The Use of Open Source Information & Planning Terrorism Scenarios

Victor Tise
Scientific Research Corporation (SRC)
(719) 554-1999
vtise@scires.com

This paper will detail the fact that there is an inordinate amount of open source information available via the internet that facilitates writing terrorism scenarios for academic and exercise purposes. The same open source material can easily be used by enemy terrorists to plan and execute actual terrorist operations against targets in Canada and the United States (CANUS).

In 2003, I served as a member of the CANUS Bi-National Planning Group (BPG). The BPG was created by the authority of a Diplomatic Note signed by Foreign Affairs Canada and the United States Department of State in December 2002 via the *Enhanced Military Cooperation Agreement.* The Agreement directed the BPG to enhance bi-national military planning, surveillance, and support to civil authorities. While a member of the BPG, I wrote ten viable terrorist scenarios using open source information off of the internet, as follows:

1. Container ship detonates nuclear devices at major ports.
2. Biological/chemical attacks from offshore trawlers.
3. Terrorism on U.S. and Canadian bridges, locks and tunnels.
4. Power grids and pipelines blown-up on CANUS border.
5. Terrorists explode a dirty bomb in Windsor/Detroit.
6. Direct attacks on U.S. Congress and Canadian Parliament.
7. Homeless in multiple cities infected with smallpox.
8. Major earthquake on U.S. / Canadian West Coast.
9. Terrorism in Puget Sound
10. Terrorism During the 2010 Winter Olympics

The BPG used the first eight scenarios for the primary purpose of conducting deliberate and adaptive planning by preparing bi-national contingency plans for joint and combined defense and security of North America. Additionally, the scenarios were used for bi-national civil support planning to respond to threats, attacks, and other major emergencies in Canada or the U.S. Existing CANUS plans had not kept pace with changes in the dynamic threat environment since 9/11. The threat-based adaptive planning resulted in joint and combined plans that could be executed in real time. To facilitate threat-based planning, the eight scenarios were developed to assess national defense plans and the potential of a combined response with a continental focus on defense and security.

The last two scenarios – Terrorism in Puget Sound and Terrorism During the 2010 Winter Olympics – were developed and used to facilitate strategic level discussions during table-top exercises at the two Permanent Joint Boards on Defense (PJBD). The PJBD is the senior-level bi-national organization at the political-diplomatic level. Its critical function is to ensure coordination and synchronization among CANUS instruments of national power. The PJBD forum provides the opportunity for senior CANUS decision makers to discuss bi-national defense and security issues in a timely manner, make key recommendations, and report directly to the Prime Minister of Canada and the President of the United States regarding defense and security matters.

In early 2003, when I first began conducting research of open source information, terrorism scenarios were found in a limited variety of websites. The best material was found on university websites, think-tank websites, and activist-type websites. The following are two examples of scenarios I adapted from

ideas I found on the internet and rewrote to best serve the threat-based adaptive planning process for NORAD and USNORTHCOM.

The first scenario was found on a university website. In this scenario the author wrote of three container ships loaded with nuclear weapons that anchored in the proximity of New York City, NY, another by the Port of Long Beach, and the third in Seattle, WA. In this scenario the ships were equipped with clocks that received signals from the National Institute of Standards and Technology, in Boulder, CO, so their timing could be precisely synchronized. Each ship was programmed so that at a coordinated time, the last known position was checked by a GPS and recorded on a computer. A subsequent check was made to see if the ship had been moved within a prescribed period of time. Once devices confirmed that the ships were at the correct locations, the nuclear devices armed themselves and later simultaneously detonated. I found the scenario to be very plausible from a technical perspective; however, the port locations did not serve the planning purposes of the BPG very well. So, I changed the scenario and portrayed ships as being anchored in Vancouver, BC, Seattle, WA, and San Francisco, CA, giving the scenario the bi-national setting required for BPG planning.

The second scenario involved infecting homeless people in New York City with small pox. This scenario took place in the coldest winter months where coats, blankets, and sleeping bags contaminated with the small pox virus were handed out to the homeless individuals. This particular author had a very plausible approach and had thought the scenario through quite well. His main position was that the homeless, infected with small pox, would not seek medical attention as quickly as the general population, thus allowing the virus to incubate for a longer period of time. Once the homeless people started to seek medical attention, their level of contagion would have increased by a huge factor. Subsequently, New York City would end up with countless people infected with small pox and would have to initiate a large-scale quarantine. Again, this scenario as it was written did not serve the interest of the BPG very well. So I simply changed the location from just New York City and included multi-cities – Boston, Montreal, and Ottawa – giving the scenario the bi-national nature it required.

There were instances where I came up with my own ideas for terrorist attacks and researched open source material to further develop my ideas. Additionally, I searched the internet to locate targeting type of data for these terrorist scenarios. For instance, I thought about planning to attack the power grid and gas pipeline interconnects between CANUS. By simply searching for Canadian and U.S. gas pipeline interconnects utilizing the Google search-engine, I was able to find websites that provided me with detailed maps of natural gas pipelines that began in the Northwest Territory, crossed various points along the CANUS border, and terminated at various points in the U.S. When I further refined my search of those areas, I was able to access maps that depicted gas pipelines crossing the international border and found them to have highly vulnerable, completely unprotected interconnects. Attacking some of these interconnects would have been easy to accomplish.

I did a similar search of Canadian and U.S. power grid interconnects and found websites with similar maps showing the complete North American power grid and unprotected power grid interconnects. I was able to acquire an open source overhead photo of a power grid interconnect in the Niagara area. Using the combination of the overhead photo and Mapquest, I was able to plan routes to get to the site, conduct the hit, and expeditiously escape. When asked how I would have attacked this particular target, I briefed that I would have used some kind of ordinary vehicle to drive a sapper to the targeted location, who could have thrown the appropriate number of satchel charges with time delayed fuses over the chain-link fence surrounding the interconnect and simply driven off.

These websites did not just provide the maps and location of these interconnects; they detailed capacity of natural gas and electricity passing through the various pipelines and power grid. Information contained in these websites practically handed potential terrorists targetable data.

When one does similar Google searches today, four years later, a plethora of websites related to terrorism scenarios can be found. Of course in the four years that have passed, much more experience and knowledge of terrorist practices have been gained and made more accessible. Today more

information is readily available to either legitimate planners or terrorists wanting to conduct planning via open source information.

I purposely did not list any of the previous websites I used to develop any scenarios, except for Mapquest. However, I feel it would be of interest to point out three types of websites that make it too easy for terrorists to plan attacks:

- Google Earth - http://earth.google.com/
- Global Guerrillas - http://globalguerrillas.typepad.com/
- Global Security - http://www.globalsecurity.org/

Google Earth will provide free overhead photography of any location on the globe. Much of this photography is of such resolution that it allows for more than adequate development of target packages for terrorist attacks. Global Guerrillas is a website that also serves as a blog. People interested in terrorism can actually post ideas for terrorism on this website and then get other people to discuss these ideas and expand upon them. The website will link internet surfers to countless other websites that will even detail how to construct various rudimentary, but effective, weapons. The Global Security website will let anyone in the world access information about military bases around the world. One can get detailed dimensions of airfields, what types of aircraft can be found at the airfields, and quality photos to go along with all of this information. The website does not leave out Army and Naval installations and can provide excellent order of battle information of units assigned, their missions, weapons, and equipment available to the units. As for the Naval installations one can find out information about the ships assigned to the bases and vital information about the ships and crews. Quality photos are available as well.

The main objective of this paper was to sensitize readers as to how easy the internet allows for planning terrorism scenarios via open source information. During my time on the BPG, ten scenarios I developed allowed for real-world threat-based adaptive planning. CANUS strategic level planning was conducted by using these scenarios in table-top exercises and NORAD and USNORTHCOM exercises. When I initially briefed the first eight scenarios to senior members of the Royal Canadian Mounted Police, they requested that the scenarios be classified because of their plausibility. Additionally, I have used some of my scenarios in critical thought discussions with graduate students at various colleges and universities.

There is not much that can be done to stem the availability of the megabytes of information available to rogue and organized terrorists, military planners, academics, or would-be terrorists when we live in this free and open society. Some ingenuity and out-of-the-box thinking combined with the availability of comprehensive information and adequate computer and networking equipment will result in future terrorist operations being planned via the internet. Hopefully, homeland defense and security entities can stay a step or two ahead of the bad guys.

Victor Tise is a Program Manager for Scientific Research Corporation (SRC). He works on an Office of the Secretary of Defense Joint Test and Evaluation Program developing Tactics, Techniques and Procedures for the planning of Joint Air Defense Operations for the Homeland in support of the North American Aerospace Defense Command (NORAD) and U.S. Northern Command. He is a retired Army officer who spent 22 years of service as a Military Intelligence and Latin American Foreign Area Officer. Prior to working for SRC, he served as a Northrop Grumman Program Manager for the NORAD and U.S. Northern Command's Bi-National Planning Group. Vic is a 1977 graduate of the United States Military Academy at West Point, New York and has a Masters of Arts degree in Latin American Studies from the University of California, Los Angeles.