In the framework of the upcoming Global Forum 2021, planned for December 6th & 7th in Muscat, Oman, should the pace of this pandemic subside, four preparatory thematic webinars, featuring contributions, reflections and dialogue among key experts and interested stakeholders, are organized.

This report sums up the discussions of the Global Forum Thematic Webinar II.

Global Forum Thematic Webinar II

April 7th, 2021

COVID-19 Pandemic as a Science and Technology Accelerator?

Disruptive Digital Technologies, Artificial Intelligence, IoT, 5G, Blockchain …

Participants (61):

Fatma Al Mukhaini, Wafa Almamri, Jora Al Qasmi, Al Waleed Al Rashdi, Eng. Amani, Ingrid Andersson, Sylvia Archmann, Sherif Aziz, Youssef Berbash, Jean-Pierre Bienaimé, Katherine Blizinski, Anatoly Burman, Marek Canecky, Jean-Pierre Chamoux, Bruno Chazal, Mariane Cimino, Donald Davidson, Bob Deller, Philippe Denis, Koffi Fabrice Djossou, Walid El Abed, Geneviève Fieux-Castagnet, Kevin Fitzgibbons, John Giusti, Alessandro Guarino, Stéphane Grumbach, Amir Johri, Nitya Karmakar, Hugo Kerschot, Eric Légale, Sébastien Lévy, Judy Logan, Tom Mackenzie, Jeremy Millard, Michele Mosca, Eikazu Niwano, Hervé Rannou, Murli Rajan, Vincent Ribière, Alfredo M. Ronchi, Susie Ruston McAleer, Gérald Santucci, Patrick Saunier, Jon Shamah, Gary Shapiro, Alan Shark, Chetan Sharma, Susanne Siebald, Baïla Sow, Michael Stankosky, Bénédicte Suzan, Yoshio Tanaka, Michèle Thonnet, Daniele Tumietto, Sylviane Toporkoff, Eliane Ubaliljoro, Oliver Väartnou, Daniel Van Lerberghe, Olin Wethington, Paul Wormeli, Sarah Zhao.

The Global Forum Thematic Webinar II on "COVID-19 Pandemic as a Science and Technology Accelerator & Disruptive Digital Technologies, Artificial Intelligence, IoT, 5G, and Blockchain" took place on April 7th, 2021 from 13:30 to 15:00 UTC+2 via Zoom.

About 60 participants joining from all over the world—for some it was very early in the morning, for others late at night—made this webinar a particularly intense and thought-provoking one. Framed by brief expert presentations, the participants engaged in high-level debates and deep discussions on critical issues and opportunities.

It was the second of a series of four live webinars (the next will be on June 9th, 2021) featuring contributions, reflections and dialogue devised for the purpose of feeding the framework of the upcoming Global Forum 2021.

Agenda

Welcome and Introduction

Topic 1: COVID-19 Pandemic as a Science and Technology Accelerator?

Stéphane Grumbach, Research Director, INRIA, France
Living under a long-lasting Pandemic & Impact on the Evolution of Technologies

Amir Johri, Senior Specialist, Ministry of Health of Oman
The Role of Digital Enablers in Coping with the Pandemic – Examples from Oman

Paul Wormeli, Innovation Strategist, USA
Cross-boundary Information Sharing Principles – Complexities and Challenges

Topic 2: Disruptive Digital Technologies, Artificial Intelligence, IoT, 5G, Blockchain …

Gary Shapiro, President & CEO, CTA – Consumer Technology Association, USA
Disruptive Technologies, AI, IoT, 5G

Geneviève Fieux-Castagnet, SNCF – L'Éthic Groupe, France
A European Perspective of Ethics for AI Systems

Michael Stankosky, Research Professor, George Washington University, USA
Internet of Ideas

Don Davidson, Director of Cyber-SCRM, Synopsys, USA
The never-ending dilemma of the need to share vs. protect information!

Concluding Remarks

Welcome and Introduction

Ingrid Andersson, moderating, together with Sylviane Toporkoff, welcomed the participants along with Sébastien Lévy to this 2nd webinar preceding the Global Forum 2021 to be held on December, 6th & 7th, 2021 (or early 2022 should the pandemic still prevail), in Muscat, Oman.

Muscat is a frequent host of international diplomatic negations and regularly proves to be a place for high level events. The organizers of the Global Forum got the strong support from several actors in Oman for hosting the Global Forum 2021 in Muscat.

Topic 1: COVID-19 Pandemic as a Science and Technology Accelerator?

Stéphane Grumbach, Research Director, INRIA, France, **opened the discussion with remarks about living under a long-lasting pandemic and the impact on the evolution of technologies**.

It is better to be resilient and try to adapt to whatever might come, rather than just trying to go back to how the world was before.

The Covid-19 crisis has fundamentally affected our societies: The limitation of liberties, such as movement restrictions or the type of meetings people are allowed to have, rise central questions and are politically very controversial. Many sectors are suffering, and some might collapse. Societies are facing new logistic challenges and there is a much stronger uncertainty in making plans. Covid-19 led to the emergence of new behavioural norms (the way we greet each other, the way we organise meetings etc.) and new forms of organisations. The pandemic also reshuffles things on the political and geopolitical spectrum.

It is a point in time where many aspects of our lives are reshaped—with a huge potential for both good and bad, and it will be important to reflect on what can be done and what should be done. Technologies play a central role. They fundamentally contribute to keep parts of our societies functioning and determine basic dimensions of our society, such as the way we meet and move, how people can exchange, but also information processing and data access. One particular aspect is the use of technologies in the fight against the virus.

Still, even before the pandemic, digital intermediation platforms already changed the way we exchange (e.g., emerging commercial and educational platforms, home delivery etc). These platforms have been essential to keeping societies functioning during the pandemic.

There are various ways to fight COVID-19 using IT, such as contact tracing, real time mapping of the spread of the disease, population monitoring or the use of coercive measures. The majority relies on smartphones linked to private actors, such as the large intermediaries, and public actors, i.e., health authorities, research institutes, police etc. These approaches are rather controversial and reveal strong geopolitical tendencies.

The way companies like Apple, Microsoft, Amazon, Alphabet, Facebook, Tencent or Alibaba increased in market values during 2020 is impressing and demonstrates the increasing universal control of platforms.

The technologies used to keep our societies functioning are mostly technologies that emerged in the last 20 years, provided by companies that are becoming the most powerful actors from many points of view. The large digital platforms are the largest market caps today and conflicts

between these digital platforms and territories are multiplying. Besides, those platforms compete with national public administrations with regards to the services they provide.

We should take the opportunity of the current crisis to rethink services and service provision. For instance, the tools that are currently used for education are fine, but they are not good enough to provide effective distance learning. The same applies for health and many other sectors. Another issue is the use of IT tools to fight the virus. These surveillance tools are extremely controversial and raise privacy and civil liberties concerns, especially when there is no real trust in the state. How can one be sure that the harvested data are used only temporarily and exclusively to fight the spread of the virus?

There is a real opportunity to rethink essential services that would make societies more resilient in times of crisis and we should take that opportunity.

Referring to the issues of dissatisfaction with remote learning and trust in governments, **Jeremy Millard** argued that some Scandinavian countries have done rather well, and those are the countries where the state is generally trusted. The question seems to be less about how the technology is used, or the competence of the governments or the big companies that are using it, but more about political culture and the pre-existing trust, the way things are presented, i.e., the people are being given clear and straight advice.

Stéphane Grumbach replied that at the beginning, European countries started developing contact tracing applications and most of them ended up proposing the Apple/Google solution. People finally had greater trust in Apple and Google than in their governments.

Singapore just passed a bill governing police use of contact tracing data to collect evidence. Imagine there is a crime, and you have the contact tracing application in use, which means that you can see who has been on the crime scene. Will you use it or not? And if you use it for a crime scene, you might also use it for something else… This question of trust is much more general and applies to everywhere in the world.

With regards to the general dissatisfaction with remote education during the pandemic, it has to be said that education has to be fully reinvented—regardless of the crisis. Currently, we just reproduce in the digital space what we do in the physical space. But the digital space allows things that are completely different, and we don't really use that. We should take this opportunity to promote other ways of organizing education, health etc.

Gérald Santucci added [via chat]: Due to climate change, wildfires, disappearance of many animal species, there will be more and more frequent sanitary crises in the future. However, the acceleration of change that has been witnessed in 2020 gives room for optimism. We could be capable of being more resilient, predictive, and ready to face such crises.

John Giusti shared [via chat]: GSMA has just completed a project as part of its AI for Impact work - with foreign aid funding from the UK and in partnership with mobile operators and national governments - using big data analytics to address specific challenges of the Covid crisis across 14 countries. The report will be made available on the Global Forum's website.

Sébastien Lévy commented [via chat]: The pandemic has accelerated the adoption of digital technologies. The broad adoption of remote processes, smart systems, and advances in virtual and augmented reality, led to a rise of what some people call "tele-everything".

Dr. Amir Johri, Senior Specialist, Ministry of Health of Oman, **presented examples demonstrating the role of digital enablers in coping with the pandemic in Oman**.

Digital technologies are being used in a very practical way by the Ministry of Health in Oman.

The Ministry of Health's *Tarassud* mobile app provides residents of the Sultanate of Oman, with transparent information on the spread of Covid-19, e.g., the number of cases and how the cases are increasing, the infection rates in the different parts of the country, but also information related to the vaccination campaign.

Moreover, the application informs about SOPs issued by different organizations and the Ministry of Health for both the general public and the Ministry of Health employees. It also updates on ministerial decrees, new laws and new information coming day-by-day.

Another application developed by the Ministry of Health in the effort to limit the spread of Covid-19 in Oman is *HMushrif*. Its objective is to ensure compliance of people who are being quarantined (both in institutional quarantine and home-based isolation) with the quarantine rules. A digital wristband is given to individuals put under quarantine to trace whether they are maintaining the quarantine or not.

Tarassud + is a powerful technological solution and extremely convenient. The application can be used while being in another country: people just download the app, they pay online, they know where their Covid-19 test can be done and they receive the results on the app, which then can be scanned at the airport.

These applications go hand in hand and digital technology was a great help in fighting the pandemic in Oman with regards to information, data collection, and analytics. It has been used responsibly, and the Ministry of Health is looking forward to a more widely use within the general population.

Ingrid Andersson stressed that people are aware of the change that happens in Oman. There is an increasing general acceptance of using digital tools. People don't really feel traced by the applications, but rather informed about Covid-19 and the spread of the virus, which has helped to keep the virus under control.

Sherif Aziz added that young people in Oman used additive technologies, like 3D printing, to produce mundane consumables, such as face shields etc. One group even produced a breathing machine. And regardless any market success, this group of youngsters innovated—or at least used technologies and localised the manufacturing to catch up with the crisis. Other young people developed applications to meet the changing societal needs.

It seems to be an opportune time to help local entrepreneurs localise manufacturing—not necessarily in the digital domain—but of very mundane consumables. Once you do this, innovation follows. For instance, there are a lot of people who can make masks. Start with this and then go further: Why not producing a mask that indicates when it is contaminated? One could use a specific patch indicating whether it is contaminated or not. You do not even need electronic sensors.

Paul Wormeli, Innovation Strategist, USA, **addressed the issue of cross-boundary information sharing principles**, emphasizing that a discussion on the impact of the pandemic couldn't be more timely: Last week, on March 30, the Science Academies of the G7 countries issued the statement: "The nations of the G-7 and beyond should work together to adopt principle-based governance systems for securing safe sharing and use of data for health emergencies; build and implement the operational systems, infrastructures, and technologies for implementing a principle-based and privacy preserving approach to equitable use of data for health emergencies".

It is a striking call that puts us all in the picture of deciding how technology can really be valuable for dealing with future pandemics. Over the last decades, we have established some fundamental truths about this. The problem of doing what the G7 Science Academies has suggested, is that we must understand some of these truths very carefully. We know that collaboration is the only way to make substantial improvements in the quality of government services. We also know that information sharing is essential to enable collaboration, but we don't do that very well on a global scale. Moreover, experience has shown that cultural impediments outweigh the technical issues in figuring out how we can share information with each other, and that the complexities increase exponentially as the scope of sharing increases.

To establish trust in governments, we have to balance the privacy policies and build the trust in the communities that support governments. And we must figure out how to balance privacy policies with interoperability and global data standards. And all this must be built on a system of governance—which we are not very good at on an international scale, especially in areas like information sharing.

It's a real challenge, but we are not starting from scratch: Back to the 1950s, the OECD created the "Fair Information Practices". These fundamental principles are at the heart of the U.S. Privacy Act of 1974, the EU General Data Protection Regulation and other laws, but they haven't been revisited and refined since. Nevertheless, some of these principals are still very important to the population, especially the principle of ensuring that data is used only for the purposes for which it was initially authorized.

These practices that were developed on an international basis need to be revisited and re-examined in today's world of technology. And we can go beyond that: We have the opportunity to develop principles of safeguarding data. Technology must be a means for protecting privacy and securing information, and we must find innovative and new ways to use technology to support the protection of individual privacy. In this context, standards are essential for supporting sharing innovation and safeguarding assets. People are more and more considering information as an asset that must be safeguarded. We have to come up with more international technology independent agreements governing privacy. One of the key difficulties, as well as opportunities, is that we need to have more effective safeguarding technologies that deal with the issues of federated identity and privilege management on a global scale. This is no simple matter, but there are already technologies that are very exiting in terms of how this could be done on a global scale.

What we need is the political consensus and the establishment of an international global will to deal with this—or, as Ronald Reagan put it in 1987: "Tear down this wall! "

Stéphane Grumbach wondered how the actual geopolitical setting, which is very conflictual with regards to cybersecurity, will impede or help accelerate international agreements.

Paul Wormeli explained that we must start with the policies that we would like to implement and then let the technologies enforce those policies. Cybersecurity is a very particular discipline that can be used to bring people together. In the U.S., the new Cyber Domain and the National Information Exchange Model are building standards on how to report and manage cyber incidents and come up with real time responses to cyber-attacks.

Cybercrime is an international phenomenon that must be dealt with on a global level. We have to figure out what we want to have accomplished and what the objectives are and then assign this to the technology.

Sylviane Toporkoff pointed to the fact that different countries have different perspectives and objectives. It might be difficult to reach consensus.

Paul Wormeli replied that the OECD demonstrated that it is possible. The UN Commission on Crime Prevention and Criminal Justice also has built an International Classification of Crime for Statistical Purposes and 170 countries have agreed to work together. It is possible, if we find the right format and organizational framework for doing so, but it requires good will and dialogue—it can't be done in a vacuum. It must be consensus based, not based on regulation.

Jeremy Millard added that we might need both, good will/consensus and good regulation that supports individual privacy but also tries to underpin those common rules.

Paul Wormeli agreed by stressing that the way to get there is the building of consensus. Regulation without involving the stakeholders tends to be nothing more than conflict.

Referring to the development of broad-based international consensus around governance questions, **Olin Wethington** added that such common principals reflect values. The challenge is that there is internationally a great disparity as to values that underpin governance questions. In terms of moving to common principles, it might be a good starting point to begin with the likeminded parties, which are essentially democratic oriented societies and do have an underlined sense of values in this area. Maybe a broader consensus then goes beyond what is possible, because, a heart, technology competition is a competition of values.

Gérald Santucci commented [via chat]: We need clear and strong principles for information sharing, especially regarding security and privacy. One first issue is the difference of vocabularies and semantics that exist among world nations, e.g., in the U.S. and EU there are slightly different meanings for "privacy". We need to set up a dialogue (the OECD could be a starting point, but we need to look beyond). Second, cooperation makes sense if it takes place over time, i.e., several years, not only when the principle meets temporary political interests.

Stéphane Grumbach pointed out [via chat]: The OECD is less than 20% of the world population and most of the largest countries, incl. the big actors in IT, are not part of it.

Gérald Santucci replied [via chat]: The OECD could be a starting point because of its potential reactiveness. But indeed, the dialogue must be spread over as many countries as possible, even if as we collectively suffer from a lack of common understanding on concepts, values, principles etc.

Topic 2: Disruptive Digital Technologies, Artificial Intelligence, IoT, 5G, Blockchain …

Gary Shapiro, President & CEO, CTA – Consumer Technology Association, USA, **set the scene with introductory remarks on Disruptive Technologies, AI, IoT, and 5G.**

With the pandemic, disruptive technologies have accelerated about 10 years. We have seen a digital transformation occur in 3 months, that normally would have taken several years. Imagine the pandemic had struck the world 10 or 20 years ago…

There is a crisis brewing in commercial real estate in major American cities and elsewhere, due to bankruptcies and the significant downsizing of companies. Studies show that even after the pandemic, employees do not want to return to the office 5 days a week, but they do not want to work from home all the time either. There is this need for social interaction. That is affecting how buildings are built, what a smart city will look like, the deployment of technologies, and the investments in commercial real estate. We are still seeing the ramifications of the pandemic.

Another noteworthy aspect is the perspective on regulation. When the pandemic struck the United States a year ago, a lot of the rules that governed business interactions were cast aside: The rule that you must be licensed in a state for medicine to practice, that you couldn't practice by telephone across borders or by telemedicine. The rules that a lot of restaurants and bars could not have takeout food or alcohol were all thrown away. The challenge now is to review old rules and make some of these changes permanent. The pandemic offers an opportunity to reshape our policy making in the long-term.

With the pandemic, there has been a proliferation of AI (and others) in this incredible multi-continent effort to develop a vaccine. AI is used to identify the best type of vaccines, predict the spread of the virus etc. Effective vaccines have been developed at record speed. However, to accelerate the deployment of vaccines, the rules for bringing drugs and vaccines to market had to be adapted. To move quickly, the U.S. Food and Drug Administration rules for vaccine validation were more than challenged.

We are also witnessing the use of technologies that we haven't seen before, such as product-delivery by drones—a non-human delivery system, with no risk of contamination. There has also been a change in investment with regards to autonomous vehicles, as they are considered as environmentally cleaner and reduce human contact.

At the G7 in Montreal in 2018, the discussions revolved around AI to be non-discriminatory, transparent and benefiting everyone. These aspects seemed important a few years ago. Today, 99% of AI applications have nothing to do with discrimination. Moreover, the desire for transparency or to make algorithms public is not at all an argument for the successful development and deployment of AI. There is a need to think about regulation in the context of countries and their values. For instance, China has successfully deployed contact tracing to contain the virus in a way like no other country in the world, especially considering the size of the country and the limited information at the beginning of the pandemic. There was a use of technology, contact tracing and surveillance, which by Western mores wouldn't have been acceptable, but the trade-off is that China has very little impact of the pandemic since the beginning. We must start thinking of these trade-offs.

We also must think about the values implemented in regulations and how we approach all these new technologies. A lot of the easy solutions are not easy, a one-size-fits-all approach is not a good approach. Rules need to consider the competing trade-offs and should not ignore the ability of smaller companies. You need values to succeed, but you also need to give companies the freedom to develop.

One-size-fits-all approaches are intentionally ambiguous and just let government regulators decide what may be politically feasible at their political time in history and what they consider to be right. It's a way to impose a geopolitical vision and values. Though, the points that should be of interest for any development are cost-benefit considerations, or the question whether it is positive for humanity in terms of environment, world hunger, human rights, security etc.

Some of the values we focus on, such as freedom of expression, or freedom of religion, may be less important in other parts of the world with more concrete needs related to food, housing, health etc. However, we need to think about the kind of society we want to leave for our children and grandchildren: We can have a perfectly orderly society where everyone is graded with little social interaction, or a more open world ensuring freedom for everyone.

Sherif Aziz added that many regulations benefit the big players. For instance, small companies have difficulties in complying with the many rules of the EU General Data Protection Regulation, unlike big players like Google or Facebook who can afford lawyers to make sure to be in line with the rules. However, AI is a powerful technology and needs to be regulated to avoid misuse, such as countries using AI to monitor the population.

Gary Shapiro agreed that the EU's GDPR has good intentions to protect privacy, but its impact on small businesses is underestimated. It is also a barrier to entry for new businesses and thus limits innovation. We need to reduce barriers to entry so that anyone with a good idea can have the opportunity to explore it.

It's the problem of one-size-fits-all approaches. Regulation needs to be smart and adapted to the situation. When human safety or lives are at issue, we accept to give up some privacy—this is what happened during the pandemic or what happens at airports all the time.

Michele Mosca commented [via chat]: We aren't looking for prescriptive regulations that might cause more harm than good (e.g., become quickly outdated and don't offer much security but prevent quick pivots needed to defend against new attacks). We really want "regulation" (in the broad sense) to enable more accurate "accounting" of cyber risk and its costs in the short and long term, and ""accountability" (so those benefiting from taking cyber risks are also responsible for the negative consequences down the road (not just the immediate consequences) … Otherwise, there is a moral hazard where people who didn't benefit from the risk-taking disproportionately pay the price).

In other words, smart regulation can accurately internalize real costs, hold the appropriate group accountable, so the natural "market forces" will take us to a better place.

Geneviève Fieux-Castagnet, SNCF – L'Éthic Groupe, France, **provided a European Perspective of Ethics for AI Systems**.

Ethics has a real double nature: Etymologically, ethos means the place of life, the habits and manners of people trying to live together in a city, a company etc. This very much depends on where you live, what you want to do and what your values are. But, according to Aristotle, ethics also allows to recognize us as members of humanity and of mankind as such. This dialectic seems very appropriate to the ethics for AI systems, too, as AI has no borders and is universally applicable.

AI has great applications in health, environment, security, mobility, transport, and the identification of human needs and desires, but at the same time, it puts human rights and fundamental freedoms at stake. Facial recognition, for instance, or tracing applications used to fight the pandemic, may also lead to surveillance and a loss of privacy.

To raise acceptance of AI and make it a competitive asset, various initiatives for trustworthy AI have been launched—at international, national, and corporate levels (e.g., OECD, UNESCO, EU, CNIL/France, CIFAR/Canada, Beijing AI Principles, but also SNCF, Google AI, or Apple).

Inspired by the European guidelines as well as its own code of conduct and values, SNCF follows the Ethics-by-Design approach for AI systems. From the very beginning of any AI project, a multidisciplinary governance team (project manager, developers, ethicists) maps the ethical risks of the project. Then, SNCF identifies remedies and risk mitigations. Monitoring the whole AI system during its entire lifetime is very important. The ideal would be to control the system throughout the whole supply chain.

Another important aspect of SNCF's Ethics-by-Design approach for AI systems, it to really ask the right questions. A catalogue of more than 100 questions is used at SNCF to map risks, among those: Which human rights or fundamental freedoms may be concerned? Is the use of AI essential or useful? Can we use a less invasive system? Can we use less data? Can we anonymise or pseudo-anonymize the personal data? Could we anticipate misuses or double uses? Can we explain the AI system? Is it safe, robust and resilient to attacks?

The identification of potential ethical dilemmas is another crucial aspect: Being France's national railway company, SNCF has developed a system to recognize the owners of lost luggage. The most efficient solution would have been to use facial-recognition technology. However, SNCF balanced between efficiency, invasion of privacy and the risk of surveillance, and therefore made the choice of developing a system based on clothes recognition, which is quite efficient, though probably less efficient than facial recognition.

AI systems are universal, and we should work on a system of international core values that the different stakeholders agree on. The Global Forum might be an opportunity to define a set of around 10 core values that could then be shared with the world.

Ingrid Andersson welcomed the suggestion to define a set of common value principles. This could be something to be worked on in the run-up to the Global Forum in Oman.

Stéphane Grumbach commented [via chat]: The lost luggage example has probably more to do with the fight against terrorism than with simple passengers. Thus, the privacy balance might be different.

Gérald Santucci told that the EU is about to release its regulation on AI. The regulation will clarify the EU's legal approach on transparency, ethics, privacy, and fairness related to AI, and pinpoint the applications deemed incompatible with EU fundamental rights.

Given the rapid change of technologies and the lack of international consensus about threats or risks, shouldn't we focus on soft law and co-regulation rather than hard legislation?

Geneviève Fieux-Castagnet pleaded for consensus building rather than regulation, except for very high-risk AI systems. Hard regulations should be applied when there are higher risks (e.g., in the area of security or transport) and soft law for other AI systems.

Michael Stankosky, Research Professor, George Washington University, USA, **introduced the Internet of Ideas.**

While the Internet is like a plumbing, the World Wide Web represents the richness of ideas and contents. We need to expand the conversation from the Internet of Things to the Internet of Ideas—and this change is already been happening on the Internet.

In March 2021, the Wall Street Journal published an article written by Jennifer Doudna (recipient of the 2020 Nobel Prize in Chemistry, together with Emmanuelle Charpentier, for their pioneering work on CRISPR genome editing). In this article, entitled "The Power of Mission-Driven Science", she describes how professors, researchers and engineers set aside their own projects to focus on how best to fight the pandemic. Once UC Berkeley had begun shutting down in March 2020 due to Covid-19, she immediately contacted her colleagues of around the world and they came up with a framework—as we know today, arriving to the vaccines in record breaking time. This example represents a great case study of the Internet of Ideas. We sometimes focus on things instead of focusing on the ideas behind the things.

The first creators of an Internet of Ideas in the history of mankind were probably at the House of Wisdom in Bagdad, Iraq, during the years 750 and 1250. The Caliphs decided to collect all the wisdom and ideas of the world without any discriminations. They collected books from the Byzantines, the Persians, the Indians, the Chinese, the Europeans, themselves… and they translated those books into Arabic. The translation was done by a team of polymaths. They wrote them down, and codified the content like Google today, they collaborated and came up with new knowledge and ideas.

Coherence is this idea of the power of mission driven science. If we ask the right questions, we may get the right answers, but most of the time we have the wrong questions. Take, for instance, the example of Amazon, which decided to build its new giant headquarter gathering 25 000 highly-skilled people in the Washington area close to the Pentagon. It is one of the most congested places on the planet, and people will blame transportation problems, although it is more an urban planning problem. We need to think broader and expand the conversation to a larger perspective.

To conclude with the 4 Cs Codification + Collaboration + Convergence + Coherence: Coherence is mission driven; Convergence refers to great minds thinking alike; Collaboration refers to the fact that no one is smarter than all of us; Codification refers to the possibility to "see further by standing on the shoulders of giants" (e.g., in the sense of what came out of the optics of what was done at the House of Bagdad).

Donald Davidson, Director of Cyber-SCRM, Synopsys, USA, **referred to the never-ending dilemma of the need to share vs. protect information in the context of cyber supply chain security.**

Just like there is an issue of sharing information and protecting information from a privacy perspective for individuals, that same challenge exists for corporations for their intellectual property, i.e., that secret source of a product. It is the never-ending dilemma of sharing and protecting data.

Each of our critical infrastructure sectors, e.g., agriculture and food, energy, financial services, industrial bases, transportation and communication networks, health etc., represents a system-of-systems ecosystem—meaning built-in in capabilities to this ecosystem that are composed of systems and sub-systems, components and sub-components. It is an aggregation of technologies, a technology stack, building that system capability. The components, subcomponents, systems and subsystems are enabled by microelectronics, integrated circuitry and software.

This involves security risks. Vulnerabilities exist in the entire system-acquisition supply chains and throughout the system-development. How to manage this inherent risk—the risk of the quality, safety, security of those components as they will perform in our ecosystems? Organizations need both centralized and decentralized capabilities to strengthen supply chain security and reduce the attack surface.

"The digital thread" concept provides supply chain visibility and an integrated view of a component's data across its lifetime for quantifiable assurance. It is a kind of disclosure of the details, the underlying components, the processes that are used during the entire process of building a hardware or software product. Some refer to that as the Software Bill of Materials or the Hardware Bill of Materials.

We need to share and protect data simultaneously. How can we use technologies like blockchain technologies, machine learning/ AI to grant row-based access to the supply chain (allowing to see only portions of the supply chain)? This is important, because it is the intellectual property that makes up a subsystem or a component and that makes a product unique. If you provide all of that data, any other company will be able to copy your product.

Emphasis has to be put on maximizing the commercial standards on this data collection, data sharing and data protection, as we go through the supply chain. Unique nationalist regulatory practices in this arena should be minimized. We have to think about how to gain visibility into the supply chains while at the same time protecting intellectual property.

Jeremy Millard reminded that Covid-19 lead to a supply side crisis. Supply chains have been disrupted, they have been shortened and diversified. There have been discussions on the concept of strategic autonomy and on-shoring supply chains.

Don Davidson replied that there is logic in that, but one can't on-shore everything. As the Fukushima earthquake or the recent volcanic eruption in Island have shown, there are natural disasters (and others), that impact classic logistic supply chains. What we are seeing right now is a little more emphasis—less on classic logistics (Covid has rather impacted classic logistics)—but on the cyber-aspects of confidentiality, integrity and availability. IT is becoming a more critical component of all those ecosystems we are seeing. I.e., how to protect trust,

confidence, safety, and quality of information, so that it is available in a critical time. National security systems or some of the most critical capabilities, such as the energy sector, might be on-shored in this respect.

Jean-Pierre Bienaimé referred to the EU initiative initiated in January 2020 to secure value chains and supply chains for 5G networks in the EU. The European Commission has published an EU Toolbox for 5G Security and is also conducting studies for the relocation of the purchasing and sensitive productions.

Concluding Remarks

Sylviane Toporkoff, together with the moderator, Ingrid Andersson, thanked the speakers and participants for the quality of their contributions. It was that kind of deep and inspiring discussions we need in times like this—discussions between knowledgeable people with different backgrounds and perspectives and mutual respect and appreciation for each other.

The moderator announced the two upcoming two webinars:

Global Forum Thematic Webinar III on June 9th, 2021

- Sustainable Smart, Cognitive Cities, Regions & Communities and Tech for Good
- Industry 4.0

Global Forum Thematic Webinar IV in September, 2021

- Health for All – Addressing preventative measures and medical interventions adopting new technologies
- Addressing Education and Learning in novel ways making use of Digital Solutions

Timing of both webinars: 1:30 pm to 3:00 pm Paris time / 7:30 am to 9:00 am Washington DC time / 9:30 pm to 11:00 pm Tokyo time.