# Misztal: “There are neither incentives nor penalties for companies to adopt cyber security standards.”

Interviews

December 17, 2014



Like 2,299 people like this.

***JTW Interview with Blaise Misztal***

USAK Center for American Studies conducted an in-depth interview with Blaise Misztal, Foreign Policy Director of the Bipartisan Policy Center in Washington D.C., on the protection of critical infrastructure in terms of cyber security, and legislative and regulatory restrictions in cyberspace.

**Why is it important to protect critical infrastructure?**

We are living in a time when society and the individual are dependent on things that they might not actually see very often. For example, think about driving across a bridge. It looks like the road is just there, but there are steel bars or columns going into the river that are invisible to us, there is a whole support system that makes it possible for the bridge to perform its function… It’s the same with our society today. Behind the scenes at the supermarkets where we find food there are trucks that transport the food, electricity that keeps the food cold, and there are telecommunication systems for payment that read our credit cards. These payment systems send information to the bank, and then the banks confirm whether or not our credit cards have money on them or not. So even the most basic tasks of our daily lives are characterized by a high degree of complexity and interdependence. This is why critical infrastructure is important.

One of the issues that comes to the forefront when we think about cyber-attacks is that they can affect the entire critical infrastructure by only targeting an individual aspect thereof. Take the electrical grid for example, operators of electricity generation plants communicate the functioning of one plant to others, and in doing so they have computers hooked up to the network that tell them how much electricity is being producing in multiple locations. They can control the plants remotely. The systems are interconnected and the rise of the internet and cyberspace have allowed for this.
In other words, different networks are connected with each other: the electrical grid is actually connected to the telecommunication system, so if the phone lines fail you can no longer operate the grid because it requires this complex monitoring system. If the grid fails then the pumps that drive natural gas through pipelines to heat our homes will also fail. So it’s not just about the critical infrastructure, it’s about, “the infrastructure of infrastructure”. Failure in one aspect of the critical infrastructure can easily create a spillover effect.

Furthermore, there is the same interconnection between banking and the telecommunications and/or electrical grid. If either telecommunications or the electrical grid fail, we cannot access services offered by the banking sector. So all these networks are interconnected. The potential failure in one area of the critical infrastructure can easily affect the order of daily life, even if we are not talking about a kinetic event. It has been shown that it is possible for a cyber-attack to cause actual physical harm but, leaving that aside, the possibility of a failure in major services can have reverberatory effects. If electricity fails, generators in the US are required to have backup fuel that provides for 12 hours of electricity based on minimum standards. If there is no electricity for more than 12 hours, hospitals cease to function and people start dying. That’s why critical infrastructure is important to sustaining the fabric of modern life.

**What are the emerging cyber threats?**

We can think about trends both in terms of “what the threats are” and “what we are doing to address them”. I think even 4-5 years ago, people were talking about cyber terrorism, or a cyber 9/11; people kept thinking that there was going to be a big spectacular cyber-attack. However, I think people are realizing the issue that “the risks of such a big attack and the benefits to be gained from expending the resources to prevent that attack don’t match up”. People are realizing that massive attacks are not going to happen, yet what is happening right now can be seen as “intrusions”. Consequences are very pronounced, yet the line between intrusions and attacks is very fuzzy.

There is a big difference in the physical world between spying on someone and being able to kill or to launch a major military operation. But in cyberspace, once you are in the system, the difference between reading someone’s email and shutting down the entire system is minimal and can be considered as a matter of intention. What we have been seeing recently is the increasing sophistication of intrusions, the development of Advanced Persistent Threats employed through social engineering. Specifically tailored

attacks are one of the most interesting phenomena that we have seen in recent years and there has been a big question of how we are going to address them. I think there has been a big shift in thinking about cyber security, at least from the American perspective, namely, it has been realized that Advanced Persistent Threats are so specific and so targeted that you cannot build enough firewalls to keep them out. I think we have gone from the mentality that “we have to keep them out” to the realization that “we need to able to make faster mechanisms for finding penetrations, intrusions, intruders and being able to kick them out”. This has been the major shift in the mentality surrounding how we manage and mitigate risks relevant to cyber security.

**What are the problems generated by legislative and regulatory restrictions in cyberspace?**

There are three primary restrictions, namely, ambiguities, conflicts and gaps.

Ambiguities occur when the law is unclear. Many laws were written that we may think apply to cyberspace, even though they were written before the invention of the internet and related technologies. In the US, we have the Telecommunications Act of 1934, which regulates radio transmissions, giving the president and the government the authority to regulate them. Do radio transmissions constitute the internet? It doesn’t really seem like it. We have internet now. Does the President have an authority to regulate broadband internet? Because of the evolution of technology, there are now such ambiguities about how the law should be interpreted.

There is also ambiguity regarding what authorities are legally granted to the institutions. Particularly, the Department of Homeland Security (DHS) is the main government agency charged with protecting cyberspace, at least internally. The Department of Defense is dealing with the external dimension of cyberspace. The authority granted to the DHS is very ambiguous. For example, in the law we see statements such as “DHS is required… to provide cybersecurity”. What does “provide” mean? Does it mean you just make tools available so that people can decide for themselves whether to use them or not? Does it mean it can force people to use these tools? We don’t have a very good idea about how to look at laws that were written in such a broad way and are therefore subject to myriad interpretations. We don’t know what the terminologies that were used actually entail.

Secondly, there are conflicts. Many different agencies’ areas of responsibility seem to overlap. In the case of critical infrastructure, the Department of Homeland Security is the main government agency dealing with the protection of critical infrastructure. Yet there are other agencies that have expertise on the particular sectors of this infrastructure. For example, the Department of Energy deals with the electrical grids, and the Federal Communications Commission has much more expertise on communication networks than the Department of Homeland Security. There is also a Security Exchange Commission that deals with the banking system. So the question of “who exactly is responsible for what?” is plagued with overlapping jurisdictions and competition.

The third problem relates to gaps. While there are certain areas and issues of cyber security which are addressed by the law, others are not. This isn’t about ambiguity or overlaps, it’s just that we don’t have any legal framework with which to address the issue at hand. This can be understood in terms of authority. Who has the authority to mandate standards in cyber security? Here, authority could be granted to the actors active in certain parts of the critical infrastructure, in the case of electrical grids, for example, the federal government is responsible for setting reliability standards for bulk power systems that are generating power and transmitting massive amounts of megawatts from the generators. But then there are also the utilities that actually take that power, downgrade it for personal use and transmit it to your home. Here, electric power distribution is not regulated by the federal government. In this case we have a crucial part of the critical infrastructure that is not covered by law or regulations, even though it is just as important as the parts thereof that are actually legally addressed.

**What do you think about regulatory schemes and company liability when it comes to adopting cyber security standards?**

In the US we have the National Institute of Standards and Technology (NIST), which develops standards regarding all sort of technologies, from car safety to electrical transmission. However, it is not a regulatory body. It comes up with ideas that are non-mandatory and often don’t even offer incentives. It has recently issued a cyber-framework, developed together with industry representatives, and it is supposed to put forth the best practices on cyber security. It is just an idea or a suggestion, and therefore not legally enforced.

On the other hand, there are a number of bills before Congress that are basically trying to either grant incentives or issue penalties to companies based on their cyber security practices. Usually, the incentive path has been opted for, but the big issue is that many US companies seek liability protection. They are saying, “if we do what the government is asking us to do in terms of securing ourselves and sharing information with the government, then we are not going to be held liable, we can’t be found responsible and have to pay fines”. There are a number of bills offering just this being introduced in Congress. Ultimately, for any framework to be effective, it will have to “possess the force of law”, giving incentives or penalties for companies to adopt cyber security standards.

***By Oğuz Kaan Pehlivan***

