ESMT Annual Forum 2016

"Digitalization. Responsible strategies for business and society"

Keynotes

Keynote 1: Dr. Dieter Zetsche

Business leaders must understand disruption and responsibility as two sides of the same coin.

The role of responsible leaders is not to refuse this change but to leverage the opportunities it brings. This requires leaders thinking disruptively about their own organizations; if they don't someone else will. According to Dr Zetsche, "It is our responsibility to hand over strong businesses to the next generation. Being disruptive and responsible are two sides of the same coin."

What does responsible leadership in the digital age mean for Daimler and what is the impact of digitalization for the organization as a whole? Daimler was founded on a disruptive idea 130 years ago and continues to value disruption in their products and in their corporate culture. They view outside innovation, such as autonomous vehicles, as an opportunity rather than a threat. Due to rapid technological progress powered by deep machine learning and artificial intelligence, Dr Zetsche predicted that we will see autonomous vehicles in most places within five years. In response to these developments, which precipitate the biggest upgrade in the automotive industry for over a century, organizations like Daimler must embrace this innovation and shift from being car manufacturers to comprehensive mobility providers.

Beyond technological progress, this shift requires a cultural change towards employees taking "a disruptive perspective all the time" and managers cultivating a "pioneering spirit." This can be hard for organizations, especially when they are doing well: change is perceived as a risk to a successful status quo, which employs and financially supports millions of people. The introduction of car2go in 2008 is a good example, in that initially there was significant reluctance at Mercedes to share rather than sell cars. This was overcome by presenting the long-term business opportunity of providing mobility concepts; today, car2go is the global leader for car-sharing. The focus must be on how to minimize avoidable risk, whilst making the most of an opportunity and motivating every employee to follow down the road of transformation. As Dr Zetsche explained, "Stagnation is the greatest risk of all. Brilliant ideas are lost to complacency and bureaucracy."

Embracing disruption also requires a new approach to leadership. To understand what form this approach should take, Daimler held a series of global workshops across the organization to establish eight leadership principles, each of which is now actively sponsored by a member of the board. Through the adoption of this new approach, Daimler

is set to make creative, cooperative, intelligent decisions, which see it sustaining successful disruption into the future.

Keynote 2: Dr. Jamie Shea

New strategies for cyber defense

Whether in industry, government, or military, most organizations are slow to recognize paradigm shifts and increasingly obsolete business models. The key to success in all of these spheres is being able to catch up quickly and anticipate what may come next. At NATO the focus is now cyber as a domain of warfare.

Cyber cannot be viewed in isolation because it is also transforming the other four domains of warfare - land, air, sea, and space - all of which are vulnerable to cyber attacks. The true extent of the cyber threat is difficult to measure. As Dr Shea set out, “Cyber creates something wholly new and daunting. It means that you can be attacked any time of the day, from anywhere, by anyone. Cyber has democratized conflict - anybody can attack anyone.” The lengthy procurement process in the military presents a further challenge. With cyber, threats evolve much more quickly and are more disparate than in the past - with data becoming as valuable an asset for governments to protect as land and oil, especially with the development of the Internet of Things, artificial intelligence, and complex cyber supply chains. Furthermore, cyber attacks are constant, which means that cyber defense must, by necessity, be developed whilst under attack. To become more cyber resilient in this context, NATO must invest across technology, people, processes, and organization to get the optimal mix for defense , as well as understand its critical dependencies on external supplier systems and secure these effectively.

As stands, NATO is focused on three main areas. First, NATO now identifies cyber attacks over a certain threshold as it would an armed attack, initiating a collective NATO-led defense. The idea is that this will act as a deterrent. Second, NATO is analyzing how cyber impacts on all areas of warfare, preparing methodologies to cope for the likely situation that any future conflict will take place in a cyber-depleted environment. Third, NATO is looking to industry for suitable products and for ideas on how to conceptualize the challenge cyber attacks pose. Partnering with an innovation hub, NATO is seeking to collaborate with SMEs, as well as the academic and corporate world, to find trusted partners.

To conclude, Dr Shea outlined future strategic challenges. These include preparing for dependence on autonomic systems in which the human decision maker is removed and artificial intelligence has surpassed human intelligence; the reality of permanent cyber infiltration with adversaries having unprecedented levels of information; and, finally, how to create greater transparency across nations as to cyber capabilities.

Keynote 3: Melissa Hathaway

Responsible strategies for the cyber security of our businesses and countries

Over the last 25 years, the internet has become a cornerstone of the global economy, supporting family platforms, businesses, and the core infrastructure of almost all countries. We have trusted the internet to deliver these services, with developments such as online shopping, drone delivery, smart buildings, smart healthcare, and agricultural technology moving additional aspects of our lives online. At the same time, our reliance on the internet has enabled state and non-state actors to cause critical harm to the services it provides. Internet espionage against corporations and against governments is taking place at an unprecedented scale.

Melissa Hathaway presented four case studies to exemplify this threat. The first is the case of Sony Pictures, which in 2014 was the victim of political activism. The attackers stole sensitive data on over 10,000 employees and caused major disruption to the organization. It took Sony three months to return to full operations, cost millions of dollars, and put their reputation at real and significant risk. What this shows is that the business continuation plans were not good enough and the cyber security was insufficient.

The ransomware attack on MedStar Health in the US provides another example. In the attack, all data on all computers, including health records and appointment schedules, was encrypted and rendered unreadable. The disruption to the business was major but, because MedStar Health's backup system was well implemented, they could avoid paying the ransom and restore normal service quickly. Most companies, however, do not have such a robust back up procedure, nor an adequate system architecture to isolate infected parts of the system when an attack occurs.

The US Office of Personnel Management's data breach in 2014 / 2015 saw information on 24 million Americans, including Social Security Number, finger print, employment history, and details on spouses and children, being lost or stolen. Enabled by significant gaps in a decentralized IT infrastructure, with no single party responsible for overall security, this case highlights both the importance of strong data architecture as well as frequent vulnerability scanning - which, in this instance, were lacking.

In December 2015, sophisticated malware erased the core systems of a number of Ukrainian utility companies. The weakness here was the one-step access to control systems. Most governments and companies are not set up to mitigate this sort of attack or contain it effectively as and when it should happen.

Melissa Hathaway rallied for organizations to learn from these case studies and to start to develop their own responsible cyber security strategies. She concluded with a set of questions business and political leaders should be

asking: “Do we understand the cyber security landscape and its relevance? Do we understand our third-party supplier network and can we isolate weak spots? Do we know our most important assets for running the business? Do we have an instant disaster digital recovery plan? What is the maximum acceptable delay and when can we get the business back online?” In answering these, they could begin to make their organizations suitably secure.