Securitas HIGH TOUCH – HIGH IMPACT Voordracht 14/03/2019

De onwaarschijnlijke evolutie van de informatie-technologie

Prof. Dr. Ir. Bart De Moor

bart.demoor@kuleuven.be
www.bartdemoor.be

De revolutie van de informatietechnologie begon meer dan 100 jaar geleden, met het fundamentele onderzoek in de kwantum-mechanica, door Nobelprijswinnaars zoals Planck, Einstein, Bohr, Schrödinger, Heisenberg en vele anderen. Rond 1950 vonden 3 ingenieurs van Bell Labs in Amerika de transistor uit, een elektronische schakelaar gebaseerd op die fundamentele inzichten, waarvoor ze ook de Nobelprijs kregen, en 'the rest is history'. De exponentialiteit van de ontwikkelingen wordt best geïllustreerd door de zogenaamde 'Wet van Moore', die stelt dat de rekenkracht en geheugencapaciteit van onze elektronica verdubbelt om de 18 maanden (dat is een intrestvoet van 56 %).

De IT-revolutie heeft geleid tot een geglobaliseerde wereld, waarin quasi alles elektronisch wordt gemeten (wat leidt tot een 'tsunami van data'), waarin iedereen met iedereen en alles is verbonden ('the Internet of Things') en waar de rekenkracht van onze computers toelaat om heel wat processen in toenemende mate te automatiseren. Denk hierbij aan het WereldWijde Web, sociale media, internetwinkels, globale verkeersstromen, financiële transacties enz.

In deze evoluties spelen Artificiële Intelligentie (AI) en Cybersecurity (CS) een steeds belangrijker rol. AI is een verzamelnaam voor heel wat disciplines uit de zogenaamde 'data sciences', cognitieve wetenschappen en toegepaste wiskunde. De kernbegrippen zijn geclusterd rond 'machine learning' en probabilistisch redeneren, neurale netwerken en 'deep learning', computer-visie en menselijke interactie, natuurlijke taalverwerking en kennisrepresentatie, planning en 'decision-making', automatisatie en optimizatie.

Het globale onderzoek inzake AI is exponentieel gegroeid, zeker in vergelijking met andere onderzoeksdomeinen. De laatste 5 jaar groeide het AI onderzoeksdomein met 12 %, terwijl dat de 5 jaar ervoor maar 5 % was. Terwijl in de VS de meeste afgestudeerden in AI naar Amerikaanse industrie trekken, worstelt Europe nog met uitdagingen: het aantal afgestudeerden in STEM, en degenen die afstuderen in AI stromen door naar niet-Europese bedrijven. Dat is merkwaardig, omdat inzake onderzoek in AI, Europa een voortrekkersrol speelt, zowel kwantitatief als kwalitatief en in diversiteit. In 2017 was de rangschikking inzake 'research output' de volgende: China, US, India, UK, Duitsland, Japan, Spanje, Frankrijk, Canada, Iran.

In plaats van 'onderzoek' (research) is 'ontwikkeling' (development) misschien een betere karakterisering. Immers, een echt begrip van hoe AI precies werkt, ontbreekt op dit moment nog volledig. Meestal is het nog echt een 'black box' waarbij er heel wat heuristiek komt te

kijken. Sommigen vergelijken de stand van zaken met het einde van de 19de eeuw, toen er weliswaar al auto's reden, maar er toch nog heel veel onderzoek nodig was vooraleer men echt begreep hoe de vork aan de steel zat. Op een betrouwbare wijze omgaan met de heuristiek van AI is dus een grote uitdaging (bvb. bij medische diagnoses, of bij 'decision support' in levens-belangrijke situaties). De zoektocht naar 'explainable AI' is dan ook nog maar net begonnen.

Toch kunnen we nu al stellen dat AI pervasief is in onze samenleving en dat ook zo zal blijven in de toekomst. Er zijn immers geweldige perspectieven in quasi alle maatschappelijke uitdagingen: Gezondheidszorg, 'Smart Cities', Industrie 4.0 met noties zoals 'digital twins', processen in de financiële wereld en bij de overheid (denk maar aan 'Tax on Web',…), enz.

In deze context wordt CyberSecurity (CS) meestal beschouwd als een eerder technische aangelegenheid die weinig impact heeft op een business als dusdanig. Nochtans is het een *conditio sine qua non* die de digitale revolutie faciliteert: betrouwbaarheid, robuustheid en bescherming van digitale assets zijn noodzakelijk voor de lange termijn en voor de adoptie van nieuwe producten en diensten. In dit soort onderzoek staan we in België aan de wereldtop, in het onderzoek naar de beveliliging van strategische technologieën bij toepassingen in 'the cloud', het web, mobiel, IoT enz., in het onderzoek naar de veiligheid van software en applicaties, beveiligingsdiensten, systeem- en infrastructuurbeveiliging, en het onderzoek naar beveiligingsbouwblokken m.b.v. cryptografie, veilige communicatie en hardware.

Beide disciplines zijn ook sterk verweven: zo is er een grote behoefte aan meer CS bij AI en meer AI bij CS. We zullen ook ingaan op de maatschappelijke/democratische deficits die in deze evoluties ontstaan, alsook op de juridische en ethische.

Tot slot zullen we kort de recente initiatieven toelichten van de Vlaamse regering, die nog dit voorjaar twee grote impulsprogramma's zal goedkeuren voor AI enerzijds en voor CS anderzijds. Elk van deze programma's bevat een luik Flankerende Beleid (ethiek, opleidingen en 'outreach'), een luik implementatie naar de Vlaamse industrie, en een luik Strategisch Basisonderzoek.