SUSAN W. BRENNER

STARS 2015 PRESENTATION ABSTRACT

My presentation will cover many of the issues I recently spoke on at an Interdisciplinary Conference on Cybercrime, held at Michigan State University. Basically, I spoke, as I have at many other venues, on how and why the current systems we use to maintain order in the physical world, i.e., law enforcement and the military, are not and cannot be effective against threats delivered via cyberspace, as it currently exists and as it will evolve.

I explain that all societies must maintain internal order and, therefore, must deal with external threats, i.e., threats from “outsiders.” The outsiders to which I refer are members of the same species who are attempting to attack and conquer another society composed of the same species. This problem is constant across all species; even ants and barnacles have war. Humans, like other animals, address this threat by using a dedicated cadre of members of the tribe (“the military”) to repel attempted invasions and repel them by deterring such attempts.

I also explain that societies composed of intelligent entities, e.g., humans and wolves, also face an internal threat, which we refer to as “crime.” This threat arises in this context because intelligent entities can contumaciously decline to follow the rules that are intended to keep order in the society: the “civil rules” which we are socialized to obey. The civil rules deter us from committing crimes, first, because we have been taught to believe that abiding by civil rules is the “right” thing to do. The problem is that because humans, like members of certain other species, are intelligent and can elect to ignore the civil rules and prey on other members of that society. In the early 1800s, London, which was facing anarchy due to massive criminal activity, eventually developed the concept of “police,” who would patrol areas in an attempt to control crime and arrest people who committed crimes.

The real focus of my presentation is demonstrating how and why the systems outlined above do not work in the physical world. For one thing, criminal law is domestic, designed to keep order in a social grouping. Cyberspace allows people to commit crimes in other nation-states . . . and while a society has an incentive to discourage crime in its territory, it really has no reason to be concerned if its citizens commit crimes in other countries. So, Russia and China, to name two, have been attacking targets in the United States, and elsewhere, for over a decade.

The threat control systems we have in place – the military and law enforcement – simply cannot deal with those threats. Absent a disincentive to attack targets in, say, the United States, people in other countries will continue to do so. And the attacks transcend crime. Members of China’s military have been attacking U.S. companies for more than a decade. The companies have no recourse.

The situation has steadily degraded and will only get worse unless we develop new solutions for this twenty-first century threat environment.

I spoke on this on March 27 of this year at an interdisciplinary conference held at Michigan State University’ School of Criminology. The audience – computer scientists, business people and criminologists – were quite impressed.