MODULE 6 - 2084

LECTURE 4 – VIOLENT CRIMES AND TERRORISM

THE ME-KNIFE-DEAD BODY THINGIE – ANY HELP?

OK, so now we're **gonna** do the same thing for **MURDER** crimes that we just did for the **LAMB/BLVA** crimes. This can get a bit tedious in just audio, if you haven't noticed, so I might just try to speed things up a little. I'm gonna use a couple of scenarios we talked about earlier – the **me-knife-**dead body thingie, and the Boston Marathon bomber case.

The first scenario, as you may recall, was the **me-knife-dead body thingie**, which was me spontaneously killing somebody with a knife. Yes, most of you would recall that. You, CURIOUS TRAVELER, stumbled upon this scene, saw me with the knife and as I ran away, and you reported what you saw to the police. So this is a reported Visible crime with a clear victim and a human witness who may have missed some of the ACTION phase, but who observed the ESCAPE phase. The police response in the FUGITIVE phase would be similar to the store burglary just discussed. The future technology that would allow the police to see and smell what happened (cameras and mechanical sniffer), and to track me down and tell if I'm lying (nanobots, face-reader), would be a **BIG help to SOLVE the CRIME in the FUGITIVE phase,** no doubt about it.

But the **alternate** scenario to the **me-knife-**dead body thingie was that you did not arrive at the crime scene, that I just walked away, and that body snatchers or something made the body disappear. So the only evidence of the crime was the cheap knife that I stupidly left at the scene. So the police never knew of the crime. But say somebody eventually reports the person I killed as missing. Or, if that person had nanobots, maybe our future technology would just routinely scan **nanobot data bases** to identify people's current whereabouts and past locations. And maybe the technology could be programmed so that if a person's nanobots didn't move from a certain location after a specified period of time, then it would self-alert the authorities to do a follow-up check or something. And then maybe a trace of those locations would bring the police to the remains of the body, or the location of that damned cheap knife of mine. And maybe traces of my **body odor** would still be detectable and identifiable on the body remains, or on my knife. Maybe by then we'd even have national data bases of body odors, kind of like AFIS for fingerprints, and CODIS for DNA. And even by chance there may be a camera video placing me at or in the vicinity of the crime scene, or at least not placing me anywhere else at the time of the murder. So I couldn't use camera video to substantiate my alibi.

Or maybe I was just identified the old-fashioned way, by my fingerprints on the knife. And maybe when a detective with Google face-reader eyeglasses interviews me, my micro-expressions might provide further corroborating evidence of my foul deed, and I crack under the weight of it all and confess and crumble into a miserable heap of agony and remorse. **It could happen**. But **lesser crimes** such as rape, robbery and assault are probably gonna **still need a person** to report them to the police, at least until 2084, don't you think?

Far-fetched? Man, I don't know. I can actually see stuff like this happening. **PREVENTing a spontaneous** crime like this may be beyond the scope of the technology we're talking about, and we'll explore more about **PREVENTing planned** serious crimes in a moment. But nanobot technology that can track people and alert the authorities when they don't move anymore. That seems like powerful but doable stuff. So for murders and the other FARM/MRRA crimes, I'd say that because criminals might know of the technology, it may **PREVENT crimes somewhat by deterrence.** So a **LITTLE** help in PREVENTION.

As for **DETECTING PLANS** to commit such crimes, it's probably similar to the property crimes. The technology can document the offender's whereabouts, but it needs triggers and alert mechanisms. For most crimes, especially spontaneous ones, it probably won't be able to alert authorities in time to stop the crime. But for some crimes it may, especially if there's tools or equipment involved, just like for burglaries. And as for **DETECTING ACTIONS,** the same issues seem to apply in general.

But this crime was **not detected** in the PLAN or ACTION phases. It was **DETECTed** in the **FUGITIVE** phase by the triggers of someone reporting the dead person missing, or by nanobot track/alert technology. Of course, there's always exceptions and stuff, but for the most part I'd say that for the **Murder crimes**, future technology may be:

1 - **a <u>LITTLE help in PREVENTING SOME crimes,</u>** due to its deterrence effect, but it can be a

2 – a <u>BIG help in DETECTing SOME crimes in the FUGITIVE</u> phase. These would be mostly murder crimes. No panacea, but some improvement over the current situation. However, again, it should definitely be

3 – **<u>a BIG help in SOLVING crimes in the FUGITIVE phase.</u>**

So, going way **out on a limb** again here, I might broaden the scope of all this and say that for **most Visible FARMLAMB/MRRABLVA** crimes, the effects of future technology may be similar:

1 – <u>a LITTLE help in PREVENTING crimes;</u>

2 - <u>SOME help in DETECTING some crimes in the PLAN, ACTION and FUGITIVE phases</u>; and

3 - <u>a BIG help in SOLVING crimes in the FUGITIVE phase</u>.

Qualifiers here would include spontaneous crimes, crimes involving lower-value or less sensitive property, and less serious violent crimes. Again, no panacea, but a definite improvement over the current situation, **eh?**

<u>THE BOSTON MARATHON BOMBERS SCENARIO – ANY HELP?</u>

Another scenario we talked about earlier concerned the **Boston Marathon bombing** and the Tsarnevs, a Muslim family that moved to the US from Chechnya, Russia, which is a well-known terrorist area. Just to catch you up on the details, one of the young men in the family named Tamerlan traveled back to Chechnya for a visit and returned to the US. The Russian authorities notified the US of the travel, and the FBI interviewed Tamerlan and several members of his family. Subsequently, Tamerlan and his younger brother Dzhokhar were reported to have exploded two bombs at the Boston Marathon in April 2013, killing three people and injuring over 250 others. Tamerlan was killed during the ensuing investigation, and Dzhokhar is currently in custody awaiting trial.

So here's a situation where the FBI was notified of the potential terrorist affiliation of the Tsarnev brothers, and it **took action to monitor their activities, but was not able to PREVENT or DETECT** their crime or their involvement. Instead they did the same old **traditional investigation process** response after the ACTION and ESCAPE phases of the crime and the brothers were in the **FUGITIVE** phase. Existing camera and face-recognition technology played a key role in identifying the brothers in the FUGITIVE phase, and good old-fashioned police tactics resulted in their neutralization. That's good, but what about the future? Can't we stop these guys before they kill people?

We talked about maybe the **FBI or the police** should have spied on them more, like Government Spies did in the past, or maybe the **Inform-and-Alert Bunny** should have alerted the local populace to be on the lookout for suspicious activities. But that didn't go over so well – all that CC vs. DP stuff kept getting in the way. And

in the Tsarnov case, **human sources** in the neighborhood were not forthcoming. And three people died and over 250 were injured.

But if **these guys had nanobots** in them, then various protocols could be developed whereby their travels could have been monitored and identified as high risk without even the Russians telling us about them. And once they were in the high risk category, in addition to monitoring all their travels, especially in the US, other technology such as cameras and mechanical sniffers could be used to get a better picture of what they were up to and whether they had contact with explosives. And of course, we still have the capability to monitor Internet activities, emails, cell phones, etc., although our surveillance of those activities apparently **missed the boat** in this case.

So the point is that nanobots, cameras, face-recognition software, and mechanical sniffers could have been **helpful in deterring, or PREVENTing** the Tsarnev brothers' terrorist activities. Of course, the Google face-reader eyeglasses could have been a big factor in **DETECTing** their activities, or maybe even their intentions, during the FBI interviews in the **PLAN** phase, and maybe even in alerting authorities regarding their activities leading up to the **ACTION** phase. But the key to all of this would have been the future tech that **identified** them initially and in more detail, and **tracked** them more closely as potential threats, and **alerted** authorities. In this case, face recognition tech at all country ports of entry, especially designated high-risk areas, could have automatically triggered a self-alert in lieu of the Russians, and may have even deterred the terrorists from traveling there in the first place.

So I'd say that in this example of a **Political crime**, future tech could **PREVENT some types of these crimes somewhat** just by making it harder to plan for them, and that it has a **significant potential to increase the ability to DETECT them in the PLAN and ACTION phases.** And of course, it should definitely be **a big help to SOLVE crime.** So for **Political terrorism** crime, we, or I, came up with general conclusions regarding the expected capabilities of future technology to CUIPDSC. In sum, they were:

1 - **SOME help in PREVENTING crime,**

2 - a BIG help in DETECTING some crimes in the PLAN and ACTION phases, and a

3 - a BIG help in SOLVING crime in the FUGITIVE phase.

So for at least terrorist activities, it looks like future tech will be of even greater help than for Visible crimes. And as we audaciously extrapolated our future tech findings for burglaries onto the whole range of **Visible** crimes, we now bravely and fearlessly do the same with terrorism and suggest that future tech should have similar impacts across **all four major crime categories** (that's Victimless, Occupational, Organizational, and Political). No? Well, prove me wrong. Come up with your own analysis.

SUMMARY

By now, you should be getting the idea here. We showed how the CONCEPTUAL FRAMEWORK and the crime continuum phases can be combined with our knowledge of crime to do the following:

1- **estimate spaces, times and sources of crime information** in each of the crime phases

2- examine the **goals, styles and focuses** of the various criminal investigation models used to obtain crime info in the different phases, to see their strengths and weaknesses

3- project how we, with **different detective models, and developments in forensics and technology,** may affect the process in the future.

We didn't go over all types of crime, or in very much detail, and we only ran through a few scenarios for demonstration purposes. But who knows what future technology may thrust upon us? I certainly never dreamt of an iPad or **Twitter or Facebook** until they happened, and I'm still struggling with the idea of such **falderal and gewgaws** trying to manage my personal affairs.

But now **you**, ACCOMPLISHED TRAVELER, have the power to use these criminal investigation **gewg--,** er, I mean tools, to examine other types of crime in all five major crime categories, and **you** can put in your own ideas about future technology, etc., and you **can** draw your own conclusions. And it's easy, right? It's KISS, right? Well, of course it is!

And if you disagree with me or any of this stuff in this course, I'd like to know what you have to say. Because, you just may be right. Of course, I doubt that, but stranger things have happened. Oh **darn**, that's just my detective modesty flaring up - again.

But one of the things that **motivates** me most in life is that I don't want to be wrong. I **don't want to be wrong.** Because that can be dangerous. I'm an investigator. I want to get to the truth, or as close to it as I can. And I want to **corroborate** what I know. And I want to do that **without favor or affection**.