Announcer: ... in defense of the German Marshall Fund, Mr Bruno Lete.

Bruno L.: Good morning everyone. And while we're doing a quick a stage change. Let me introduce you to the next session title, protecting civilians in times of cyber insecurity. We at GMF work a lot on traditional teams, but we're also committed to engage on cutting edge domains. And cybersecurity admittedly is one of those domains where our programming has increased substantially over the past years. Now it's not difficult to understand why the digitalization of everything has brought untold human welfare. But on your hand, it has also exposed us to some vulnerabilities including cyberattacks, cyberattacks that are conducted by individual hackers, by organized crime and by nation states.

Bruno L.: And these cyberattacks are becoming more frequent and more sophisticated. In this lights, there's really two aspects that concerns our work at GMF. On the one hand, we see that nation states still play a significant role in the world's most destructive cyberattacks. And that is due to the fact that they have access to technology, to finances, but also to the fact that there's still no clear international framework how to regulate the behavior of states in cyberspace.

Bruno L.: On the other hand, we also see that ordinary civilians are increasingly put in the line of fire of the cyberattacks. For those that recall the WannaCry attacks, one of the impacts was basically the fact that dozens of hospitals in the UK National Health Service were knocked down, endangering the lives of people that needed urgent surgery. These are serious issues to consider. In this respect, our work really focuses on the one hand on finding policies that can protect civilians in cyberspace, but also on the other hand trying to shape the rules of the game in cyberspace. What rules should they be against?

Bruno L.: When we talk about rules, we think they should not only be shaped by governments, but also have a more inclusive approach, including business and civil society that have their own valuable input to give to this. We look forward to work on these issues at GMF to do programming on cyber governance, and to identify the policies to include multi stakeholders in this debate. As a matter of fact, we will be launching a major publication on exactly this topic in September after the summer. I invite you to stay tuned for that. And without much further ado, let me perhaps now introduce you to the Chair and Motivator of the session Diana Kelly, CTO for cybersecurity solutions at Microsoft.

Diana K.: Thank you. Thank you so much, Bruno. Hello everybody. How are you today? You've got a great panel here. We're going to be discussing, protecting civilians in the time of cyber insecurity. And we'd like to make this really interactive. So if you have questions, we've got time worked in, so you can answer questions. And we're actually going to start off with a question with a poll just to get a feel for how much you may know about a certain cybersecurity things. And this poll is what do the letters APT mean? So if you've got APT, if you've ever heard of this, you probably heard of this phrase maybe in relation to cyber criminal gangs like Fancy Bear or Cozy Bear.

Diana K.: So what do you think? You can just pull that up on your app. What do you think an APT is? While you guys are looking at that, we have four options for you, and I promise one of them is correct. While you're looking at that, and filling those in, let me just briefly introduce who's here. We have Mark Green from the U.S. House of Representatives. Eckart Von Klaeden who is the VP Global External Affairs for Daimler and Antonio Missiroli, who is the Assistant Secretary General for Emerging Security Challenges with NATO. Welcome.

Antonio M: Thank you.

Diana K.: So what did we get? Okay, we've got a smart audience. You guys know what APT is. We can't trick you. We tried [crosstalk 00:04:39] to make them very viable, but so you guys know. Yes, it stands for advanced persistent threat. And that's because these campaigns are very sophisticated, that's the advanced. The persistent part is that they're very good at getting inside of networks and staying in there and getting a toe hold so that they can stay in a network for six months, 12 months at a time.

Diana K.: And then a threat obviously because they're trying to attack the company that they're in, or the organization that they're there in. So congratulations. All right. To get us started, I'm going to just get a little bit of a level set from each one of our panelists. I'm going to start with you Antonio. The question is about cyberspace being a new battlefield, a new battle dimension for NATO to address. What does that mean?

Antonio M: Well, certainly not just for NATO. NATO only owns a little portion of that space and that mandate. Yes, cyberspace is an increasingly contested space. It is a battlefield. If I may paraphrase phone Klaus of its, it is where conflict is happening by other means, conflict of confrontation. And it is a space where they folk of war is thickest and where disruption is most likely. It is a battlefield of capabilities in the sense that a number of essential services in our societies and economies are potentially affected by that.

Antonio M: The critical infrastructure of our societies and economies is affected by that finance, transport, energy health services as Bruno pointed out, communication in general and therefore also military activities are affected by that. It is a battlefield of narratives, increasingly so. And it is the critical infrastructure of our democracies, the credibility, the integrity of our democratic processes and the electoral process that are affected.

Antonio M: And it is also a nonconventional battlefield as compared to the past. It is a battlefield in which the battlefield is not shaped by states. States may still have the legal monopoly of force, they don't have the monopoly of court. And it is very often the private sector that shapes the battlefield. The cyberspace is mostly privately owned and privately run. And it is also battlefield where in a plurality of actors, both state and non state actors operate, and they have a very different methods, very different capacities and very different objectives. So it is not just a job for NATO, it is a job for everybody [inaudible 00:07:14].

Diana K.: Yes. Yeah. You're correct. Thank you for correcting me. And on that line, since it is a job for everybody, for all of us globally, as a private sector company at Daimler in this age of cyber insecurity, what are some of the big challenges for Daimler right now?

Eckart Von K.: Thank you. Before we start discussing the challenges, I would like to say some words about the huge advantages coming along with it. Because often the challenges are mirrored by the advantages. And regarding cars and trucks, I would say especially regarding cars, there are three or four huge promises coming along with it. The first is about autonomy and self determination. The second is about safety. The third is about privacy and the fourth is about comfort. And all this advantage is coming along with cars, are multiplied with the new or not so new abilities coming from digitization and artificial intelligence. And if you mirror them with the challenges, you also can see that the threats coming along are also multiplying, they're attacking these four advantages.

Eckart Von K.: And we have seen so far that trucks, cars and even in a broader sense, devices for mobility, civil devices were used for terrorist attacks. It's starting with 9/11 and civil airplanes we saw by Daesh the abuse of cars and especially of trucks in Barcelona and Berlin and somewhere else. But these were always with drivers or pilots, humans, and if you have all the other, but it is you can see how much the threat could grow and will grow if you do not have the appropriate security answers to that. So frankly speaking, maybe we will see or have not seen so many attacks with trucks and cars because of the lack of suicide drivers.

Eckart Von K.: If you have cars driving autonomously and trucks driving autonomously, of course a threat will grow. This is just one spotlight on this, and there are of course further more regarding the safety and security of the data, the passengers, the ability to attack the infrastructure within the car, via the car. And then of course in the broader sense, all the threats and changes coming for a company as a general. But maybe this is a spotlight for the opportunity.

Diana K.: We'll be getting there a little bit deeper in today. You took us from the positive straight into the suicide drivers-

Eckart Von K.: That's [crosstalk 00:10:16].

Diana K.: All right. Mark, given what you've heard so far, what do you think the responsibility is of a state, should one of the companies in that state be attacked by another nation state?

Mark G.: Sure. First let me just take a second and set the conditions of what we're talking about. You probably have all heard of the DIME model or paradigm of warfare.

And you've also probably heard of the domains of war. We think of an attack, we think of a strike against a building, and you see people and you see the wounded. But with a cyberattack, you don't see that. It's a totally different domain. But what you can see is the economic impact or the information or diplomatic impact on a country.

Mark G.: In the United States, one in five companies has lost IP, intellectual property to China. The economic impact on our nation is believed to be between 300 billion and $600 billion each year. That's dollars off of our GDP. And our GDP of course, is what fuels our ability to build the military, to protect the sovereignty of our country and the peace in the world. So it is a direct attack on the United States. And to get more specifically at your question, you take a company like Motorola in 1997 owned 80% of the market share of cell towers and networks in the world. It was a $17 billion company.

Mark G.: It did a partnership with Huawei to get into China. They stole the intellectual property, sold it on the market, subsidized by the Chinese government, and Motorola was put completely out of business. Again, taking billions of dollars off the GDP of the United States, an economic attack. And the question is how do countries, how do governments respond in a situation like that? If Daimler were to be attacked by a state entity, what is Germany's response? If Motorola is attacked, what is America's response to protect that company and to protect our GDP? And finding that measured response is the challenge that we face as governments today. So that frames the question I think.

Diana K.: Thank you. Really good. Good way to start. Does that stir any questions for anybody? If you have any questions from the audience after the opening? Comments? Yes, [inaudible 00:12:54] one.

Speaker 7: I'm going to pick on congressman Green, especially with your background, with the night stalkers. You used to have a target and a way to take out the target. I have been listening, for a decade now it feels like two conversations about cyberattacks by non state actors or state actors and we don't know what to do about it because we're worried about escalation. What would you recommend that country do when a U.S. company is attacked?

Mark G.: There are lots of options out there. Lots of options out there. On one extreme the United States government could attack a state owned entity and release its IP on the open networks. The challenge to us is to create a mutually assured destruction situation with nuclear. Clearly they know that if they respond, we have a second strike capability and we can take them out, and that's maintained peace in a nuclear world. We have to figure out the second strike capability with cyber. And I can just say the United States is leaning very far forward in that area. And my comment to the players in this arena, we see you and we're engaged.

Diana K.: Thank you. Okay, we're going to go into a question now for Eckart. Looking at car hacking, recently in an article cars were noted as a two-time connected mobile computer on wheels. The average new car has more lines of code in it than windows. So when you're in a car, think about that. You really are in a connected computer, you're creating very complex systems now. When you step on the brake or you actually stepping on the physical brake that's now controlling the brake system, or you stepping on basically a game controller and the software is then indicating to the car system that you need to stop. Right. These are complex systems.

Mark G.: And that's right.

Diana K.: And they've been hacked. Miller and Valasek are two famous researchers who a couple of years ago actually got into a jeep and we're able to control it, to steer it, to stop it. Given that, should we trust our cars? How can we trust our cars? What do people need to know about automobile security, and what will this mean when we get to autonomous automobiles?

Eckart Von K.: First of all, the huge advantage of all this technology is that we increase safety and security for the cars. That we give access to mobility for people who had only a limited access so far. Children, elderly people, disabled. You gain more time within the car. And if you come to trucks of course, and especially with an electric power trend, we will see more flexibility, less noise, less pollution. So these are all the huge advantages come along. And the second thing of course is, we have to be very, very careful about the threats and challenges. So one reason for instance for us, and I would say also for the European car companies, is that we bring autonomous technology on the streets if we're really ... That's of course never 100% security. But if we really can say it's reliable to do so.

Eckart Von K.: Our technology and in some regard also the legal framework is far than we're acting now. If there's an accident, and some competitors of us heard this of an autonomous driving car, one accident, it is all over the world news. And, “Ordinary accident even with severe consequences is maybe only report in the local news.” So the first thing is really to be aware of that and change the construction of the cars. So you have to put, of course, as we already did, safety first and then designing the car around these needs and the new digital challenges. And then of course, creating the framework with other car companies. For instance, avoiding direct access of third parties immediately with the car.

Eckart Von K.: We invented the idea of a backend server where others who have a legitimate interest in the data collected in the cars can get the access immediately, not directly to the car because of this safety reasons. And the third, of course, be in a constant dialogue with others, with competitors in a legal antitrust compliant way of course and with the authorities to be in a constant, a permanent process of improving and exchanging. And this is also a challenge for the law maker because the current way of lawmaking I think is not fast and not flexible enough to follow the tremendous process of technology.

Diana K.: Yeah. The technology is moving very, very quickly. And that's great to hear about the information sharing even among competitors because we know criminals are sharing their tips and tricks with each other. And we the defenders need to share too. Thank you. We have a poll now. Just out of curiosity, how many folks here, are you ready for a driverless car? If Daimler had one available for you tomorrow to go out and buy, who's ready for it? All right, while we're answering that, I'm going to get started on a question for you Antonio. We've got an article here, it's been reported that in retaliation for the drone that Iran allegedly shot down the US drone, that the United States launched a cyberattack against Iran that disabled some of their missile launchers.

Diana K.: So, what are your thoughts on, what can be done if militarily and globally strike back and does it make sense? As Mark is alluding to, are we getting into a situation where we're perhaps putting civilians more at risk when we're doing cyber response or a cyber response, something that nation states are going to need to be prepared to do as part of defense?

Antonio M: Yes. This is an intriguing question. It is not the first time that cyber weapons or tools have been used against an opponent. During the fight of the Global Coalition against Daesh. There were cases in which the coalition used cyber effects in order to disable air defenses and by Daesh in order to carry out certain types of operations. In this particular case, I think the peculiarity is that the cyber tools were used to respond to known cyber operations. The claims against Iran were not related to cyber activities and response was through cyber means.

Antonio M: On the right side, if I may put it this way, and I think that has been the perception of the international community, the United States used a tool that was less violent in it's immediate and direct potential consequences. You remember the debate between the air strike with the potential casualties and the use of cyber weapons. So it is a truth that the potential level of kinetic violence generated by cyber weapons is lower than traditional kinetic operations. On the other hand, as you correctly pointed out, there is always the risk, first of all of unintended consequences.

Antonio M: Cyber weapons are one shot weapons, they can be used only once and it is not entirely clear whether they will be control over the potential side effects of that weapon. It could be reverse engineered, it could be used and hacked back by [inaudible 00:21:43] player. And of course there is a more general issue related to the controllability of these weapons once they're used. I think in this particular case, the case as you mentioned, the reception was positive because it was a better alternative to the one that was initially envisaged.

Diana K.: That's a great point. Sometimes it may be that when you've got options of bombs or cyber, yeah [inaudible 00:22:08] you weigh them differently. All right, so what do we get for the poll? Are we ready to drive our autonomous if Daimler had-

Antonio M: Oh, wow.

Diana K.: We almost split-

Eckart Von K.: Wow.

Diana K.: 50, 50. I know I'm ready when we get them right because I don't like driving.

Mark G.: Wow. That's a surprise my love.

Diana K.: Are you surprised?

Mark G.: Yeah. I actually as a state senator passed the legislation in Tennessee that defined automated vehicles. And I thought people would be ... 92% of automotive accidents are human error. So as you were saying earlier the automation actually, even with bad accidents that would occur is still way more protective than without it. Because most errors are human and when the machine takes that, we're much better protected in the automated space. That's why I'm a little shocked to see that

Diana K.: Although the machine was made by a human-

Mark G.: That is true.

Diana K.: ... we may need to make sure that we did it right here.

Mark G.: They make great cars though.

Eckart Von K.: Yeah, thank you very much.

Diana K.: Okay. So pivoting back to Mark and to election security, the Financial Times reported on the US midterms, some of the ways that they were attempts to tamper with them. So they use an example of DEF CON which is an annual conference in the United States for hackers of hackers being able to hack some of the common voting systems by doing things like finding known set passwords that were available, discoverable on the internet. Discussions of phishing attacks to get into emails. We saw this also in the 2016 election with the DNC. How vulnerable are our elections both in the US but also nationally? And what impact will this have to democratic society if they are very tamperable?

Mark G.: If they're effective.

Diana K.: Yeah.

Mark G.: In the United States, our election systems are run by the states. So, the secretary of state of each state is responsible to that state for setting up the systems that run their elections. The question for us at our level, at the federal level is, well now this could be impacted by global actors, should we get involved in the states. And those of you who know our constitution, whenever the federal government comes in and does what's supposed to be the state's responsibility, that creates a lot of tension in the United States of America. So we're struggling with that issue.

Mark G.: And do we have the authority to tell a state, “Well, we're going to take over this domain and protect you from the hacks.” It appears from the past all of the retro analysis that there were no machines hacked in any election to date, although the capacity is there. Most states now in Tennessee or in America are doing a paper backup system. So you have the electronic system, but you also have the paper. And those states that are being rated as more prepared, better prepared, have that paper system, the ones that don't, are being told you're really not ready for the next attack.

Mark G.: So that's where we're struggling with this. The ramifications of having an election hacked are huge, but it's not just the hack, right? There's also changing people's perceptions. Marketers are out there using analytics to change people's minds about a purchase. So perhaps you google watches and you send an email that says, “I'm thinking about buying a watch.” That is analyzed and now your ads are all about watches on your feeds.

Diana K.: Or Mercedes.

Mark G.: Or Mercedes. Right? So that targeting of you is what concerns us in elections, so we can change people's minds. And that is very powerful. And that is the greatest concern I think.

Diana K.: Yeah. Changing minds. Okay. We have a question for the audience now which is, do you feel that elections now there was a bit of a wake up call in 2016 and are you feeling that now we're addressing this problem and that they're more resilient or are you feeling a little bit nervous and like, “Oh, maybe we're in a worse state,” now that you've understood that there can be tampering with elections and with people's thoughts and helping to shape their viewpoint. All right, we're getting that set up, I'm actually going to go back if it's okay, go back to you Eckart.

Diana K.: And we're going to take a look at an attack which is the NotPetya attack and as it went through Maersk, which is a shipping logistics company and the lessons learned out of NotPetya were one that ... and it was very nice because Maersk actually as a company has discussed openly their response and their lessons learned, which is really ... this is a great gift to us as a cyber defense community because it's very rare that a company will talk about their lessons learned, so they stay private.

Diana K.: But Maersk has talked about NotPetya, the destruction that it went through. Their systems very quickly impacted 50,000 systems, $300 million in loss. What is notable also about the NotPetya attack is that Maersk was not the target. They weren't going after Maersk. They were going after Ukrainian company and Maersk was collateral damage, which is I think an eyeopener for ... We have a very connected supply chain, we have a very connected business world. So an attack on one of our partners may ultimately get back to us.

Diana K.: And Maersk said that they've learned that they needed to focus on both prevent and recover. And I'm wondering, from your viewpoint, how do you balance that, especially in an operational technology, manufacturing environment, the cars themselves have operational networks in addition to information networks. How do you balance, prevent and recover in those kinds of systems to make sure that civilians are safe?

Eckart Von K.: Of course I cannot go in technical details.

Diana K.: Yes, no.

Eckart Von K.: But the main thing of course is what I already said is, being aware constantly about the threats and challenges from the ongoing development of this in exchange with security administration and other companies. And then of course, also thinking about what could happen step by step. For instance, from a car company in that we got the Maersk example is a good one that it was not the primary target of the company. It could be the passengers in the car. So for instance, if you close the doors that they cannot leave the car and steer the car assemble against their will, it could be someone around the car, it could be the infrastructure or the car or the truck could be used or the company to attack another company, or even the infrastructure of the country.

Eckart Von K.: And for all of these different layers of threats, you have to have your own answers and to improve and constantly improving them. I would say, and this of course is a huge challenge. But again ... and coming back to the Soviet whether people would like to use an autonomous car. This is what we see also reflected by our ... This is what we see also among our customers that beside of the huge technological advantages it has, there are concerns and there's skepticism. And we have to take this very, very seriously because this is, I would say a natural attitude of the desire for safety. All in all, we trust our industries very, very much and our infrastructure. So, for instance, if you're crossing a bridge, you're trusting that this is well constructed and it will not break down if you're on it.

Eckart Von K.: If you put your beloved ones in to a box of metal on four wheels and drive with them 1000 kilometers with 200 kilometers per hour, this is of course a huge statement of trust. And it's about food. For instance, former times in the past, the fear getting poisoned, it was huge. We know that from history, literature and so on, today we have no concern buying a hotdog at a railway station or something like that. So our whole society, although we talk so much about mistrust, it relies on trust and confidence on each other.

Eckart Von K.: And maybe in the broader sense for the political process, this is a tech. But in the broader sense, we have really to keep this and be aware that maybe this trust, this gloom of our society could be the main attack of someone who wants to hurt us.

Diana K.: Yeah, great point. And it's very much trust but verify. All right. But-

Eckart Von K.: Yeah, trusting is not enough because it has to lay on really on a constant safety and security strategy.

Diana K.: Yes. And testing.

Eckart Von K.: Yeah.

Diana K.: Yeah. And I love that point about layered because it's true. We have layered systems, we have to test them individually, test them as a whole in order to really get that full picture.

Eckart Von K.: And supervise them.

Diana K.: Yes, in production. Yeah, thank you.

Eckart Von K.: I did practice of course. And not only in production.

Diana K.: Yeah. That's actually so. When we say in production, it means when a website is running, but you mean when you're producing the car versus when I'm driving it. Yeah. Yeah. That makes sense. Okay. Thank you. Antonio, let's go to sanctions. The EU was ... I think they just passed, they'd been discussion, but now the EU is looking at sanctions for if there are state linked hacking and addressing that. And I'm wondering what are your thoughts on sanctions? Are they going to be useful, not useful, how they're being implemented. Do you think that we're going in the right direction?

Antonio M: Well, sanctions are part of a broader conversation on deterrence in this field as you got this. And of course the peculiarity of cyberspace is that hostile operation is very difficult to detect, are very difficult to deter and are very easy to deny. And that is the dilemma public authorities are confronted with and states, and international organization.

Antonio M: The EU is true just a few weeks ago, approved what they call a cyber sanctions regime, that is offspring of the cyber diplomatic toolbox that the U.S. launched one year ago. And it puts into play the capabilities the European Union as a regulatory body, and what is envisaged is the possibility, for instance of asset freezes or travel bans on people who are identified as perpetrators of cyberattacks. So it is a way of using known cyber responses to cyber operations. It's the flip side of what we discussed-

Diana K.: The other side of what we talked about.

Antonio M: ... earlier on. I think the main value is political that is imposing costs on those who carry out these attacks and to do it publicly on top of that. There's an element of naming and shaming in public that is important as a political form of deterrence. Yet again, the flip side of this is that precisely for the reasons I mentioned early on, these attacks are difficult to detect and easy to deny, the kind of intelligence that can generate the evidence that could lead to imposing sanctions against the specific individuals or organizations or states, is sensitive. It is very difficult.

Antonio M: You would probably not stand in a court of law, or we wouldn't like to present it in a court of law because we would show our end. That is the dilemma that was already presented. We were already presented within the fight against terrorism. In certain cases we had evidence, but showing the evidence would have showed our ends and our own sources of intelligence. And therefore I think that it is still predominantly a political tool that has to be used.

Antonio M: The senator spoke of DIME that is the magical formula, Diplomatic Information, Military and Economic means that have to be used in order to deter at these operations. But deterrence is deterrence by punishment. We mentioned earlier on the possible use of active or offensive cyber, could also imply known in kind operations like the ones that I mentioned. But deterrence is also deterrence by denial, is about building resilience. And I think that is the biggest part of our task in this particular domain to build resilience against all these forms of cyber attacks.

Diana K.: Yeah, completely agree. And this is something that we've been really promoting very much in the cybersecurity space is that, it was all about prevent, keep them out, keep them out. But we've learned that there are so many attacks against organizations that ... Assume at some point someone's going to get in, that doesn't mean that they got your data, that they hurt you, but you probably will have some successful infiltration. So detecting them or responding being really quickly and being resilient, that's what resiliency is.

Diana K.: That ability to detect and respond so quickly that even though they may have attacked you, they haven't actually damaged or gotten your data or put your cars out of production. So can we pop back to the autonomous car? I think we had ... Was it the ... No, oh, the elections. Yeah. So how are we feeling about the elections? We're still concerned, right? Let's put it that way. There's some more work for us to do, I think as a community elections.

Diana K.: And in that vein, I'm going back to you Mark, looking at spreading out beyond U.S. elections and looking and even going out beyond this specific campaigns itself. But we've seen some activity and it's reported here in this piece and the EU elections activity, not just at the campaigns or the candidates, but going at the think tanks. So that, again, to your point about your influencing mind, right? You're the think tanks, those organizations that monitor elections. So now that's where the attackers are spreading out. So what are your thoughts about that and about again, what we can do to address this?

Mark G.: Sure. My response is similar to what's been said already. It's about all aspects of national power. Sanctions is an option, right? But that's only one Arrow in the quiver. At some point a cyber attack becomes so devastating that a kinetic response might be appropriate. Then how you measure from the extreme to something that's less than the extreme becomes the real challenge for nations. Whether it's an election or whether it's a weapon system that's disabled, or an attack on one of our companies, our challenge is first of course attribution, which hasn't been mentioned yet.

Diana K.: [inaudible 00:37:45].

Mark G.: Okay, I missed that. But that's the first step, is figuring out who actually did the attack. And then of course, measuring the response based on what the attack is. And again, being willing to go outside of cyber to create that deterrence is I think, critical. When someone knows that for example, NATO or America will respond kinetically if a cyber attack is bad enough. Hopefully that's a term.

Diana K.: Yeah. Interesting. So, being prepared to take some action.

Mark G.: Absolutely.

Diana K.: Okay.

Mark G.: Absolutely. That's what I mentioned earlier about having a second strike capability, whether that cyber or whether that's kinetic, or whether that's economic, or whether that's embarrassing them, which was mentioned earlier.

Diana K.: So on that point we have another poll. And also I'd like to again, open it up to questions. If anybody after [inaudible 00:38:45] we're talking about elections, we're talking ... Okay, great. So I'm going to throw up the poll first and then we have a question over here. So on the topic of sanctions, and we do understand right? There have to be multiple kinds of deterrent, multiple responses available, but sanctions themselves, what are the thoughts in the room about are they going to be effective to help us stop or at least to deter some of the nation state attacks. And while we're getting your responses, we've got a question over here.

Laura Rosenberg: Laura Rosenberg from the German Marshall Fund. Congressman, you mentioned earlier Huawei as you were talking about some of the threats that we face. The president at the G20, following his meeting with Xi Jinping just said that he's going to allow U.S. companies to continue to sell parts to Huawei. He's apparently now clarified that that doesn't mean they're off the entities list yet, but they're going to be reviewing this in coming days. Just curious, I know that you've introduced a bill in Congress that would prevent sensitive tech transfer to China, be curious for your reaction.

Laura Rosenberg: For Eckart, I'd be curious for your perspective from the industry, which I know has been really wrestling with this whole supply chain question. And Antonio, I'd be curious for your perspective from allies who I know have been really trying to think about how to handle the Huawei issue. Seems that the president's message coming out of Osaka is a little bit confused in my opinion. We've said Huawei is a national security threat. The president's message today seems to be that it's more of a bargaining chip, which is exactly what we've told our allies, it's not. So I would just be curious for all of your reactions. Thanks.

Diana K.: Thank you. And let's answer in the order that you had asked.

Mark G.: Okay, sure. I'd have to go back and look at what the president said, I'm not sure. Oftentimes he uses generalities to create confidence in certain things when we turn around and do maybe things a little bit differently. And so I would have to go back and look specifically at what he said. In terms of my bill, we can't allow ... When a company does business with China because of their company's involvement in the state and the state's laws, which say they can go and take from those companies whatever they want, that is in China's laws.

Mark G.: We have to have confidence that when that company does business in China, a lot of things are happening. Number one, the military sequence in technology is being transferred to the PLA. But what about human rights? Google, when you do a deal with China, give us some assurances that the technology that's being used isn't going to be used against the Muslim population in Eastern China. So there's lots of demands that we should be doing on those companies in that technology transfer, not just make sure technology doesn't get to the PLA.

Diana K.: Okay. Thank you. Eckart.

Eckart Von K.: I would say this is just one part of a broader development we see, we regret, but nevertheless we have to adjust. And this is more or less in all major markets with the section of the European Union. So this process of de-globalization decoupling UC everywhere, we have concerns about some spare parts. We cannot use any longer in China, for instance, coming from South Korea. And we have also the debates on Huawei in the U.S. And my answer to that would be, politicians and the states should try, the international communities should try to stop this de-globalization tendency, this decoupling by international framework and regulation and treaties as good as possible.

Eckart Von K.: And if this is not possible, of course we have to adjust. We have three huge markets, the European Union, the U.S. and China and all these markets. This is a simple statement, we have to be compliant and then of course, we will follow the regulation. But at the end, if you have to develop every product more specific for the several markets and we cannot benefit any longer from international supply chains. At the end, the customer has to pay this higher prices, less products, less comfort, all the ... And maybe this could be an encouragement for politicians to avoid this as possible. But at the end we will have to adjust. We have to be compliant.

Diana K.: Yeah. And you're connecting that in the complexity of supply chains these days, it's really staggering. And to throw that way off with eliminating whole country does-

Eckart Von K.: At the end, no one has to wins on that-

Diana K.: We changed this.

Eckart Von K.: ... or will win on that. I think at the end if you see a tendency for more de-globalization for a shrinking free trade in a market system and also in non-market systems at the end, the customer has to pay,

Diana K.: And nobody likes to pay more. All right. Antonio, your thoughts please?

Antonio M: Well, it is no secret that discussion on that started only recently, mainly out of the initiative of the U.S. administration. I think it is a discussion that takes into consideration three potentially distinct issues. One is of course 5G technology, the next generation of communication technology. Another one is Huawei and all components made in China. And the third one is China itself, the big elephant in the room is China itself. And to some extent, the conflation of these three issues creates a little bit of confusion in the strategic discussion on this.

Antonio M: Let me just say that the decisions on the first element of this equation that is telecommunications networks is a national responsibility. So it is individual states that decide through attendance and their specific processes what kind of technology to use in the future and who would be the vendor that would benefit from that? Of course a degree of coordination is necessary precisely because of the nature of cyber space and the fact that we're all connected. And this is a technology that increases the degree and intensity of connectivity. It is an area in which probably it is too late to have just a binary choice. Either Huawei or not Huawei.

Antonio M: Some countries I've already decided to ban Huawei. Australia is probably the most spectacular case in point, but in Europe I think the Czech Republic has gone down the same route. Other countries are already working with Huawei also in Europe, and therefore it is extremely difficult to have a one size fits all approach to this. Even the European Commission that has marginally more regulatory authority than NATO is struggling to come to terms with this. There's a process currently underway to assess the level of dependency on that.

Antonio M: We use exactly the term supply chain security. It is a trade off between the way people put it, it is economic prosperity on the one end and security on the other. And we know the security is by nature and definition a trade off in this particular domain. And I think this is a moving target and I think the conversation will continue for quite a while precisely because it's crucial. At the same time the seizures that being taken as we speak on a national contract that have to be allocated this year and next year. I think a majority of your member states will decide who to give a responsibility for the 5G network.

Diana K.: Yeah. Interestingly and the planes coming over at the airports, there are a number of Huawei charging stations and I didn't see anybody hesitating. They're just going up and going up. It's power. So they were plugging in. Yes. We have a question over here.

Hirakita: Thank you very much. Hirakita from Nicki newspaper, Tokyo. My followup question about the Huawei to the Congressman. So according to a report, president Trump said, "U.S. companies can sell their equipment to Huawei. There's no great national emergency problem." So if this is ... I know that we shouldn't overreact to his tweet or his remarks, it is not necessarily the policy, but my question is that if he really tried to the delist Huawei from the list of national security concern, what would be the reaction of the Congress and what can Congress could do to stop? Thank you.

Mark G.: I'm certain that the president didn't mean that current laws that restrict the transfer of sensitive technology to China would be undone, right? So clearly he's talking about technology that does not have that national security threat, right? And he's talking about in one direction from the United States to Huawei. He's not talking about Huawei to the United States. We still insist that our 5G networks, we're not allowing Huawei in.

Mark G.: That is the key piece because the 5G is the highway for the Trojan horse. And when you think of all the connected systems that will be running on those networks, healthcare, automated vehicles, aircraft, we have to do everything we can to protect the network. So again, I think this is nonsensitive technology going in one direction, not the other.

Diana K.: Thank you. We're not super stocked on sanctions as being effective in this room. So that's an interesting set of feedback. I think as Antonio pointed out very rightly, is that NATO is going to be the only thing to use, but just really a tool in the toolbox. But interesting that we don't have a lot of faith, at least in this room right now with sanctions. I think there was a question over here. Yes, sir.

Kevin Y.: Hi, I'm Kevin Yonkers with Deloitte. I work in cybersecurity, so there are a lot of investigations into these types of attacks. And I think one of the key problems we see is with attribution of some of these attacks. I hear about sanctions and retaliation [inaudible 00:49:27] those type of things. But, how do we think or others I'm interested in native perspective mainly I think. How can we deal with the lack of a decent attribution or doubts about the attribution of a specific cyberattack in the future?

Diana K.: Antonio, do you want to lead with that?

Antonio M: Well, attribution is a complex process especially as carried out by States. There is an element that is traditionally called forensics that can be also be carried out by private actors. It is often carried out by private actors and companies, and it is very, very technical. There is a second level that is about assessing intent and motivation and it's more an intelligence type of work that is carried out by intelligence agencies.

Antonio M: And there is a third level that is the political/public element that is going public about that. First of all, it is entirely possible to do attribution without going public. There are countries that already practice this by reaching out to the identified perpetrators say, “Listen, we know that you did that, stop it or we will take counter measures to that effect.”

Antonio M: But of course there is also an element of public attribution that has become more frequent recently. A number of states attributed are NotPetya to Russia and WannaCry to North Korea last year. So that is not a secret that that has happened. Yet again, attribution requires to some extent unveiling evidence and that is a very, very difficult issue to do. But of course there is also merit in just saying, intelligence agencies tend to say, “It is highly likely that the actor behind this is A, B or C.”

Antonio M: It could be a state actor, it could be a state sponsored actor. You mentioned APTs at the start of this conversation. APTs traditionally are state sponsored actors. There could be also non state actors including potentially terrorist groups or criminal gangs. And of course depending on who you want to deter, you have also to calibrate your response in that particular domain. In this field, there is no such thing as international legal regime or international agency, such as the International Atomic Energy Agency in Vietnam for nuclear, or the OPCW in The Hague for chemical weapons. And therefore there is also if you like a vacuum there that we are all confronted with.

Antonio M: I think that the drive towards attribution is increasing by like-minded countries, potentially by coalitions, possibly also by international organizations as such. But attribution is just the beginning of a process because after attribution there must be a followup. After you attribute, what are you going to do about that? So attribution is disrespect, not the silver bullet, but it could be a step in the process.

Diana K.: It's a great point. It's true. Once you figured it out, are you going to take the action? The tree falls in the wood. Well, our time is just about up and I wanted to have everybody close with something. A lot of times you'd go to a talk like this and you walk away with, “Well now what?” So I've asked each of the panelists to give us a call to action, something to go read, something to go do, a takeaway from this talk that they'd like you to go with. And I have a takeaway for you.

Diana K.: I'll start with which is, if you're at all interested in what encryption does for securing civilians and people, but you're scared of encryption because it's a lot of math and it seems really weird and hard to get a handle on, there's a book Simon Singh called The Code Book. And this book is so readable, you could take it to the beach with you on summer vacation.

Diana K.: So I highly recommend if you're interested in what encryption can do to help protect us, but don't understand encryption. Take a look at Simon Singh's, The Code Book. And I'm going to start with you Eckart. What's your takeaway for everyone?

Eckart Von K.: Yep. I would recommend if you try, not only ours of course, at best ours, but not all here, our products and see what kind of contribution to safety and comfort already are there via assistant systems we have, maybe get an idea what is going on, come further. The second is we always need the right balance between data privacy, data protection and data security.

Eckart Von K.: We maybe missed a little bit the data privacy because if we talk so much about security and surveillance, we have to keep our freedoms. And third is there are so many politicians and policy makers around. I think we need on this a global regime as we have or had on arms control or on clamped protection to take the right measures here. Last point, I love the idea of Hippocratic Oath for those who make data and design this.

Diana K.: Staying, "I'm going to follow a code of conduct with my code, with my data." Yeah. Thank you. Antonio.

Antonio M: Well, the professor in me cannot resist suggesting readings. One is a book that I read already sometime ago and I found at the same time inspirational and scary. And it is written by a professional psychologist called Mary Aiken and it is titled The Cyber Effect. And she has analyzed the effect of cyberspace and the web on our social behavior, individual and social behavior. And it is very well written, it is easily accessible, it keeps you awake at night.

Antonio M: And the second one is a book titled LikeWar and subtitle is The Weaponization of Social Media written by two American analysts. It is a very instructive story of how this started out a few years ago and that how it translated into the reality, the brave new world we're confronted with right now. And it is not only based on the United States but also on experiences made in Europe. It will have to be updated regularly. I think because the pace of development in this field is so fast that it will require second, third, and fourth editions in the years to come.

Diana K.: Yeah. Thank you. Those are great insights. Mark.

Mark G.: I would just suggest at the hundred thousand foot view, you talked about the China as an entity itself, as a nation. The Hundred-Year Marathon by Michael Pillsbury is very enlightening. And I would suggest folks look at that. And also RAND Corporation, I think is got some of the best analysis on cyberwarfare. Look at RAND Corporation, they have some really good resources out there. And the last thing I want to say, just because it seems like your nation isn't necessarily responding, they still could be.

Diana K.: That's true. There's a lot of work that's not publicized, so, yeah.

Mark G.: Right.

Diana K.: Thank you all so much. Please give this panel a great round of applause. Thank you.

Antonio M: Fantastic.

Mark G.: It's a pleasure, Mark.

Eckart Von K.: Thank you.

Mark G.: It's a pleasure.