CANADIAN GERMAN CHAMBER OF INDUSTRY AND COMMERCE INC.
LA CHAMBRE CANADIENNE ALLEMANDE DE L'INDUSTRIE ET DU COMMERCE INC.
DEUTSCH-KANADISCHE INDUSTRIE - UND HANDELSKAMMER

TORONTO

Conference Report

"Big Data & Cybersecurity Conference in Ottawa"

The Transatlantic Dialogue Initiative – Together Into the Future

February 19, 2018, @ Bayview Yards Ottawa

www.germanchamber.ca / www.transatlanticdialogue.ca

Supported by:

Federal Ministry for Economic Affairs and Energy

on the basis of a decision by the German Bundestag

As part of the Transatlantic Dialogue Initiative, which is financially backed by the Federal Ministry for Economic Affairs & Energy of Germany, the Canadian German Chamber of Industry & Commerce Inc. organized a Big Data & Cybersecurity conference on February 19th 2018 in Ottawa. The chamber hereby brought several German experts to Canada in order to discuss relevant topic within the field of Big Data & Cybersecurity together with Canadian experts during three panel discussion rounds. The three topics of interest which were discussed were *''1. Facing the big data revolution - Are Canada and Germany ready?''*, *''2. Cyber hacking and its threat to successfully progressing towards fully autonomously driving vehicles''* and ''3. *Bridging the skill gap - How can the education system satisfy big data & cybersecurity industry demand?*".

This report outlines the different conversations and its key discussion points made between the Canadian and German panel participants.

Panel 1 - Facing the big data revolution - Are Canada and Germany ready?

For the first topic Rami Abielmona (VP of Research and Engineering at Larus Technologies), Craig Burkett (Data Scientist at Lixar I.T. Inc.), Paul Mundt (Founder & Managing Director at Adaptant Solutions AG) and Mike Sips (Scientific Leader of Big-Data Analytics at the German Research Centre for Geosciences), with Stefanie Dreyer as moderator, discussed the readiness of Germany and Canada for facing the big data revolution, also referred to as the 4th industrial revolution. The focus of the conversation shifted towards Data-Control, -Privacy and -Protection on the one side and Education on the other side.

Data Control, -Privacy and -Protection

One of the key points was made about how third parties can use personal data. The European Union is ahead of Canada with its data protection regulations. The way how personal data is being treated in the USA and/or China is highly unregulated. The GDPR, which will become enforceable on May 25, 2018 in the EU, is a first good example of regulations which can be developed and implemented for data protection. This is where Canada can learn from its European counterpart and try to copy certain regulatory aspects from the GDPR for personal data protection of its citizens. Canada is indeed already more in line with the EU model for how to deal with data privacy compared to the US and it's a great opportunity for the country to become North America's leader in how to responsibly treat data.

Another subtopic of discussion which emerged throughout the conversation was the need to also regulate the analysis of big data and its outcomes. How will the regulatory institutions manage AI and user interaction? The future difficulty with any sort of application which is being used under the GDPR in Europe and uses artificial intelligence made somewhere else around the world – let's say somewhere where personal data protection regulations are weak: what will happen with the data fed to the artificial intelligence and where will it end up? Which entity will control this process and until where should the boundaries of where this data is protected be defined? In some cases data is being transferred back to the US or China in order to analyse it and reproduce a service in Europe. However, revealing the path of where the data of users eventually ends up when providing such services can also reveal the technology behind the application, which is part of the IPR and therefore considered as a trade secrets. How should we solve this dilemma of bringing transparency into how customer data is being used on the one side and simultaneously not revealing the technology behind the application on the other side?

Finally, another challenge is to bridge the dilemma of data privacy and its protection on the one side, and technological advancements on the other side. Technology tends to move faster than society, causing a particular challenge for the regulatory bodies when it comes to data protection. Data scientists need to integrate data privacy into the fundaments of their data architecture of each new project. The emerging issue is that even when there is good coding of data, decoding will eventually catch up. Hence, the architecture of the data needs to be consistently updated and designed in a way that data breaches will not give access to the entire critical data set at once but only segments of it in the worst case scenario.

Facilitate access to education and integrate data science

In order for the West to stay ahead of its competitors in the big data revolution and stay in control of its own data, its younger generations need to be better educated in the data sciences and introduced to it at a much earlier stage in life. Besides, during this education there should be a focus on what vulnerabilities there are in today's world filled with technology and what kind of data traces one leaves behind with his or her behavior.

During the discussion it was proposed that younger generations should be targeted more for considering to pursuing a career in data sciences. The education system needs to teach younger generations the benefits of data sciences and its practical aspects. In Germany, an entrepreneurial esprit

is missing when it comes to data sciences, which leads to a lack in start-ups in this particular industry. This is where Canada is doing much better and where Germany can learn from its partner. Incubators and accelerators, together with the support of the government, private sector and academia, are able to scale start-ups with a viable business model in a very short time frame in Canada. Good examples of such Canadian incubators and accelerators are Tandemlaunch, the Creative Destruction Lab and the DMZ at Ryerson University.

As data is the new oil of our new digital economy and companies will come up with all sorts of incentives to acquire it, consumers will likely give their personal data away for free in the future. Hence, society must start thinking about self-determination, raise the education level and disclose vulnerabilities for future generations. Our youth needs to be educated on what kind of data of them is out there and what data is being generated through their actions and how companies use it.

Panel 2 - Cyber hacking and its threat to successfully progressing towards fully autonomously driving vehicles

The second panel consisted of Daniel Weissland (President and CEO of Volkswagen Group Canada Inc.), Stacy Janes (Chief Security Architect – Automotive at Irdeto), Fabian Koark (Principal Consultant and Manager at Invensity Inc., Detroit), and Tamara Tomomitsu (Lawyer at Borden Ladner Gervais LLP), where Barrie Kirk (Executive Director of the Canadian Automated Vehicles Centre of Excellence) moderated the panel discussion.

Throughout the discussion the focus shifted towards what the dangers of using autonomous vehicles are and how we can establish more trust in the technology.

What are the dangers?

It was pointed out that autonomous and connected vehicles will make drivers more vulnerable to cyber hacks and cyber-attacks in the future. Using autonomously driving and/or connected vehicles will emit very interesting data sets and information for hackers, who will want to get access to this and manipulate it. Selling this data after successfully hacking a system and acquiring its data to third parties is a lucrative business with excellent growth prospects. Encryption researchers and the regulatory bodies need to work hand-in-hand in order to ensure that we come up with solutions to lessen the negative impact of data theft and manipulation.

Moreover, the vulnerabilities with autonomously driving vehicles will also entice hackers for sabotage attacks. Blackberry/QNX which is heavily

involved in cybersecurity and AV research already showed through the case of where the hacking of a connected coffee pot can enable hackers to get access to other devices and hack them, how vulnerable connected devices (IoT) are. Another example which displays the vulnerability of connected vehicles is the case where hackers remotely took over control of a Jeep Cherokee on the highways of St. Louis and kill the car's engine with the driver in it. These are horror scenarios which present windows into the future of what criminal forces will be able to do.

In technology we trust

Consumers, however, will expect their autonomous vehicle to be 100% safe and uncheckable. That is unfortunately not feasible. There will always be methods and ways to crack a human made safety system. Developers need to work with several stakeholders in order to ensure that these systems are as safe as possible and that breaches are detected at a very early stage. As only very few data streams are critical in an autonomous vehicle, it is not impossible to shelter them well from potential attacks. Developers need to come up with safety systems which increase the price and difficulty of hacking critical devices for running the systems in the vehicles as much as possible.

In the end, autonomous vehicles will still be much safer compared to contemporary vehicles. This makes it worthwhile to continue our efforts to progress towards fully autonomously driving vehicles whenever the safety systems, critical infrastructure and society are ready.

Panel 3: Bridging the skill gap - How can the education system satisfy big data & cybersecurity industry demand?"

On the final panel Melike Erol-Kantarci (Assistant Professor at the University of Ottawa), Matthias Hagen (Head of Big Data Analytics Lab at Bauhaus University of Weimar), Bhavani Krishnan (VP of Program and Product Management at the Centre of Excellence in Next Generation Networks) and Daniel Craigen (Director of Carleton University's Global Cyber Resource Centre) discussed how society can bridge the skill gap and how the education system can satisfy future big data & cybersecurity industry demand. Jeremy Depow (VP of Research and Policy at the Information and Communications Technology Council) hereby moderated the discussion.

Data Sciences - Our stepchild?

Amongst the panel participants there was general consensus: demand for well-educated data scientists in Canada and Germany already significantly outpaced supply and that this gap will broaden in size. It is clear that a

pathway for solving the talent shortage and the required changes within the education system needs to be defined for solving this serious shortage.

As one of the speakers pointed out: ''data science subjects are not treated in the way they should be in the education system. Expectations are mostly off, as there is not enough contact with this field in high school and initial contact at university level is too late. Students do not see the practical benefits of studying data sciences and have difficulties seeing themselves pursue a career in this field.''

How can we make data sciences more accessible and desirable?

The regulatory bodies need to come up with an up-to-date curriculum and innovative ways of how to make data science more interesting and appealing to youngsters. Additionally, society needs to create more role models in the computer science field for our youth and depict the sector in the media from differently, in order to attract future talent. There are still a lot of stereotypes about data scientists and the ''geeks'' who work in it.

An idea is to develop more student internship programs through membership sponsoring, where participants are exposed to potential employers at an earlier stage in life. It was pointed out that the University of Ottawa already has such a job readiness program. This six to eight months long program gives participants practical experience. After graduating with work experience in data science the participants have good prospects to start work at the company where they completed their internship. A focus should hereby be on getting more females into this field and connect them with data science companies, as there is large inequality in the sexes when looking at the prospect workforce in data sciences in both countries.

Society tends to shift a lot of its attention towards the threats associated with progress in AI, Big Data and Cybersecurity. However, we need to see the current technological advancements in a more positive light and think how it can save lives, make life easier and our economy more inclusive. A first good step would be to think more about the ethical aspects of technology and spend more time researching areas which hinder this field from being a threat, such as "machine unlearning". If we do this, our future generations will see this sector from a different perspective and see the opportunities offered to them in this field.

END

This conference is part of the Transatlantic Dialogue - Together Into

the Future initiative. The Federal Ministry for Economic Affairs & Energy of Germany together with the Canadian German Chamber of Industry & Commerce Inc. have called into life this initiative in order to strengthen the cooperation between Canada and Germany on the field of Big Data, Cybersecurity and AI. The goal of this initiative is to facilitate the exchange of best practices, concepts, new ideas and the creation of a new network between both countries, thereby creating a platform which fosters innovation. Innovation means progress, and only through progress can we create the future.

This six conferences long series will take place at different locations across Canada (Ottawa, Montreal and Toronto) and Germany (Karlsruhe, Dortmund and Berlin). Each of the conferences will have three panel discussions about sub-topics within the field of Big Data, Cybersecurity and AI. We will hereby organize a delegation with experts to the host country in order to vividly discuss the topics of interest at each conference and show the participants for a week what the other country has to offer in this area.