

TRANSCRIPT PODCAST INTERVIEW JOHN W. BIRD - U.S. MISSION TO THE EU – 11 JUNE 2015

Hello my name is Wally Bird, I am the Department of Homeland Security Attaché to the USEU Mission. I also have responsibilities at the U.S. Mission to NATO. One of my roles here is to coordinate the cyber working group among the three Missions: USEU, USNATO and our Mission to Belgium.

So the biggest challenges are large-scale infractions, hacking into our systems, theft of information and the destruction or the enabling the destruction of critical infrastructure systems. The United States and the European Union work together at very different levels. The highest level is the Cyber Dialogue which is a dialogue between our governments all the way down to the US and EU CERTs which are Cyber Emergency Response Teams that actually share information in real time and have a working knowledge of each other as professionals so those are the spans of the different levels that we work together.

I don't think it is any easier for the United States or the European Union to deal with cyber threats. I do think we have different approaches. We are at different stages in our process of our overall government development of these. The United States of course has a sort of easier process in the sense that we have a federal system that we have had for many many years and through that federal system we can administer certain rules, executive orders in a manner that is more developing right now in the European Union.

The threats that we all face are international in level and they challenge us in very different ways based on the gaps that we have in our law enforcement systems and our sharing of information, those are the major differences. Once we start sharing information and having a common approach I think that you will probably find that we have more of a partnership in dealing with cybercrime and cybersecurity.

The main threats are coming from our own inability to develop working systems, starting with the fact that it is very hard to hire people who have expertise so just having adequate personal who are trained in this area is a big challenge, a big weakness. The second is to eliminate divisions or competition among the federal government agencies or governments to provide services. And the third is to make sure that we have a common ground for the way that we all as nations and industry apply our solutions.

Financial services are certainly vulnerable just as critical infrastructure is, just as the average user of cyber systems is vulnerable. And there are individuals who operate from all over the world, you can have a server in any country that you want to have it so it is really a borderless crime. Whether or not we have identified more intrusions from certain physical locations, the answer is yes but I would prefer to just look at it as a case by case basis and not overshadow a discussion of solutions by implicating any one country.

The U.S. and the EU need to focus their attention on developing approaches to cybersecurity that allow them to share information effectively, that allow them to support the industry innovation and

commercial progress so that there aren't two different sets of rules for different players. The U.S. and the EU are making progress, we are working together to look at the different ways that we can share information, different ways that we can create structures. There are some fundamental differences in the way we look at these and it is important to talk to the industry also about how those will affect commerce but also the development of new technologies.