How Overclassification Undermines America's Cybersecurity

Harvey Rishikof

I would say this overclassification issue in cyberspace, or the classification in general, is an issue we have been fighting concerning the number of attacks and the sharing of information between the public sector and the private sector. We have clearly not resolved the issue of the public private sharing of information in the context of the cyberthreats. I would say that when I was on the government side in counterintelligence there were certain types of information we had that I think the private sector would have liked to have had but we had a number of restrictions either with legal frameworks involving violations of antitrust or a decision on the government side for sources and methods. We did not want to give up the information because of the fear of burning the asset. And we did not have a systematic, I would say, policy approach for how we racked and stacked the assets and which assets might have been worth us sharing the information so that it would have improved the ecosystem of the cyber world.

We have a similar problem with the issue of how we dealt with the concept of zero days. Those are, as you know, flaws in a code that have never been seen but that are discovered by individuals reviewing the code which allows us access to exploit those zero day codes in order to make a penetration or to cause a cyber effect. The attack on the nuclear facility in Iran as an open source proposition had at least three zero days that were involved in that operation that were exploited [by] whoever was the aggressor to get into that facility. So that issue of what is the appropriate balance of sharing information on the government side when it has these types of zero days and what it should be doing to improve the ecosystem, again, has not produced a consistent and structural policy.

We recently had a moment in which the intelligence community came forward with a fix for a Microsoft problem. The decision was made that the problem was so structural in the Microsoft app, the platform, that it should be made public in order for it to be fixed. On the other side, when I wear my private sector hat, there is a deep resistance in major corporations and companies to be able to come clean with attacks that have taken place on their networks and their willingness to share with the government for fear of either being prosecuted because it would demonstrate that they had been negligent or potentially grossly negligent in some aspect of their network maintenance. There is fear that if they share the information that information will be shared with the inappropriate regulatory group and that regulatory group would then penalize them for their inaction on the network. So that level of the need of transparency in the public private world, in the sharing of information given our vulnerabilities in cyber, is something that literally I've been working on or involved with, it's embarrassing to say, for almost over 25 years, 25 or 30 years. And it's a very similar conversation that happens all the time; and we in a report that I was involved with at MITRE called "Deliver Uncompromise," we recommended that there be an entity created, probably under the counter-intelligence directorate that's under Bill Evanina. They should be able to have jurisdiction that would include both the intelligence community, the Department of Defense, DOJ, the FBI and also the DHS. All of the authorities under one hat so that they could gather the information and keep it classified where it had to be

but also they'd be able to pass the information back through to the companies when it was appropriate. We have not solved that riddle.

Now going forward, there are some people on the call, trying to get that piece of legislation and that put in the bills for either the NDAA or else with the IC Authorization Act in order for the U.S. to create this entity. It's similar to the entity that we created for the National Counterterrorism Center (NCTC). The NCTC has had some degree of success in sharing information and gathering information. And I think we clearly need something in the cyber arena that is similar.

Alex has just pointed out I was referring to the National Counterintelligence and Security Center. The NCSC is where we thought it should be housed. We got a little bit forward in the last IC and NDA but not all the way there. But this is a huge problem that I think requires some legislative response in order for us to be able to grant immunity to certain companies so that they can feel comfortable sharing that information. We need to "illuminate the supply chain" in order to move forward to be more securing of the post 9/11 world where our adversaries are using asymmetric cyber vulnerabilities.