INTERNET SECURITY ALLIANCE

www.isalliance.org

Larry Clinton Comments – Munich Cyber Security Council – Thursday, February 14, 2019

- The theme of this session is: do we need a paradigm change in cyber security? My answer is unequivocally, yes. Perhaps the only issues virtually every speaker at this conference will agree on are that our cyber security problem is getting much worse and what we have been doing is not making nearly enough of a mark so that we can see when we will turn the corner.

- The old adage is that if you want to get out of a hole, the first thing to do is stop digging.

- We have already heard about the creation of technology replete with technical vulnerabilities. Not only do I agree with my colleagues about that, but I will go even further – the entire system is vulnerable. The Internet was BUILT VULNERABLE.

- Where I differ from my colleagues is that I think the dominant narrative, which focuses on vulnerability, culpability and penalty is misplaced and actually counterproductive because it leads us to ask the wrong questions and when you ask the wrong questions you get the wrong answers.

- One reason I like speaking to EU audiences is because they are often classically trained. With that in mind we ought to listen to the wisdom of Marcus Aurelius who advised to ask of each thing: what is its essence?

- So, we should ask: are technical vulnerabilities the essence of our cybersecurity problem? The answer is NO – they are incidental.

- Technology is just HOW cyber-attacks occur. To truly combat this problem, we must also focus on WHY the attacks occur.

- Allow me to make an American illustration. The signature security event of this century for America are the 9/11 attacks. Was the World Trade Center taken down because it was standing out in the middle of Manhattan all vulnerable? No, it was attacked because Al Qaeda was motivated to attack it. Put another way, Al Qaeda was incentivized to attack the WTC because they saw the profit in doing so – political profit in this case but profit, nonetheless. We couldn't secure the WTC by eliminating its vulnerabilities by putting anti-aircraft guns on its roof or building a perimeter around it. We needed to get at the cause of the attack not just the methods.

- This is similar to cyber security. The essence of the cyber security issue is not that the technology is faulty, it’s that the technology is under attack – that is a very different sort of problem that requires very different public policy answers.

- Consider the cyber security economic incentive structure we currently have. On the one hand cyber-attacks are cheap and easy to acquire and implement, they are low cost and very highly profitable – hundreds of billions of Euros a year. The business plan is very attractive. On the defense side we are protecting an inherently vulnerable system, the attackers almost always have first mover advantage, it's hard to show ROI to things you prevent from happening and we get very little help from law enforcement.

- To address this 21stcentury problem we need to develop far broader 21st century solutions that embrace technology and public policy and economics in equivalent measures -- that is a new paradigm.

- At ISA we have proposed the need for a Cyber Security Social contract. Just as in the 19th century when Hagel, Locke and Rousseau redefined the relationships between the state and the private citizen, now in the 21st century we need a new Social Contract that redefines the relationship between the state and the private sector.

- The traditional parental, punitive, regulatory model of the 20th century does not fit the digital age. Technology changes too quickly, the attack methods change too quickly, the world digital economy out spans traditional regulatory structures.

- The narrative that this model generates focuses on industry as too profit motivated, uncaring and selfish on the cyber security issue and hence must be managed by government,

- To be clear, are there industry players who don't care enough, don't invest enough in cyber security – sure but that is not the essence of the problem. And while we are on the subject, most consumers frankly also don't care enough and don't invest enough of their time and money to protect themselves and if we are being totally candid most governments – frankly I don't think ANY government – and I work colligatively with governments all over the world – and there are none who, from my perspective invest enough energy or money to address this problem – not even close. Just to take a U.S. Example everyone knows the U.S. Is losing hundreds of billions of dollars to cyber-attacks. The DHS budget to protect private critical infrastructure is about 1 billion.

- Not only don't we pay enough attention to the cyber issue and invest enough I cyber security, but the current model leads to a dramatic mis understanding of the problem. The reality is cyber attackers are stealing individual private information, they are stealing corporate intellectual property and they are stealing national secretes. The essence of the cyber issue is not corporate malfeasance. This is not Volkswagen or Enron.

- In the cyber security space, the attackers are after government, industry and consumers – we are all on the same side in this fight. The longer we spend pointing fingers and threatening each other the longer we will miss the essence if the issue and the attackers will continue to win.

- We need to realize the old paradigm of government parental ism needs to be scraped for one wherein industry and government act like the y are in a good marriage. Equal partners with differing roles that they negotiate collaboratively in the mutual self-interest of the country. We need to understand we are in this together. We need to develop new models of collaboration -- not warmed-over versions of the old structure -- and we need to invest more -- all of us.

- I think we can alter the cyber economic incentive structure and create this new social contract while still reaping the benefits of the digital age in terms of consumer service, job growth and economic development already exist in many economic sectors. In many cases we simply need to adapt incentive programs from environment, pharmaceutical, transportation to the cyber security issue of the 21st century -- in Descartes's words we can be midgets standing on the shoulders of giants.

- I leave you with one final thought. For centuries, Millenia, there was virtually constant war on the European continent. Yet since WWII we have had 75 years of essentially uninterrupted peace and prosperity – things aren't perfect –but from a historical perspective this is one of the greatest eras in Western European history. How did you do that? Did you eliminate all the vulnerabilities among your many boarders? Or did you realize that in essence you are all Europeans and needed to work together – create new models and with new roles and responsibilities? 100 years ago, I doubt you could have found many Europeans who would have believed that the continent you now live in was possible.

- I think we can do that in the 21stcentury also. I think we can work together, find new models and solve the cyber security issue. Anyway, that's what I think. What do you think?