DC Sniper: Beltway Attacks

Table of Contents

DC Sniper: Beltway Attacks

DC Sniper:
Beltway Attacks

18

**018 So let's look at a real-world example. While not specifically cyber-related, it is a common case study for how to use a key assumptions check and where a key assumptions check could have helped.

For those of you who may not know, the Beltway Sniper attacks were a series of coordinated shootings that took place over three weeks in October of 2002 in the Maryland, Virginia, and Washington, D.C. area. Ten people were killed and three other victims were critically injured in several locations throughout the area alongside Interstate 95 in Virginia. As it was going on, police were working off of the following assumptions.

Key Assumptions Check: 2002 DC Sniper Case

Key Assumption	Assessment
The sniper is a male.	Highly likely (but not certain) given past precedent with serial killers. We are taking little risk by not looking for a female.
The sniper is acting alone.	Highly likely (but not certain) given past precedents.
The sniper is white.	Likely, but not as certain, given past precedents. We would be taking some risk if we rule out nonwhites as suspects.
The sniper has military training/experience.	Possible, but not sufficient reason to exclude from consideration potential suspects who have not had any military training.
The sniper is driving a white van.	Possible because you have a credible eyewitness account but worthy of continuing scrutiny given the number of white vans in the area (more than 70,000 registered in the Maryland suburbs of Metropolitan Washington, DC) and that different kinds of vehicles are being described.

https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/Tradecraft%20Primer-apr09.pdf

19

**019 So here's the list of key assumptions and the assessments that police were working off of. They were going off of these assumptions for three weeks while the D.C. area was in a complete state of fear. They also included in their assessments the likelihood of the key assumption.

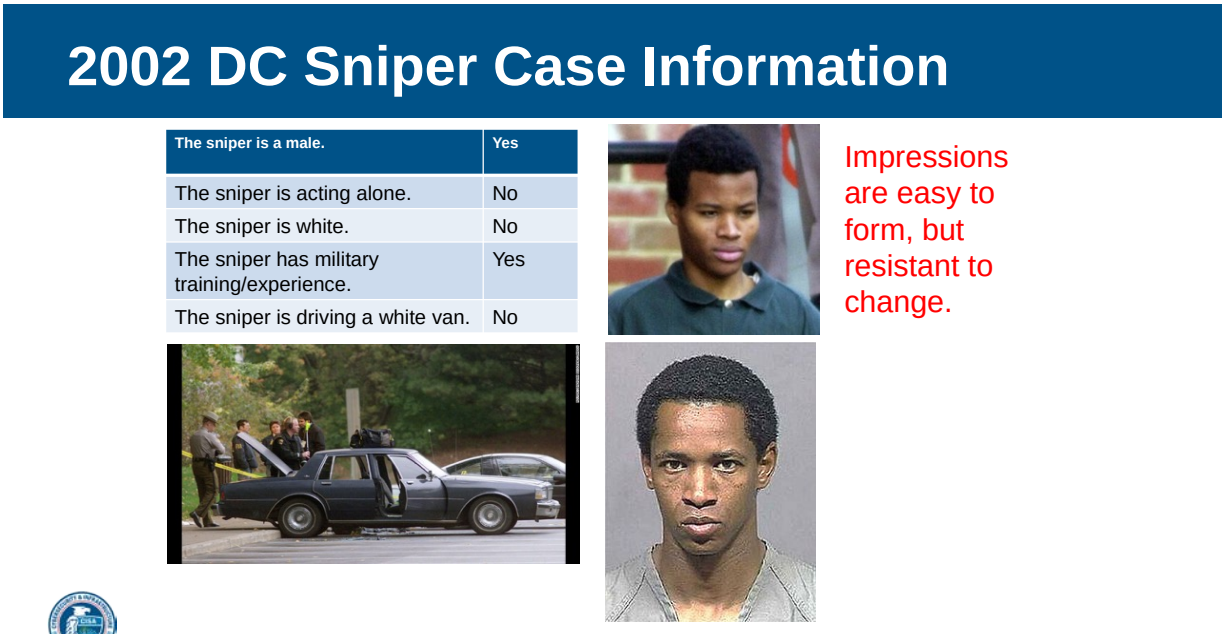
So, the sniper is a male: Highly likely but not certain given past precedents with serial killers. We are taking little risk by not looking for a female. The sniper is acting alone: Highly likely. The sniper is white: Likely but not certain given past precedents. We'd be taking some risk if we would rule out non-white as suspects. The sniper has military training experience, and the sniper is driving a white van, and that assessment was possible because you have

credible eye witness accounts, but worthy of continuing scrutiny.

So these were the assumptions that the police were going on, and I myself remember at the time for about three to four weeks a ton of white vans were being pulled over almost daily by police and traffic was out of control in the entire Washington, D.C. metro area, and there was a lot of fear and anxiety about going outside.

They did not, however-- the police-- do a key assumptions check. If they did, however, at the time, they could have found out new additional information.

2002 DC Sniper Case Information



**020 One could argue that a key assumptions check could have allowed law enforcement to examine

each assumption and avoid prematurely narrowing down the potential pool of aspects to a group that did not include the actual perpetrator. They could have avoided jumping to conclusions that the sniper was white, had military training, and was driving a white van. That did not hold up under closer scrutiny. They could have asked themselves or done a key assumptions check, "How much confidence do you have that your assumption is correct, and what circumstances might undermine the assumption? Why must this be true?" Could the assumptions have been true earlier but no longer true in the past, and what were they willing to accept as new information that was coming in? Could they have been more receptive to new leads and citizen tips such as eye witness reports that the sniper fled the scene in a specific Chevy model of a blue car? More seriously consider evidence that subsequently became later available which contradicted even key assumptions that the sniper was acting alone. If officials had stated explicitly that they were assuming the sniper was acting alone, they might have been more sensitive to new information that contradicted all of those assumptions.

So that is an example of a key assumptions check that could have helped and possibly even saved lives.

Notices

This material is based upon work funded and supported by the Department of Homeland Security under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

DM20-0262