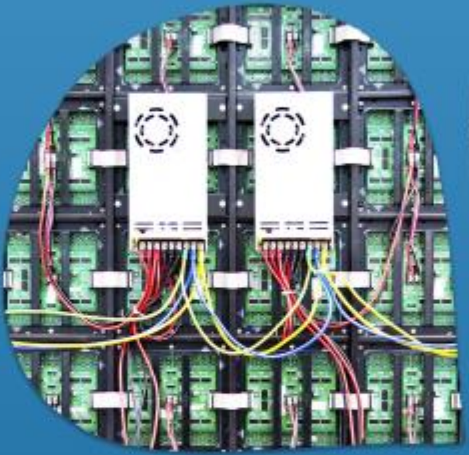

Grid Security:

Between Hype and Heads in the Sand

Brigham A. McCown
George Mason University
Schar School of Policy and Government
October 25, 2017

Introduction

Thank you Ambassador Kauzlarich for your very kind introduction. It is a pleasure to be here with you all on the campus of George Mason today.

In teeing up today’s conversation, I'll be relying upon some of my own experiences gained in the public and private sectors.

This is indeed a serious topic, and one which requires our attention. It also requires us to bridge the divide between those prognosticating doom and gloom, and others who prefer to bury their heads in the sand because the challenges we face are too daunting and complex to confront. These threats are magnified by the fact that they are directed at our transforming energy sector and other critical infrastructure across our economy.

Later this month I'm heading to Warsaw to join colleagues at the annual Warsaw Security Forum where we will discuss cyber threats of the most serious kind, exploring concepts of cyber security interwoven within asymmetric and hybrid warfare models.

Today’s panel discussions involved lots of issues, and we are becoming conscientiously aware just how much this topic permeates many industries.

The Grid

An article in Scientific American has called the electric grid the “largest interconnected machine” and that may well be the case. 7,000 plus power plants, over 55,000 substations, 160,000 miles of high voltage lines and millions of miles of lower voltage distribution lines makes our grid very complex indeed.

Yet stop to ponder for a moment just how connected our daily lives have become. And while the grid is massive so too are other forms of critical infrastructure: telecommunication networks, water and sewage facilities, liquid and natural gas pipelines, and the list goes on.

All of these facilities have faced physical vulnerabilities in the past, and yet today, it is fair to say, that we’re just beginning to understand the complexities of cyber security and the new pathways adversaries can use to gain access to critical infrastructure.

We have witnessed offensive application of such tools on the electric grid in Ukraine as well on nuclear facilities in Iran. In order to defend against hostile actions, I’d like to spend a bit of time talking about the past.

We are also being taught in business that relying upon past skills and outcomes are no longer predictive of future success. And while we may subscribe to that theory in general, the truth is that some things are more static in nature than perhaps we realize upon first glance.

> “ We’re just beginning to understand the complexities of cyber security and the new pathways adversaries can use to gain access to critical infrastructure.

The Shadow

The introduction from *The Shadow* radio program "Who knows what evil lurks in the hearts of men? The Shadow knows!" That line was spoken by actor Frank Readick, Jr. who held a glass of water next to his mouth for added echo effect. That famous line has earned a place in the American idiom. These words were accompanied by an ominous laugh and a musical theme.

My Dad used to listen to this very popular radio show, which debuted back in the late 1930s. It helped launch the career of a 22-year-old named Orson Welles who starred as Lamont Cranston, a "wealthy young man about town." And while Welles departed the show, the program did not leave the air until December 26, 1954.

Cloak and dagger

We have always been fascinated with cloak and dagger activities.

"Cloak and dagger" refers to situations involving intrigue, secrecy, espionage, or mystery.

These phrases referred to a genre of swashbuckler drama in which the main characters literally wore these items. In 1840, Henry Wadsworth Longfellow used the term and Charles Dickens subsequently used the phrase "cloak and dagger" in his work *Barnaby Rudge*.

The imagery of these two items became associated with the archetypal spy or assassin: the cloak, worn to hide one's identity or remain hidden from view, and the dagger, a concealable and silent weapon.

Initial concerns associated with cyber threats centered on “espionage” the practice of spying or using spies to obtain information about the plans and activities of a foreign government or a competing company: industrial espionage.

Prior to the 1990s government, state, and non-state actors relied primarily on other tradecraft for intelligence, surveillance, and reconnaissance. Organizations have an unquenchable thirst for information. Information and intellectual property theft are certainly not new.

The combination of espionage and its assorted use of human and machine have been around for centuries. In fact, it is hard to believe that only a few years ago the Internet did not exist. Yes, for those of you who are at college now, it must be unfathomable to imagine a world without the Internet.

While I did not, at least in my own eyes, graduate from university that long ago myself, I somehow managed to eke out a feeble existence. It’s a wonder I survived at all.

Cue the Internet

It is also hard to believe that until the 1990s our infrastructure and communications networks functioned in a world where the Internet as we know it was just beginning and was not for civilian use at all. It was a military tool.

I was recently reading “The Fundamentals of Counterterrorism Law” produced by the American Bar Association when I came across an interesting perspective. The authors pointed out that during the Vietnam War, a letter sent from nearly anywhere in the war zone could be received and responded to within 5 days, which was considered extraordinary! They went on to say that we would expect the end of the world if such a communication took so long today.

As the Internet took hold, it became a virtual highway for the free flow of information. The exchange of data has benefited us all; it has simply been revolutionary, enabling us to connect to each other. While connectivity is now seen as a concept as important as physical mobility, that very connectivity is agnostic in that it offers a potential pathway for good intentions as well as those seeking to harm us.

Hacking into computer systems is not new and I suppose we should not be so naïve not to think that with new technological opportunities come similar corresponding challenges.

The technological advances have been stunning, and have allowed us to see and do things that only a generation ago were unthinkable. And the pace of innovation is occurring more quickly than ever. The rapid advance of technology has effectively altered time.

No longer do we have the luxury of being able to see measures unfold. Perhaps this distortion of time has had the greatest effect in how we address cyber threats. While careful strategic planning is often needed to pull off the most complex attacks, responding in real time does not afford the same luxury.

> “The rapid advance of technology has effectively altered time.

The game is afoot.

Used often by Sherlock Holmes, this metaphor has extraordinary meaning for me.

Its origins however come from Shakespeare's King Henry IV, Part I. 'Before the game is afoot, thou still let'st slip.' The literal meaning of which is that the prey (“game”) is out of covert and running (“afoot”), and usually implying that it’s time you were up and after it.

The word "game" has two meanings. One is "quarry" or "spoils," and it would be the main meaning in Shakespeare’s and Holmes' words. However, the other meaning of "game" is, "a diversion, pastime, or amusement; or a form of mental or physical competitive play, governed by specific rules and testing the skill, endurance, or luck of the participants."

Cyber Security

If we ponder cyber security as the convergence of old style espionage with military tactics and a cat and mouse exchange imagined by Sherlock Holmes you begin to see the cyber domain as simply a new field of play concerning actors which have been moving in the shadows for centuries.

Albeit with some significant changes.

With technological advances come dependencies and vulnerabilities. We have all recently witnessed that disruption though recent meteorological events that have literally upended life for millions.

It is not therefore unexpected that cyber warfare and cyber terrorism threats are real. But just how real are they?

For the purpose of this discussion, I am laying aside those aspects of intelligence gathering and am really concentrating on the ability of an opponent to inflict harm to our critical infrastructure.

Whether regulating from a security, economic, or safety perspective, this complex situation can be broken down into an X and Y chart. Up the Y Axis we increase the probability of an attack, and the X Axis is expressed as an increasing level of impact or consequence.

When we look at cyber threats we have to break down the actors as well as their intentions.

Potential adversaries include State actors, Sub-State actors, and non-State actors. Some act with the intent to cause division and discord (recent elections). Others act to disrupt or to inflict harm and so when we discuss cyber security we should carefully consider both defensive and offensive capabilities.

Cyber Defenses

Layering defenses in depth are crucial to identifying and predicting threats before they emerge. That said, predicting and stopping the ability of an actor to attack infrastructure will become harder and harder. That’s not to say that hardening is not important, it is and defense in-depth is crucial to stopping or slowing down access. We have to take concrete physical and non-physical means to strengthen our defenses. To echo one panelist’s earlier comments, we must deter and know when someone is knocking on the door.

Realistically however, it is almost impossible to defensively prevent all attacks, thus we must rely on two additional means: resilience and deterrence.

Let me first talk a little about resilience. It's a pretty straightforward concept that refers to the ability of infrastructure to recover following a disruptive attack. Creating electric switches that power down to prevent transformer damage for example was recently on display in Florida where they worked very well. Yet despite some success, we remain behind the eight ball in implementing a bit of a belt and suspenders approach. I suspect we could spend an entire panel on this point alone.

Deterrence

Deterrence is also an easy concept to wrap one's hands around, yet in the context of the cyber world, it has proved elusive to implement.

When we were young we learned deterrence. If a child slapped or punched another, there was likely an equal or greater response. Thus being held accountable for an action deemed inappropriate served as a counterbalance to restrain others.

While the diplomats in the room refer to this concept as deterrence, at its core it's a counter threat, right? "If you do this to me, I'll do this to you."

Deterrence has, at least up until this point, worked in many areas. Yet deterrence only works when the response is credible. If a potential adversary does not believe that the response will be at least as damaging, and in many cases more damaging than the original attack, deterrence tends to fail.

So deterrence is about being able to clearly message boundaries and consequences. In our context, the U.S. must be able to clearly delineate what constitutes inappropriate behavior and embrace a wider range of retaliatory measures to deter attacks. Call it the doctrine of massive retaliation, or simply the Chicago way: the US cannot be afraid to respond in kind. That's not to say every response is the same, there is obviously some discretion; but the point is that the offensive response must make it clear to a belligerent that the cost was higher than any benefit.

Given that much of our own infrastructure is in private, versus public hands, this creates for some ambiguity as to what role the government should play. That ambiguity leads to certain dangerous misperceptions, both on the part of an adversary, and potentially on the part of government as well.

Further, offensive capabilities are developed in the dark, and are the sort of toolsets we are hesitant to discuss. Nonetheless, if an opponent does not see our offensive capabilities as credible, deterrence could lead to a serious miscalculation. Ambiguity in a national cyber security policy does not enhance credibility. Nor do responses which appear to only constitute a slight slap on the wrist in response to meddling.

Finally, it can be difficult to determine who is actually behind a cyberattack. A few countries have the ability to launch sophisticated attacks from outside their borders, using hosts in any other country, or countries of choice. Thus aside from stopping an attack, we must quickly identify the potential aggressor within a reasonable confidence factor.

Wrapping up

We must see the world as it is, not how we would like it to be. That said, it is time to strengthen infrastructure security; we cannot afford to delay. We must also articulate clearer lines of engagement and clearly bring private infrastructure, and I'd argue technology, under the government's protective umbrella. We must remove the zone of ambiguity so that it cannot be used as cover for future aggressive acts.

Finally we cannot shrink from fears of escalation as has occurred in the past and instead must embrace the use of well-reasoned retaliatory actions as an effective deterrent.