
Asia-Pacific Homeland Security Summit 2008

Mr. Robert Eidson

Asia-Pacific Homeland Security Summit 2008 Fellow

UCLA Anderson School of Management

Mentor Dr. Starnes Walker

Director of Research, Science & Technology Directorate

U.S. Department of Homeland Security

A NEW FRAMEWORK FOR UNDERSTANDING OUR VULNERABILITIES

The maginot line and our neglected left flank

Robert Eidson, UCLA Anderson School of Management

In the first fellows meeting at the Asia-Pacific Homeland security Summit (ASHSS) Major General ANM Muniruzzaman (ret) aptly described the current status of our homeland security from a international Muslim perspective [60% of his staff are Islamic]. It is clear that the threat of cyber terrorism is omnipotent and we are woefully unprepared to respond to such an attack, much less counter this threat in any meaningful way. While ideology is what we must confront in the grand strategy, it is necessary to counter such imminent threats as cyber terrorism in a way that cripples the ideological tentacles of terrorism while securing our vulnerabilities. In this paper I propose an economist's framework of the capital and labor function of homeland security and terrorism. Using this framework, we see that our left flank is exposed and that there are still some opportunities remaining in which we could take the offensive in the cyber war on terrorism.

CAPITAL/LABOR FUNCTION

Much like any other form of production, homeland security is a function of capital and labor.

Our level of homeland security increases as we increase the variables of capital and labor [observe diagram 1, and the subsequent change resulting in a higher production of homeland security in diagram 2). Science and technology advance the capital frontier, such that we achieve a higher production function. The terrorist attacks we have seen thus far occur when terrorists are able to reach a tangential point of the frontier of our homeland security (diagram 3). The terrorists have chosen techniques that are not overly technical or overly labor intensive. Almost anyone can learn to fly a plane into a building – landing is more challenging.

Asia-Pacific Homeland Security Summit 2008

In diagram 4, we can imagine a Maginot Line where America is safe from attacks. The line could hit a different tangential point, and have a different slope, but the line is negatively sloped. This is a general indication that with a certain amount of labor, we achieve homeland security, even if it involves a policeman every five feet in America. Or, conversely, with enough technology and very little labor, we can also achieve homeland security. Imagine cameras and RFID technology in every room, on every street corner, and all around every building. We would still need people to monitor the data, but you could have significantly less labor. At the extreme right end of the Maginot Line – between points A/B/C - we have the military (diagram 4). If the terrorists mounted a traditional, large scale assault on domestic soil, the military could counter the terrorists use of a labor intensive production function, lacking in capital intensive efficiency. At the far left end of the Maginot Line - between points A/C/D – we have the DHS, NSA, CIA, & FBI. These three letter organizations do a fine job and it is their domain to tackle the white collar crime, cyber threats, and other highly capital-intensive dangers. But as General ANM Muniruzzaman pointed out, our cyber vulnerabilities are more significant than the amount of safeguards we currently have in place. Nearly every IT service is virtual, as is most of our financial, government, military, and commerce. According to the General, it is surprising we have not seen an attack similar to the one in eastern Europe, where the nation's infrastructure ceased to function until the IT system was secure.

It is alarming that the production function of terrorists is shifting to the left. Notice that T'' is less steep at the tangent. This is indicative of increased marginal returns to scale – an economic phrase indicating “more bang for your buck.” This means that a terrorist can infringe upon our homeland security by increasing their technical skill level and using more capital intensive techniques. It would take marginally less additional input of capital to infringe upon our homeland security versus recruiting/training/executing additional suicide bombers. But, this is intuitive if we consider the following example.

- Terrorist A is has a PHD in Computer Science and Engineering. He can spend the rest of his life completing his mission by sitting behind a desk in an air conditioned

Asia-Pacific Homeland Security Summit 2008

room and writing codes or viruses that repeatedly cripple our nations cyber infrastructure.

- Terrorist B spends time in the economically depressed parts of the Muslim world. He is constantly fearful of foreign and/or domestic government agents killing or capturing him. It is his job to identify bodies to commit a perverted definition of holy jihad. Once identified, they have to be trained before they can execute their mission. The pipeline for a terrorist is not relatively short. The damage he can commit is limited by physics. How much bio/chem agents can he disburse? One can see that increasing returns to scale can be achieved by recruiting one PHD student versus numerous unskilled terrorists.

SOLUTION

What we are left with is an exposed left flank. Counter measures, at surface value, should include an offensive strategy. The terrorist propaganda websites are updated constantly. Real-time information and statistics about terrorist operations keep marginalized Muslims informed 24/7. Nations fighting against terrorism should engage in direct action to bring down such websites. Imagine recruiting talent in the hacker field to execute code/viruses to cripple their infrastructure. First, the terrorists would have to re-allocate resources from cyber warfare to defending their own infrastructure. This strategy is akin to the saying, "the best defense is a strong offense." At the least, we should harness these "freelance" hackers to identify vulnerabilities in our system. Patches and work-arounds could be designed in the short run. In the long run, we require better IT security on a massive scale.

MAGINOT LINE

The Maginot Line was a series of walls and defensive structures that the French built before the second World War to protect themselves from the Germans. It was an elaborate line drawn along the border and Generals assailed it as a modern marvel. In reality, the Germans rolled right through this line with little resistance. Every Americans' Maginot Line is their antivirus software. We have come to see this as a tax and we

Asia-Pacific Homeland Security Summit 2008

expect a certain level of protection. But, this is our personal computers. It is our infrastructure that is at risk.

What will it take to get Americans to face this risk? Unfortunately, it is the unthinkable. It is when our entire IT infrastructure is crippled and transactions simply cannot take place. How many days supply of cash do we carry? Imagine if every ATM in America was crippled for a month. That is why we refer to those in the three letter agencies as silent professionals. Their deeds go unheralded. But so does the grand strategy on ideology – where most experts agree victory lies. Most importantly, the opportunity to take the offensive is a window. Once an attack is launched on America, we will be on the defensive; the window for action grows shorter each day.





