements calling for attacks on U.S. military personnel, law enforcement (in general), FBI personnel, government officials, and media figures.

The bulletin cited what is believed to be the first public calls to violence against countries considering military action in Iraq, including a recent post from chief Islamic State spokesman Muhammad al-Adnani for 'lone wolf' attacks in the West, a post in September calling for an "'open source jihad' by lone wolf terrorists targeting 'military, law enforcement, FBI personnel, government officials, and media figures'" (*InfoWars Online,* "FBI and DHS Issue Bulletin Warning of IS Attacks on Police in the U.S."). The bulletin further mentioned foiled plots in Britain, an attack in Australia, and a second foiled plot to carry out public beheadings in Sydney.

The organization's "social media strategy" is discussed in the bulletin as well, warning authorities that ISIS has pledged to continue to use Twitter as a means of spreading its message. ISIS's use of social media is meant to demonstrate the extent of the group's a global reach.

INSIGHTS AND LESSONS LEARNED

General

- The position of Sergeant-at-Arms is usually both the head of the Parliament's security Unit and also a ceremonial position. It is not considered an operational position. It is to be expected that a deployed protection officer with defined operational duties would be the first to respond to an active shooter incident.
- Public calls made by ISIS through social media to attack law enforcement/military personnel may continue to motivate terrorists to carry out similar attacks.
- Armed assaults/active shooter scenarios are a significant threat and all sensitive installations must be considered potential targets for this kind of attack.
- Security decision makers and field commanders cannot rely solely on intelligence and must therefore work under the assumption that a terror attack will occur without warning.
- Time and time again, social media proves to be a channel that the adversary will utilize to incite, recruit, train, and organize terror attacks.
- The outer security ring is a vital component of any security deployment, as it enables detection at a distance from the protected entity. It can be the main measure in preventing a terror attack of this nature.

- From an observation of the CCTV video footage of the assailant's arrival and entry into the Parliament building, it would appear that there was a lack of visible security guards on the outer perimeter (outside the gate). The absence of any visible security portrays a lack of visible deterrence and is thus a vulnerability which may attract an adversary.

- Armed assaults by terrorists were a common modus operandi in the 70s and 80s. For a period of time afterwards, the use of IED and VBIED became a more common method of attack. However, in the last few years, we have seen a rise in the number of armed assaults around the globe, including Mumbai (2008), Norway (2011), Nairobi (2013), and Brussels (2014).

Parliament Security

- The overall responsibility for the security of the Parliament is divided among several agencies: the Ottawa Police have responsibility for areas outside of the Parliament precinct, the RCPM has responsibility for the Parliament grounds and building, the RCPM Prime Minister Protection Detail (PMPD), as well as the Senate and Home of Commons with their own respective security forces, the military, and Ontario provincial police. At the time of the incident, the Quebec provincial police were also involved due to their jurisdictional control over the bridges and checked vehicles.

- There are no physical security barriers (i.e., mantraps, CAD swiping, or other barriers) at the entrance of the Parliament via Centre Block.

- Access control procedures for members of Parliament was limited; MPs are only required to show their ID badge to an unarmed guard at the gate (***Note*** – plain clothed RCMP officers are present at this entrance area as well). This can be compared to measures taken at the public entrance where visitors are required to pass through a metal detector and have their personal effects checked.

- Anti-Terrorism Domain: It is clear that if a terror attack is not challenged and defeated or at least mitigated at the start of the incident (within seconds) the situation is likely to deteriorate rapidly with severe consequences (i.e., hostage situations or mass killing sprees).

- It is often the case with large protective entities, many agencies are involved in ensuring the overall protection of the facility. A situation of multiple security agencies with divisions of responsibility can cause confusion, overlapping in responsibilities, and a lack of a central command.

RECOMMENDATIONS

- Armed assaults will continue to be a viable threat and need to be addressed by both government security agencies and private sector security alike.

- At times of elevated threat, national monuments should be considered potential targets and be adequately protected.

- There is always a danger of the copycat phenomenon whereby previous modus operandi will be emulated in the future. We saw in the case of Martin Couture-Rouleau and the 2013 machete attack in London, the attackers chose to use a vehicle to ram into military personnel. We recommend that authorities be especially vigilant in the days and weeks following a terror attack; tactics previously witnessed may be copied.

- All sensitive facilities and potentially attractive targets should carry out a Threat, Risk and Vulnerability Assessment (TVRA) which should form the foundation of the facilities' security plan.

- The security plan should determine the level of protection for a facility and what security measures and actions need to be taken both during routine operations and in times of emergencies. The plan should encompass all relevant and defined threats.

- Emergency plans for high risk installations should include measures for evacuations relating to both hostage taking and armed assault scenarios. They will also need to determine when "shelter-in-place/taking cover" takes priority over evacuation and how this is communicated. The security plan should include a methodology for post attack sweeping of the facility to ensure there are no further threats present.

- The security command and control room should be designed to be able to collect the situational picture and act as an immediate support tool for the field commanders during an emergency situation.

- It is critical that the different agencies required to respond to the attack be able to communicate with each other. This may be achieved by allowing the command center the ability to override/break into existing frequencies in order to inform forces of the event as it unfolds and have the relevant factors move over to the designated emergency channel.

- At facilities that have multiple agencies involved in their protection, there should be one regulatory body that determines the level of protection and ensures, through a quality assurance program, that the level is being maintained.

- It is recommended that protected facilities should have an overall security manager who will have initial command of an emergency situation until it is handed over to a more senior officer arriving on scene.
- Active shooter policies should focus firstly on prevention and detection and then on immediate and effective response based on in-house capabilities. Active shooter plans and policies need to be practiced, through drills and table top exercises (TTXs) on a regular basis by all agencies including the Prime Minister's personal detail.
- In the vast majority of cases, terror attacks begin from outside the facility and therefore it is recommended that security on the outer rings should be both visible to increase the deterrence factor and be equipped with behavior detection tools.
- All threats should be addressed by more than one security ring. If one security ring fails, there is an additional layer in place to prevent a breach. For example, an entry point should have both a protection officer and physical barriers.
- Social media monitoring tools should be used to track the activities of suspected individuals and the potential threats they pose.