Council of the European Union
General Secretariat

Directorate-General Administration
Security, Safety and Communication and Information Systems
Directorate Communication and Information Systems

Report of the CII 2016 US Study Trip

April 18 till 22, 2016

		Initials	*Institution/ Organisation*
Time:	April 18 till 22, 2016		
Place:	San Francisco and Silicon Valley		
Present:	Mr Bernard MAGENAHNN	BMA	EC
	Mr Philippe VAN DAMME	PVD	EC

Objectives:

There are four main objectives:

1. Understand the strategic trends of products and services and their impact for international public organisations;

2. Get insight on how to lead the digital transformation of organisations, in an innovative way;

3. Observe trends in management of digital talent and corporate social responsibility;

4. Build management relationships.

In this context, different companies will be visited, covering seven areas of importance in ICT:

1. **IT Security**: this is one of the biggest operational challenges for all European Union Institutions (EUI). Cyber threats are increasing in number and sophistication and the EUI are high-value targets. At the same time, EUI are knowledge-intensive organisations, have an increasingly mobile work-force and are under increasing pressure for ubiquitous access to information. A delicate balance between security and meeting user demands is needed.

2. **Big Data & Analytics**: big data and big data analytics have a huge potential, yet they are complex to handle. Wide use of big data raises many questions to the EUI as a regulator, as a policy maker and as an organisation. The potential of big data is yet to be exploited for better design and policy making, taking into account the wealth of data available in the public domain. At the same time, EUI will be equally under pressure to strengthen privacy and protection of personal data.

3. **Open Source**: the EUI are strong supporters of open source. Open source is embraced to avoid lock-ins, increase flexibility and lower costs for EUI. A major example for adoption of open source solutions is the recent decision to migrate the official website of the European Union (europa.eu) to the open source content management system Drupal.

4. **Cloud Computing**: cloud technology has an big potential to improve the quality, cost effectiveness and agility of the EUI IT environment. In 2015, the EUI completed a large experimental public procurement for Cloud services, which is now progressively being exploited. Yet many challenges remain, e.g. on security and privacy, integration of existing information systems, ensuring data/information systems portability. At the same time, the EUI Data Centres need to be further automated and transformed to a 'cloud'-like facility.

5. **Mobile**: mobile devices, smart phones and tablets, are becoming ubiquitous. EUI staff increasingly expect to be able to work anywhere, anytime, communicating and collaborating in more fluid and interactive fashion. These new tools offer huge possibilities for better and different ways of working and collaborating together (together with better knowledge sharing, productivity and work-life balance). Yet they also raise serious questions regarding e.g. security, data protection, applications design and architecture.

6. **Talent Management**: the increasingly digital world requires new skills. Digital skills and talent are becoming harder to attract, develop and retain. The planning and management of digital talent has gone high on EUI's agenda.

7. **Social Responsibility**: along with the above-mentioned challenges, the EUI have a particular role to act as a guardian of the EU law and lead by example. In that respect, a particular attention is given to the impact of organisations' practices on staff, the wider community, the society and the environment.

Agenda:

1. Day 1 (April 18, 2016)
    1.1. Partech Ventures
    1.2. Skyhigh Networks
    1.3. Box
    1.4. Cloudera
2. Day 2 (April 19, 2016)
    2.1. Cisco
    2.2. US Federal Government (supported by Cisco)
3. Day 3 (April 20, 2016)
    3.1. FireEye
    3.2. EMC (VMWare)
    3.3. Red Hat
4. Day 4 (April 21, 2016)
    4.1. Oracle
    4.2. Google
5. Day 5 (April 22, 2016)
    5.1. Splunk
    5.2. Debrief with the group

More details and practicalities regarding the agenda, as well as some of the slide-sets used by the different companies, can be found on the wiki provided by the EC (available only for the participants).

1. **Day 1 (April 18, 2016)**

   1.1. Partech Ventures

   People:

   Company:

   Partech Ventures (originally a subsidiary of the Paribas Bank) is a venture capital firm specializing in information and communication technologies, and operating in Europe (Paris and Berlin), as well as in the US (San Francisco). Partech Ventures currently manages investments across three separate funds, each dedicated to different stages of investment: SEED, VENTURE and GROWTH.

   SEED is always co-invested with typically 2-5 other investors, investment consists of typically up to 1M€, Partech manages to have a failure rate of around 50%. Some successes are PriceMatch and Bugcrowd.

   VENTURE is mostly co-invested with another investor, investment consists of typically up to 20M€, Partech manages to have a failure rate of around 20%. One to two deals per year are followed-up, over a horizon of 8 years.

   For GROWTH, a 0 failure rate is expected, on one to two deals per year, with an investment of between 10 and 40M€.

   Main takeaways:

   - A big difference in approach between the Silicon Valley and Europe is the ambition level: if a SEED does not grow high and fast, it is sold within 12 months in the Valley, whereas in Europe steady growth is considered as a moderate success;

   - Developing a product goes further than developing a new technology. European entrepreneurs sometimes forget to go further than developing a new technology;

   - The prime element for deciding on whether to invest in a company or not, is the people driving it (not the financials, metrics etc). And these people are found mainly via introductions/connections, human interaction, chemistry between people.
     Key criteria for people are integrity/transparency, determination and especially the ability to build a team (leveraging distributed capabilities);

   - What Europe could do differently:
     - make more 'smart money' available (not big programs);
     - make Entrepreneurs heroes, rather than the people working in big companies;
     - use Venture Capitalists instead of banks for entrepreneurial investment.

1.2. <u>Skyhigh Networks</u>

People:

Company:

Skyhigh Networks was founded by ▮▮▮▮▮▮ in 2011, investment by Greylock Partners and Sequoia Capital Venture Capitalists. It is a cloud security company, delivering a service used by companies to discover the cloud services being used by its employees, to analyse usage patterns in order to detect anomalies and malware, and to encrypt data stored in the cloud.

Main takeaways:

- Cloud is happening today, whether we approved it or not; people are using applications like Evernote from the office, or any other consumer app in the cloud;

- Cloud is believed to be more secure than trying to keep all data in one's own hands:

  o 95% of security failures are consumer's fault (e.g. passwords not securely stored); 92% of companies have compromised credentials for sale; companies block well-known but low risk services more than services that pose high risks to the company's data security;

  o Cloud suppliers can invest much more in security than each individual customer can;

  o a Cloud Access Security Broker 'CASB' can bring centralised control of multiple services which would otherwise require individual management (and which might, each on their own, not detect any problem).

1.3. <u>Box</u>

People:

Company:

Box was founded in 2005 and essentially provides for a content management platform which provides file-sharing, collaborating and other tools (workflow, search, encryption, retention, policies, …) for working with files that are uploaded to a Box environment. Enterprise clients include GE, Coca Cola, Nike, Unilever, Eurostar etc.

Main takeaways:

- Mega-trends such as new ways of working, collaborative business processes beyond company boundaries, digitalisation and increased emergence of security threats, are driving the Enterprise IT transformation towards cloud usage (Office 365, Salesforce.com, NetSuite, …).

The difficulty is to handle and share the content in an easy way in this context, with a cohesive user experience;

- Box claims to deliver such an cohesive and secure content platform (incl. deep integration with Office 365 for co-authoring, partnership with Skyhigh for cross-service security   etc.). Introducing Box in a legacy environment will however require moving all content to the Box stack/cloud;

- Regarding Digital Workplace / New Way of Working:

    o Open space, free food, drinks, …;

    o Choice between Apple laptops and Windows laptops (80% choose Apple). First-line IT helpdesk (15 people for 1500 people) have seen a tremendous decrease of tickets following the move to Apple laptops and the obligation to physically go to the IT helpdesk when one has a PC problem (versus calling, sending an e-mail, etc.).

1.4. <u>Cloudera</u>

People:

Company:

Cloudera was founded by three engineers from Google, Yahoo and Facebook in 2008 and now counts around 1200 employees. Cloudera provides Hadoop-based software, support and services for big data handling. Cloudera interfaces with viewers like Tableau, ClickView, SAS, Hunk, … The business model followed by Cloudera for big data is similar to the business model used by Red Hat for Linux (stable distribution, security checks etc.).

Main takeaways:

- The reason for the evolution towards big data is the combination of new types of data (especially unstructured data) and new algorithms, such as predictive, pattern recognition rather than simple SQL;

- The main reasons to go for Hadoop-based solutions for big data analytics are the cost and the scale.   The cost for less relevant data typically ranges from 100€ to 1k€ per Tb, versus 10k€-100k€ per Tb via traditional Oracle, Teradata etc. solutions. With Hadoop, one can go 100 times faster thanks to parallel processing and 'schema-on-read', versus 'schema-on-write' (on structured data).

2. Day 2 (April 19, 2016)

2.1. Cisco

People:

Company:

Well-known by all. Interesting to know is that around 98% of Cisco's production is outsourced, and that around 3.000 out of the 70.000 employees work in IT (so not in the Network part).

Main takeaways:

- Digital disruption is ahead of us, following hyper-connectivity (Internet of Things - IoT), an addition of 5 billion people connected to the Internet over the next 5 years (via mobile, satellite) and the extrapolation of Moore's law: in 2023 a $1000 computer will have as much computing power as the human brain, in 2050 a $1000 computer will have the same computing power as all humans on Earth;

- Cisco's strategic priorities:
  - o Evolution of the network;
  - o Focus on operators/service providers;
  - o Security (most of the 14 acquisitions the last year);
  - o Internet of Things;
  - o Enable customers to migrate to a 'Hybrid Cloud' (partially public, partially private);
  - o Analytics and big data;
  - o New generation of data centres;

- Cisco's innovation eco-system has extended from the traditional 'Build, Buy, Partner' approach, to the 'Invest & Co-develop' approach since mid last year. To that end, 9 innovation centres have been created (in EU: Berlin, Paris, Krakow, London) to work together with customers on the development of new ideas. Ideas for co-development have to be submitted via the local Cisco teams;

- Regarding HR policy (programme called 'Breaking HR'):

- o Cisco just moved away from a formal performance management system (stopped ratings & rankings);

- o This did not change the attrition rate, nor the number of promotions, but now they are based on the empowered decisions of the 'leaders' (typically equivalent to director level in EUI), who in turn are followed-up closely by senior management. This requires more formal and informal gatherings with staff;

- o For technical people, there are two possible career tracks (expert track versus management track), which are considered equivalent. There's also a special focus on 'pay parity' (also for men);

- o The best performing teams seem to have 3 things in common:

  - ▪ Focus on individual strengths within the team;

  - ▪ Environment of safety and trust in the team;

  - ▪ Shared values within the team;

- Regarding IT:

  - o There's a tendency of convergence between the 'Network' and the 'Data Centre' business/solutions/vendors. The traditional 'Network' vendor Cisco is hence moving also into the Data Centre business, with systems like UCS (Unified Computing System, including a UCS Manager), e.g. enabling the push of network, server and storage policies via a single platform, or the brand new Hyperflex product e.g. for smaller VDI deployments (max. 10k virtual desktops);

  - o Governance of IT investment/changes:

    - ▪ There's a Service Owner for each service, who is end-to-end responsible (cost, revenues, security, …) and who is driven by an architectural roadmap. All changes to services need to be defended before in an 'Architecture Review Board', chaired by the CIO;

    - ▪ All changes to services that are under the responsibility of the CIO (e.g. networks, collaboration tools, …), get their investments approved by this 'Architecture Review Board';

    - ▪ All new capabilities for other business units need to be approved by the business owners, and hence prioritised within that business unit's envelope;

    - ▪ All investments launched within Cisco's 'Transformation Portfolio', are to be approved by the a committee composed of the COO (chair), the CDO (Chief Digitization Officer) and the CIO;

  - o Cisco has a clear focus on simplification and standardisation of IT infrastructure (in the cloud), application driven. Through this thorough standardisation and via its internal e-Store for ordering virtual environments, applications and resources, Cisco claims to deliver to a developer a full operational environment (infrastructure, middleware, automated build and release, …) *in 8 minutes, instead of 8 weeks before.*

- o 80% of development is now agile-based, 20% is using the traditional 'waterfall' methodology. Agile development has been introduced 2.5 years ago.
- Regarding Networks:
  - o Cisco considers that new networks are needed for new solutions, i.e. networks will need to go beyond delivering static connectivity. Cisco refers to this as (software driven) 'Digital Network Architecture' (DNA).
  - o DNA is focused on:
    - Digital (software) capabilities, enabling simplicity and automation of network adaptations, in order to increase agility and to drive costs down;
    - Security and compliance, using the network as a 'sensor' for analytics of what is going on (e.g. during an advanced persistent attack) and as an 'enforcer' for network segmentation/partitioning.

2.2. <u>US Federal Government (supported by Cisco)</u>

People:

Company:

US Federal Government spends approximately 100 billion USD per year on IT, of which 75% for 'keeping the lights on / keep it running'. There's a substantial increase for Security (18 billion USD) and an exceptional 3.1 billion dollars requested for 'IT modernisation'.

Main takeaways:

- The IT modernisation will mostly rely on services purchased rather than on own development, and foresees a horizon of four to five years of work. Flagship projects could not be disclosed. However, the idea is to have core capabilities (needed for all Agencies, like e.g. a payment function) in the cloud, on which all Agencies can develop thin layers of features (via a standard API) which are specific to them;

- Each Agency will need to provide a self-supporting business case in order to receive a part of the 3.1 billion budget, so that the returns/pay-back can be used for continued modernisation later on. Budget will only be released gradually, based on the achievement of milestones;

- Governance will be based on a 'bi-modal IT' model, where each CIO of each Agency will have the leadership over 2 distinct parts: 'keep it running' and 'transformation'. However, organisational resistance is the key factor to overcome, which will be tackled with a three-step approach:
  - o have a clear understanding across the organisation of where one currently is;

   o have a clear 'to-be' model;

   o engage a team for the transition (incl. the appropriate pace of transition);

- Whether to have certain applications/capabilities in the public or in a private cloud is dependent on the certification level the public or private cloud has received (based on FEDRAMP - Federal Risk and Authorization Management Program) and the required level deemed necessary for each application/capability;

- A recent breach of the personnel records, due to stolen user credentials and the subsequent access to system admin rights, has led them to the implementation of 'two-factor' authentication and the reduction of people with system admin rights.

- Tony Scott would be an interesting person to keep in touch with, especially considering some parallelisms between the US Federal Government and the EUI (challenges, link with Agencies etc.).

3. <u>Day 3 (April 20, 2016)</u>

3.1. <u>FireEye</u>

People:

Company:

FireEye is an integrated security company, covering the assessment, the prevention, the detection, the analysis and the response related to ICT security matters.

The company was created some 12 years ago, and delivered its first products 5 years later.

It has now a billion USD turnover, with a positive cash-flow (roughly 40% of the free cash flow is re-invested in R&D). FireEye has approximately 3.500 staff of which 900 world-wide in 66 countries, hiring mostly ex-employees from US Agencies. Around 300 staff work on incident response.

Main takeaways:

- FireEye has an integrated platform (called 'MVX' - Multivector Virtual eXecution engine) for threat detection, covering network, e-mail, endpoint and mobile solutions, whereas competitors would have tendency to focus on each individual domains (e.g. Palo Alto firewall, McAfee virusscan, ...). Such integrated solution is claimed to outperform sandboxing.
  Adding this to the threat intelligence (DTI - Dynamic Threat Intelligence, in the cloud) and the services and support, like incident response and attacks on request of customers, results in a service offering referred to as *'FireEye as a Service'*, including a 'Single Pane of Glass' possibility integrating third party products;

- A market consolidation is expected in the security area, as it is anticipated that the money taps will be (partially) turned off. Especially small companies are expected to be taken over;

- FireEye addresses Privacy in 3 ways:

    - Minimization: collect only the needed information, mainly looking at patterns rather than at content itself;

    - Communication: say what they do, including who, what, when and why information is accessed;

    - Allow for customer auditing;

- The three mechanisms to establish adequacy of privacy safeguards in the US (Safe Harbor/Privacy Shield, standard contractual clauses and binding corporate rules) can all be legally challenged based on the same arguments as used against Safe Harbor. The US Authorities can always issue either a US National Security Letter or a FISA Warrant, obliging any US based (parent) company to give access to data without informing its customers.

3.2. <u>EMC</u> (with focus on <u>VMWare</u>)

People:

Company:

Well-known by all. Interesting to highlight is the recent merger with Dell.

Main takeaways:

- Regarding the Dell-EMC merger, the statement is that VMware will remain independent in the new structure (as was the case up to now), and that Documentum will stay as a product line, whether within EMC or in another structure;

- Expertise to run a Cloud is difficult to find (only 3.000 people world-wide);

- According to VMWare, the 'third platform' (i.e. the computing platform adapted to mobile, social media, cloud computing, big data and Internet of Things) engenders:

    - Abstraction of the infrastructure for applications;

    - Resilience moving away from the infrastructure into the applications;

    - A new, more agile and standardised operational model ('DevOps').

3.3. <u>Red Hat</u>

People:

Company:

Red Hat is a software company providing open-source software products to the enterprise market (not to the consumer market), using resellers as primary channel They have around 8.500 staff and a 2 billion USD turn-over (of which 12% from Government). 90% of the Fortune 500 uses Red Hat, 25% of bookings in 2015 came from the EMEA region. Since last November, there's a stand still in the patent war with Microsoft.

Main takeaways:

- Recommendations from Red Hat when thinking about moving to the Cloud:
    - Start small, as people have to learn;
    - First automate and standardise, before 'lifting and shifting';
    - Have an exit strategy (for applications and data), as often so-called 'open APIs' are not entirely open. Cloud has hence the potential to be the mother of all lock-ins …

4. **Day 4 (April 21, 2016)**

   4.1. Oracle

   People:

   Company:

   Well-known by all.

   Main takeaways:

   - Oracle has a software-defined IaaS offering providing a virtual Data Centre (for storage, servers and network) and a PaaS solution, allowing for a customers to develop, run and manage applications without the complexity of building and maintaining the infrastructure associated.
     The value presented by Oracle in this is:
       - The high level of software-driven automation, leading to a claimed productivity increase of 50-60%, reducing the need to have the right skills on board;
       - Allowing to move also one's legacy systems into this environment, as opposed to Amazon, Microsoft, Google etc.;

- o Oracle Cloud has several locations in Europe (Germany, UK, Netherlands), but the service can also be offered on customer premise (private cloud) by Oracle staff;

- o Through Oracle's Enterprise Manager, a single pane of glass is provided, integrating different applications in an Oracle cloud (e.g. Salesforce.com and EBS);

- Oracle's vision for the cloud in 2025:

  - o 80% of production applications will be in the public or private cloud, 85% based on SaaS;

  - o Two full suite providers will have 80% of the SaaS applications market;

  - o 100% of the new development/testing will be in the cloud;

  - o Virtually all enterprise data will be stored in the public or private cloud, especially considering the impact of IoT;

  - o Enterprise clouds will be the most secure IT environments.

4.2. <u>Google</u>

People:

Company:

Well-known by all. Interesting to know is that Google now employs around 61.000 staff, in 100 offices across 50 countries, and has a turn-over of 74 billion USD. All this in 15 years time since its creation.

Main takeaways:

- One cannot direct innovation. The only thing that can be done, is to create an innovative environment, based on 3 principles:

  - o Focus on the user. User experience goes above market share;

  - o Give freedom and information to your employees, give people a bit more freedom than you're comfortable with.
    E.g.:   and   speak every Thursday via video conferencing, open to all employees, about confidential matters; people should spend 20% of their time on new ambitious ideas.
    Employees are recruited, mainly based on general cognitive ability, leadership, role-related knowledge and the level of 'Googlyness' (default to open, don't be evil, …). There are 2 million job applications per year, filtered automatically, after which a selection is initiated mainly based on referrals. The next step consists of interviews by a hiring committee

(without the hiring manager). Only after that, the hiring manager comes into picture for final recruitment;

  o Think big and be bold in your ambitions, mediocrity is not OK. People not meeting their ambitions can still perform extremely well. Google believes in 'rapid ship & iterate', i.e. nothing should be perfect during the first iteration;

- Google considers that the main drivers for the public sector to move into the cloud are the cost reduction (60-70%) and providing a more attractive and collaborative environment to one's staff.

- Cloud is believed to be more secure than trying to keep all data in one's own hands (no upgrade of hardware, patches every month, nothing is stored on the device, …), but the question about trust/privacy remains.

5. Day 5 (April 22, 2016)

5.1. Splunk

People:
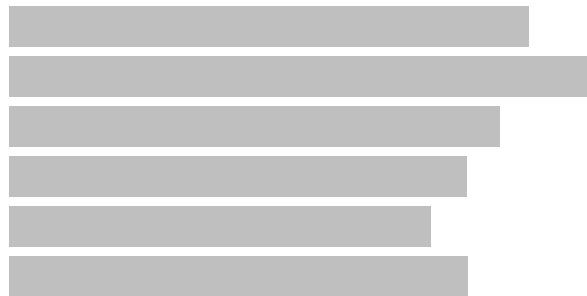
Company:

Splunk is a software company, specialised in software for (machine) big data collection, monitoring and analysis, especially in the security domain, but also beyond. It was founded some 10 years ago, and had a turn-over of over 650 million USD in 2015 (with a YoY increase of nearly 50%) and around 2.100 staff. Splunk is used in many EUI, such as the EEAS, the ECB, the EC, the EP, the GSC etc., and has 11.000 customers across more than 110 countries.

Main takeaways:

- As the volume of data across all EUI has gone above 1Tb,　　　　　　　announced that the invoicing for Splunk products to the different EUI would be adapted to take this into account. Practically speaking, the price for Splunk products would go down, also on the current contracts;

- Splunk's approach to big data is based on unstructured data, universal indexing and schema at read, which enables large scale fast data collection, analysis, dashboarding etc.;

- Splunk is available on premise, but also in the cloud (on Amazon web-services, e.g. in Franfurt or Dublin), with a possibility to have a hybrid approach, including hybrid searches and single pane of glass visibility;

- An impressive demo has been given on the possibilities to create an integrated dashboard overseeing an entire Data Centre, highlighting the possibilities beyond the traditional security analysis used at many EUI (such as network monitoring, website usage, etc.). It has to be noted, though, that creating such dashboards would easily require some months of work, including several weeks of Splunk professional services;

- Splunk is also to be positioned as a more extended Security Incident Events Management system - SIEM, especially when using unstructured data. It is one of the leaders in Gartner's SIEM Magic Quadrant;

- With the evolution towards more agile delivery and deployment of applications using so-called 'containers' and micro-services (avoiding the overhead of starting and maintaining virtual machines), Splunk has taken steps towards a partnership with Docker for collection of container logs and statistics.