17 December 2018
16h30-18h30

Salle 11
European Commission,
Berlaymont building, 200 rue de la Loi

Report from the High-Level Hearing

'Strategic Autonomy in the Digital Age'

European **Political Strategy** Centre

Purpose and Scope

Mastery of digital technologies has become an integral determinant of strategic autonomy, affecting today's cyber resilience as well as future capabilities. While digitalisation and ubiquitous connectivity expose nations to new threats and vulnerabilities, a weakening of the EU's industrial and technological base has led to an overreliance on non-EU components in the value chains of certain sectors. These developments give rise to growing concerns over security of supply and the integrity of critical information infrastructure. At the same time, the blurring of lines between military and civilian applications means that shortcomings in digital technologies might directly translate into security and defence challenges.

Faced with this changing paradigm, the EPSC chose to reflect on the question of how Europe can best protect its strategic interests in the digital age. On 17 December 2018, it hosted five leading international experts for a High-Level Hearing on 'Strategic Autonomy in the Digital Age.' During the Hearing, the experts were asked to address a set of predetermined questions with the knowledge that a full transcript of the Hearing would be published online.

The Hearing, moderated by **Ann Mettler**, Head of the EPSC, and **Lewin Schmitt**, Policy Analyst, convened:

- **Daniel Castro**, Vice-President, Information Technology and Innovation Foundation;
- **Lucas Kello**, Director of the Centre for Technology and Global Affairs;
- **Bridget Kenyon**, Global Chief Information Security Officer, Thales eSecurity;
- **Hosuk Lee-Makiyama**, Director, Centre for European International Political Economy;
- **Uku Särekanno**, Head of Cyber Security Branch, Estonian Information System Authority.

The full replies can be found in the transcript. As a 'teaser', the first section provides a key takeaway from each speaker. The quotes and bolded text have been selected by the European Political Strategy Centre.

Highlights from the Hearing

Daniel Castro

‘The EU therefore has a strong interest in addressing supply chain vulnerabilities for hardware and software, especially for those that could affect critical infrastructure. […] The EU should implement stronger measures to stop Chinese firms from acquiring European advanced technology companies. China’s indigenous innovation strategy is focused on unfair trade-distorting policies such as forced technology transfers, standards manipulation, subsidies, intellectual property theft and more.’

Lucas Kello

‘The globalisation of technology production cycles over the last few decades means that vital infrastructure increasingly relies on off-the-shelf and offshore manufacturers for other components which has introduced significant vulnerabilities into the supply chains. […] The most worrisome prospect is the scenario where foreign agents or private contractors preload software or hardware components with malware whether for attack or exploitative purposes. [Merging] this technological reality with geopolitics, sleeper payloads are remotely inserted and activated to achieve a preferred outcome in a future diplomatic or military crisis that is unfolding outside of cyberspace.’

Bridget Kenyon

‘The digital world is a reflection of all that is good and bad about every one of us. Organised crime exists there, espionage exists there. Pretty much every one of the technologies that we currently develop can be used for offensive and defensive capabilities, as well as simply for commerce. There are entire economies [in the Dark Web] which are based around the notion that everything can be turned to an offensive purpose.’

Hosuk Lee-Makiyama

‘Under the Chinese National Intelligence Law that was enacted this year, the Chinese government has actually the ability – under penal sanctions – to require Chinese citizens, organisations and even their equipment to collaborate with the Chinese national intelligence. And in that regard, I think it is evidently clear that the threat goes across the entire infrastructure, and what is really vulnerable is all the data.‘

Uku Särekanno

‘There is a growing pressure for the agencies like ours to start really blacklisting some of the products which are available at the internal market on the basis of the security concerns. And this is something which needs to be addressed in a more coordinated manner in Europe. […] The Commission should be very forceful when it comes to the enforcement of the existing legislation. Go for the infringement procedures, go for higher penalty fees. GDPR was very successful and understandable for entrepreneurs thanks to the fact that it had very high penalty fees foreseen. Try to raise the awareness, try to get kind of a mindset change there.’

Jump straight to ‘In a nutshell’ (p. 24)

Structure of the Hearing

During the Hearing, the experts were prompted to reply to six main questions, including a number of sub-questions, which had been shared with the speakers ahead of the event. The questions were drafted by the European Political Strategy Centre for the purpose of stimulating the discussion. The questions provide no indication as to the European Commission's views on the subjects discussed.

Here are the questions:

- **Question 1**: Please state your name and affiliation; please flag any potential conflict of interest (if you are providing consulting services to a client potentially affected by the European Commission actions in the digital or security domain, please state so). Please describe your background and your experience in dealing with topics related to digital technologies. You are welcome to briefly express your general views on the topic of 'Strategic Autonomy in the Digital Age'.

- **Question 2**: What are the most important trends that you observe in the development of digital technologies and how do you think they can affect Europe's ability to protect its strategic interests?

- **Question 3**: What supply-chain dependencies and vulnerabilities is Europe facing in the domain of digital technologies and how might they relate to the integrity of critical infrastructure? What are the ramifications on European strategic autonomy?

- **Question 4**: Which drivers are affecting Europe's present and future capabilities in digital technologies? To what extent are they defining Europe's level of strategic autonomy?

- **Question 5**: How should the EU respond to these developments in digital technologies? What would be effective and sensible measures and policy responses, both in the short- and in the long-term?

- **Question 6**: In a nutshell, your message to the European Commission: What should (or should not) be done to ensure an adequate level of European strategic autonomy in the digital age?

Full Transcript

Ann Mettler: Good afternoon. It is my pleasure to welcome you to this hearing on 'Strategic Autonomy in the Digital Age'. My name is Ann Mettler and I am the Head of the European Political Strategy Centre, which is the European Commission's in-house think tank. To my left I am joined by Lewin Schmitt. He is a Policy Analyst at the EPSC who is also responsible for organising today's hearing. We will ask the questions and rotate between us. Today's hearing is very much an effort to shed light on the various issues underpinning strategic autonomy in the digital age. And I am delighted to welcome such a high-level group of experts who will help us today to shed light on what is by all accounts an urgent emerging policy issue.

Before we start the hearing, let me briefly give you some instructions. The hearing will last for two hours, until 6:30 this evening. Each speaker will have a certain amount of time to address each question and speakers were provided with an extended list of questions ahead of this meeting. The hearing will be on the record and a full transcript of the hearing will be published on the EPSC website. And given the format I would appreciate if the audience would be in full listening mode, as no interaction with the speakers during the hearing will be allowed. However, there will be an opportunity for an exchange of views after the hearing is over. From 6:30 onwards, we will be serving refreshments outside of this room. Also, two more announcements: one minute before the time limit of an answer expires we will signal this by showing you an orange card. Once you have used the maximum time allotted to a question, you will be shown the red card. Once that is shown (the red card) we will ask you to conclude your remarks, and if you take a bit longer in one question, we ask you to reduce your time accordingly in another question. Also, we are rotating the order in which speakers are called on. So the order will be different for each question so that we do not always have the same person starting or concluding a question round.

Question 1: Introductions

Ann Mettler: We will now start the hearing. So, question one: **please state your name and affiliation, please flag any potential conflict of interest, please describe your background and your experience in dealing with topics related to digital technologies. You are welcome to briefly express your general views on the topic of 'Strategic Autonomy in the Digital Age'.** You have two minutes for this round and we start with Daniel Castro.

Daniel Castro: Good afternoon. My name is Daniel Castro and I am Vice-President of the Information Technology and Innovation Foundation. ITIF is a non-profit non-partisan think-tank whose mission is to formulate and promote public policies to advance technological innovation and productivity. I am also director of ITIF's Center for Data Innovation, an affiliated research center focused on the intersection of data technology and public policy. ITIF receives funding from a variety of sources including individuals, governments, foundations and the private sector. However, all of our work is conducted independently. I am not aware of any conflicts of interest regarding the subjects to be discussed here today. My research focuses on the policies that support digital innovation in both the public and private sector. I worked on a variety of policy issues at the Center for Data Innovation and ITIF such as copyright, privacy, security, accessibility, as well as technology specific issues, such as electronic IDs, drones and artificial intelligence, plus sectoral issues such as e-government, health IT and fintech. I have an undergraduate degree in foreign service from Georgetown University and a master's degree in information security, technology and management from Carnegie Mellon University. Prior to my position at ITIF, I worked as an analyst for the Government Accountability Office, where I audited security control of government agencies. And I was also a visiting scientist at the Software Engineering Institute. I appreciate the opportunity to join you here today to discuss how vulnerabilities related to digital technologies might affect Europe's ability to advance our strategic interests and potential policies to safeguard Europe's strategic autonomy. Given the vital nature of certain emerging technologies, especially artificial intelligence, to European interests, as well as new threats, especially from China, this is an important issue to explore and one in which greater transatlantic cooperation would be mutually beneficial. Thank you again for the opportunity.

Ann Mettler: Thank you so much. And next up is Lucas Kello, please.

Lucas Kello: Good afternoon, it is a pleasure to be here. My name is Lucas Kello. I am a senior lecturer in International Relations at the University of Oxford, where I also serve as the Director of the Centre for Technology and Global Affairs, as well as Co-Director of the University's Centre for Doctoral Training in Cybersecurity. By way of background, I think it is important to clarify that I am a political scientist primarily by training and there are not that many of us in political science, especially not in international relations, that focus our efforts on analysing cyber threats in the international system. But what this means is that the perspective that I adopt towards these problems is often quite a different one than that of a political scientist, or other sort of technical expert. And I think that is important to recognise, because this is very much an interdisciplinary and intersectional field of study, but we often use the same terms in very different ways. So, in terms of my broad views, I will state briefly that, and as my comments will make clear later, my sense is that **we are undergoing a technological revolution in strategic and security affairs, by which I mean the appearance of a new class of weapon, and I will call it a weapon, that is difficult to model and regulate even amongst conventional state actors, and which challenges some of the basic assumptions of strategic theory.**

Ann Mettler: Thank you so much. Next is Bridget Kenyon, please.

Bridget Kenyon: Hi, and thank you very much for inviting me to this event. My name is Bridget Kenyon and I am Global Chief Information Security Officer for Thales eSecurity, which is part of the Thales group of companies based out of France. My background started off with physics and drifted gently into IT. I then realised that information security was a) fascinating and b) incredibly challenging. So I have been working in that field since about the year 2000. One of my other main interests is development of international standards. I have been working with the International Organisation for Standardisation since about 2008, and I have edited a number of international standards relating to information security management systems.

Strategic autonomy and the information age is an incredibly vital concept – and it is something that is slippery. Every time you read it, the meaning changes, because the people who read it change. I think the most important thing about this event is the different groups and the different backgrounds present. I have a mixture of a cyber background and I have a mixture of human communications and understanding. So, I have got a masters in Physics with Astrophysics, but one of the best parts of that was learning approximations. Learning how to make assumptions. Learning how to understand risk. So, it is risk, it is people, and it is technology. Thank you.

Ann Mettler: Thank you very much. Next is Hosuk Lee-Makiyama, please.

Hosuk Lee-Makiyama: Thank you. My name is Hosuk Lee-Makiyama and I am the Director of European Centre for International Political Economy, ECIPE, which is an independent and non-profit think tank here in Brussels that primarily focuses its research on economic policy and international and global economic governance. One of the areas of my expertise is trade policy, which includes policy instruments, such as trade agreements, but also domestic sector regulation that has an interaction with the international trading systems. One of those sectoral aspects is the digital economy, which have been one of my focuses for the last decade. And starting from the WTO IT agreement, and onto the current multifaceted dimension of the digital economy we see today, a geographical interest of mine is, of course, East Asia. And that comes with the current structure of the global economic governance as such.

Ann Mettler: Thank you so much. And last is Uku Särekanno, please.

Uku Särekanno: Thank you very much and good afternoon to everyone. I am the Deputy Director-General of the Estonian Information System authority, which is a central agency responsible for the e-governance infrastructure. We are running the electronic identity management. We are responsible for the government network, where most of the agencies are connected, we are the internet service provider there. We are also responsible for the X-Road, which is one of the cornerstones of the e-governance system that we have. X-Road enables different databases to interact in an encrypted manner. And last but not least, we are responsible for the election security and cyber security in Estonia. Earlier I have mostly worked in the field of internal security and on track record there have been posted to European Commission last year working for the Task Force 50, in Brexit-related matters. All in all, my area of expertise is related to police cooperation and different IT matters related to that. Thank you.

Ann Mettler: Thank you so much. I will now hand over to Lewin Schmitt who will ask the second question.

Question 2: Trends affecting Europe's ability to protect its strategic interest

Lewin Schmitt: Thank you. We now move to the first core question. **What are the most important trends that you observe in the development of digital technologies and how do you think they can affect Europe's ability to protect its strategic interests?** We will start with Lucas Kello. You have four minutes.

Lucas Kello: This is a broad topic and the set of sub-questions was diverse. I want to draw attention, in the limited time that I have, to the question about the concerns over a blurring of lines between civilian and military capabilities, especially in the cyber context, which is my own area of expertise.

First, let me state that I agree with the premise of the question. **There is indeed an intensifying fusion – if not of civilian and military capabilities, then at least civilian and military concerns and activities.** And this fusion is evident to me in three basic ways. One is in the growing relevance and capacities of private threat actors. Previously, the main question of security policy for international relations thinkers was what actions of other sovereign states threaten vital national interests. This is, however, increasingly supplanted by the concern of how do forces operating outside and below the state structure imperil the nation, or in the case of today's discussion, the Union. So it is no longer the case that states and regional bodies have to contend exclusively or even primarily with threats presented by other states. It is increasingly the case that those direct threat actors have a different form, and they may include political activism, proxy actors that are not quite within the formal structures of other states, but work in some informal or formal way with them. Transnational terrorist groups, even your occasional lone wolf, are a cause for concern on the threat actor side.

Second, it is important to note the **growing role of private actors**, in particular, the large technology companies, **in the provision of European national security**. I cannot think of another time in history, and I thought extensively about this question, in which the private sector has been so important in the provision of national or, in this case, regional security. I think this problem manifests itself repeatedly in a number of incidents that we have observed. To take just one notable incident from across the Atlantic in 2015: there was a terrorist shooting in San Bernardino, California. The FBI presented Apple with a warrant to decrypt one of the terrorists' iPhones. Apple famously replied very publicly that it would not do so, because it believed that doing so would undermine the entire encryption environment of the iPhone. For a brief moment, you had a multinational company dictating to the most powerful government in the world which of two seemingly competing goods would prevail: the protection against terrorism or the protection of privacy rights. And the story concluded by the FBI turning, reportedly, to another private actor, an Israeli company, to decrypt the phone. That is not quite a victory for the broad question of the relationship between the state and the private actors because what it showed us is precisely the point that I am making, that states increasingly have to resort to private industry players in order to achieve their core security concerns.

Third, and last, it is important to note **the growing ability of private actors to precipitate an interstate crisis or to disturb one that is already under way**. I think we saw this quite clearly in the first significant international cyber incident, which was the distributed denial of service attacks that hit Estonia's computer infrastructure in the spring of 2007 and of which my colleague here will, I am sure, know a lot about. So I do not have time to elaborate on this point, but let me simply state that all future international crises in this domain will involve some risk, sometimes a significant risk, that private actors working in collusion, whether under the direction of any particular state, may intervene in the crisis and accelerate it in ways that the state parties involved neither desire nor anticipate.

Lewin Schmitt: Excellent, thank you. We now move on to Bridget Kenyon.

Bridget Kenyon: In terms of trends, one of the most interesting ones has been the enthusiasm with which organised crime has taken to technology. The creation of that, which is now known as the Dark Web, or the Deep Web, for the semi-illegal areas. It is not just a company. **This Dark Web is like an**

entire economy that runs in parallel to the legitimate one. You have situations where companies, organisations and individuals being infected with things like ransomware, as an example, not only have the opportunity to phone help desks to assist them in paying the ransom – help desks operated by the attackers! – but on top, have the 'opportunity' (again) to provide feedback and a star rating to the people who have stolen their money. This is a very structured environment. There are health plans in certain countries for people who are working for organisations running malware. This is very complex and very advanced. And it pays very well. So, you then compare that to the military. Let us look at the other angle; in a lot of organisations and a lot of countries, the military is hampered by the fact that they, frankly, do not pay very much. People who choose to work for the military are doing so out of an allegiance to their country. And yes, that might be a great way of identifying people who will stay loyal, but you are not necessarily going to get the most competent people, because competence does not correlate to ethics. Sorry. But that is how it is.

Personal versus work life. Here is another pair of things that are getting blurred. People's personal lives, where they store their data, what they do with it, they start to do that with their work information that they hold. That information can move into and out of the EU without anyone really understanding, including the organisations for whom they work. It is an ongoing problem, then. That is an aspect, in a way, of supply chain management, but it is also what they call… there is a lot of interesting phrases that have started to surface, but dark IT is another one – where you may have your official IT department, but you have your unofficial IT department known as Google, or for that matter, Amazon. It is the methods by which people bypass official techniques to obtain what they need, because in those official techniques the bureaucracy is too strong and it gets in their way. So, from the point of view of working within the EU versus working out of the EU, one can no longer tell the difference, and the problem is: it matters, because the laws change depending on where your data lives and where you are accessing it from.

Finally, I would say you have got a problem with… well, *we* have a problem, with the loss of agency by individuals. There is a feeling that everything is going too fast for the average person out there, and they do not really understand. At large, what you find is that sometimes governments do not understand the implications of their decisions. Most recently, the decision in Australia to essentially hamstring the concept of encryption. That is going to have global implications, and it was taken as a result of people being afraid. Anyway, thank you.

Lewin Schmitt: Thank you. Mr Hosuk Lee-Makiyama, thank you.

Hosuk Lee-Makiyama: I will primarily focus on digitalisation, as an economic phenomenon, and how it corresponds to the European policy response. And I would like to state that digitalisation is not a new [industrial] sector, but an economy-wide process. And it seems self-evident by now, but it is very important to point out.

And also, the digital dependency is already here. If you look at the share of inputs that comes from data, software and connectivity – that dependency actually already exceeds the importance of electricity or labour in sectors like services and machinery. In other words, it is not just a question about a pure economic interest of commercial viability in digital sectors. It is also, actually, about keeping the cost of inputs from digital sectors low, in order to maintain the competitiveness in other [traditional] sectors. And if you look at global trade, then **half of the global trade in services are already dependent on connectivity** – which means basically that the half trillion of EU exports will cease to exist if we are disconnected from the Internet or if certain economies decide to raise insurmountable trade barriers in disguise of cyber security. At the same time, the inter-economy dependency will increase.

Another phenomena that I will talk about is 5G which will enable, inevitably, delivery of industry 4.0. This will be the first network that is not designed for consumers but primarily designed to actually connect the industry. And we are now looking at 26 billion pieces of industrial equipment, transport equipment, and different kinds of industrial infrastructure going online, with a speed that is 200 times faster than the 4G, which basically allows for real time applications like industry 4.0. This means, clearly speaking, that we will not just store 'data' online – as we do today – like different kinds of blueprint, formulas, IPRs, documents or trade secrets. Entire companies will go online. That means control, settings, rather than just formulas and blueprint –actual control of equipment. And that means that the design departments sitting somewhere in the Single Market can be directly connected to a manufacturing plant somewhere in Southeast Asia, while the customer services may be sitting in some other parts of the world, which are all connected in real time. **That also means that the dividend of cyber espionage will increase, where you could steal a basic formula for a very commercially lucrative chemical in the past, you will be able to copy-paste the entire industrial organisation with two keystrokes if you have the right password.** This is very important to bear in mind, and also it has a clear impact on the competitiveness of our economy.

This will be further emphasised by AI which will be a productivity driver. For Europe, this is an important point, because if you look at the propensity of European competencies, it is not necessarily geared towards actually accessing [foreign] markets and AI will support re-industrialisation and export strategies of the European firms. But by diminishing the return of investment in AI by different types of regulations, we are basically crippling our own economic competitiveness compared to other economies. That is one key point.

I would also add that, **in our institutional setup, the EU is not necessarily equipped to deal with these challenges simply because the common commercial policy (CCP) is not necessarily geared towards supporting non-economic objectives. There are clear security threats that are geo-economical or strategic which cannot be addressed through CCP**, which would be possible in a normal economy. Also, our **industrial policy in the Member States have been basically rendered ineffective due to the fact that the digitalisation has changed the parameters of how the economy operates.** And as a final point, maybe I should also add that, **at the EU level, we do not necessarily have the international policy and the treaty instruments that are available to the other major powers, in terms of creating either a strategic deterrent, or capacity to address the cyber security issue.**

Lewin Schmitt: Thank you. And Mr Särekanno.

Uku Särekanno: Thank you very much. Two particularly concerning trends from the cybersecurity point of view that we would like to bring out first is related to the impact, the net negative impact, that we have seen that the cyberspace has had on the democratic processes lately over the last few years: the meddling with elections, the asymmetric approach that some state actors have taken to influence democratic countries. This is one of the trends we see that is going to last for many years and it is particularly going to be a challenge for many Western countries. Second issue is related to supply chain and the fact that if you are running a e-government system, a system which is based on many components, then the mere fact today is that you are not able to control all of the components because they are either produced somewhere else – they might have the best certificates, you might have the best agreements in place, but the mere fact is that there is a risk that you might face a big vulnerability which you are not simply aware of.

Starting with the first one, the democratic process: this is a particularly concerning matter in the longer run. Our president Toomas Hendrik Ilves has pointed out several times that **a like-minded coalition is needed from Western countries who would be defending democratic values and would be able to stand up and would be willing to demonstrate that there are measures that will be taken in case of intervention or meddling with elections or democratic processes.** This kind of attribution issue is still something which is very premature and we are very far from perfect and I think we have a very long way to go there. In order to do something practical, Estonia together with 20 other European countries drafted up 100-page long recommendations on how to secure your elections, how to do the technical steps in order to ensure that nobody would be hacking any of your systems during the election process. This is a list of recommendations that we published in August. And this goes for any electoral system. It is not about advocating our own Internet-based voting system. There are practical steps what to do but the biggest concern probably is related to the false news, fake news and the misuse of social media platforms for creating cleavages and then misunderstanding in the society.

The second issue, **supply chain, is probably one of the biggest challenges** for us. If you ask **from the cybersecurity point of view**, I mean, 'what is the key concern for Estonia?' I would say that this is supply chain. Last year we were facing a very serious crisis. Basically, our e-government system is running on two core elements. One is the X-Road. As I explained earlier, this is the platform which enables different databases to connect. And the second one is electronic identity management, is basically ID cards: mobile

ID and smart ID that we have as well available. What we were facing was a situation where the ID cards that we had available and roughly 800000 Estonians using them actively. There was a malfunctioning chip on the card and the chip was produced in line with the best practices, the best standards. We had the best agreements in place. We had already a long-term practice on how to produce the cards, how to pick the partner, et cetera et cetera. But in the end of the day, this malfunction emerged with millions of chips globally. These chips were also used in many European countries. There were, I think, five or six different EU countries which were facing a similar problem. There were several companies who had the same problem. And from the contractual point of view, our agency did not even have any direct contractual relationship with the chip producer. So what I want to say here is that this changed completely our understanding on the e-governance system that we are running. We felt really that we might have the best agreements, the best certified products, but **we simply cannot control all the components of the system. And that is why the early warning and rapid information exchange about the vulnerabilities is absolutely necessary here.**

Lewin Schmitt: Thank you. And Mr Castro, please.

Daniel Castro: There are a number of important technology trends that I think will affect Europe's ability to protect its strategic interest. First consider connectivity: continued growth in broadband connectivity, including with emerging 5G wireless networks, has resulted in more devices coming online and staying online with data linked and synced though the cloud. And **this change has created important new stakeholders in critical digital infrastructure such as the wireless equipment providers and the cloud service providers, many of which are foreign firms.**

Second, there are growing numbers of connected devices – collectively known as the Internet of Things – with significant amounts of computing power. This trend has significantly expanded the potential vectors for cyber-attacks, as the number of intelligent endpoints on the network multiplies. **Connected devices are both new targets and, if compromised, they can become part of adversarial botnets.** The risk from these devices is exacerbated by the fact that many of these systems will be directly connected to 5G networks. Unlike many of today's devices which reside behind the firewall and, thus, they will be more vulnerable to cyber threats.

Third, artificial intelligence or AI is creating massive disruption across virtually every industry as firms use the technology to increase automation. **The rise of AI creates new vulnerabilities as attackers learn how to exploit automated systems and also new methods of attack. Hackers wield AI for malicious purposes such as using it to create deep fakes to spread misinformation online.** Notably, AI is also a tool for those defending against cyber-attacks and could be a useful countermeasure especially given an undersized cybersecurity workforce. However, to date at least this capability has been underdeveloped.

Lastly, blockchain – which still is in its early stages – has the potential to weaken traditional forms of institutional power and control by decentralising trust in various systems used today such as identity systems, financial systems and security systems. These changes may in some cases undermine traditional forms of state control, limiting the ability of government to protect its national interests.

Now the EU has the potential to thrive in the development and use of many of these technologies especially if it focuses on applying these technologies to specific sectors. For example, European start-ups which make use of AI and blockchain technologies are already attracting considerable amounts of investment. In the first half of 2018, fintechs in Europe saw an estimated €23 billion in investment compared to about €12 billion in the United States and €14 billion in Asia. EU efforts to build a Digital Single Market support many of these technologies as they all benefit from scale.

Successfully developing digital technologies generally requires relatively high fixed costs, particularly R&D and software engineering cost. The more customers a company can amortize these costs over, the more successful the company can become, and it can reinvest profits in the next generation of products and services. This is why having access to a European market with harmonised rules can help firms grow. However, the EU also needs not just the same rules. It also needs the right rules and here is where the EU may be falling behind with the GDPR. For example, the Centre for Data Innovation – my think tank – has published a report earlier this year that analysed how different provisions of the GDPR would negatively impact the adoption and use of AI by European firms. Similarly, others have looked at how certain provisions of the GDPR such as the right to deletion have created serious headaches for those trying to use blockchain systems which establish immutable records. So while the EU has made strong commitments to technologies like AI, including through R&D funding and proposals from most Member States to develop their own national strategies, it still lags.

With AI, in particular, China has developed a more ambitious strategy than the EU. China's State Council issued a development plan for AI in July 2017. The plan's goal is for China to be equal to countries leading in AI by 2020. Then over the subsequent five years, China will focus on developing breakthroughs in areas of AI that will be 'a key impetus for economic transformation'. Finally, by 2030 China intends to be the world's premier artificial intelligence innovation centre to support the development plan that China is also preparing: a multi-billion-dollar investment initiative to promote AI start-ups, academic research and ambitious moon-shot projects. By most accounts, these efforts are working. For example, Boston Consulting Group just reported that 85 percent of businesses in China have either adopted AI or are piloting the technology versus 49 percent when they looked at France and Germany. Finally, it is worth noting the virtually all of these major technology trends involve dual-use technology that has both civilian and military applications. This means the countries will be hard pressed to restrict advances made for military purposes because it will restrict commercial opportunities, but also that success in civilian applications of the technology can translate into military advantages. So this is all the more reason why the EU should ensure its strategy is on par with or surpasses that of China.

Question 3: Supply-chain dependencies and vulnerabilities in critical infrastructure

Ann Mettler: Thank you so much. We now proceed to core question two, to the identification of critical dependencies and vulnerabilities. So the question goes: **what supply chain dependencies and vulnerabilities is Europe facing in the domain of digital technologies and how might they relate to the integrity of critical infrastructure. What are the ramifications on European strategic autonomy?** And you have six minutes for your answer. And we start with Bridget Kenyon please.

Bridget Kenyon: Thank you. I do not know if people have heard of the allegations from Bloomberg relating to the Super Micro issue that really brought into an immediate highlight the problem with supply chain. If you have a piece of technology which is used across the world in a million different ways, and a single allegation comes to light about that technology, trust is lost. The organisation manufacturing that technology may stop existing, may not be able to continue in operation, or equally, where perhaps a nation state is alleged to have had a part to play in a key piece of anti-malware technology and suddenly no other nation state will touch it with a barge pole. Basically, **everything is connected at this time. If you want to look at vulnerabilities and dependencies, so many organisations, so many activities are connected to each other now that as soon as you see one change, one issue in one area, many other sectors and many other organisations will be directly or indirectly impacted.**

So, obvious things: if you look at Maslow's Hierarchy of Needs, you start with things like 'people need shelter', 'they need food', 'they need communications', then – going up – things like entertainment. You look at that and you think about what digital technology does, and it underpins every single one of our hierarchy of needs. So we talk about critical national infrastructure, that I believe is taken from that same hierarchy: you can affect communications, you can affect every single part of our supply chain. Not necessarily by interrupting it, but by altering it: you double what someone wants, you halve what someone's asking for, you change stock prices. That could affect pretty much everything we have.

Can we be independently acting within the global economy? We cannot shut ourselves off. So that is in itself a vulnerability, that necessity.

Another major controversy we have across the globe at this time is what we call basic housekeeping: the common-sense stuff that in fact turns out not to be common sense. 'Everybody patches their computer', 'everybody uses antivirus'. 'Everybody has a firewall that by default does not allow things in'. It allows people out—people can go talk to things on the Internet but things on the Internet by default cannot get into your company. I have been what they call a Qualified Security Assessor, so that is someone who goes around and talks about how people handle payment card data, and when you look at how large organisations, including financial organisations—I shall not name them but they are large—are handling card data, it is shocking. The very basic concepts of getting rid of insecure systems or protecting them is missing, because the driver is always towards the next big thing. 'We will do some upgrades, but we will never get rid of our old equipment.' How many people have heard the word 'legacy' in relation to IT? If you substitute the word 'legacy' for 'insecure' or 'possibly vulnerable', that is slightly more accurate. Every legacy thing you have is a hole for someone to get in through, unless you have taken extra measures and spent extra money to protect yourself.

Foreign investment always comes with strings attached. Always, because if the foreign investment is from a nation state, that nation state has its own interests to protect – as do we. The question is: 'how do your nation's politics align with the nation that intends to invest in you?' If you take it to that level, it is not really about technology in the end, it is about politics. Hence my colleagues on this panel.

Another interesting thing to bear in mind is that nation states stockpile vulnerabilities. They keep them to one side for when they might need them. So that when you do have that Apple device falling into your hands you can say 'right, well, down the back of the sofa I happen to have stashed a neat way of getting into this Apple device' and then perhaps that wonderful list of vulnerabilities gets into the wrong hands, and maybe it is published on the Internet. Things then happen as we all know. And finally, on the dark web, vulnerabilities have a price. You can invest in vulnerabilities. I suspect they may even have their own stock price at some point. It is about cause and effect: quite often the cause is insufficient housekeeping, but the effect is sufficiently badly correlated to the cause from the point of view of the organisations in question, that steps are not taken until after an incident has occurred.

Ann Mettler: Thank you so much. Next is Hosuk Lee-Makiyama please.

Hosuk Lee-Makiyama: Maybe I should say at the onset that pursuing full autonomy across the supply chain and to completely remove the supply chain dependency of other countries and other economies it is not feasible and it is not in the interest of Europe. We have a fragmented supply chain where Europe participates across all the steps of the value chain. Also, supply chain security does not necessarily mean supply chain isolation in terms of autonomy. I question whether full economic independence is even compatible with Europe's vision of global governance and the ultimate endgame: Our goal is to maintain an open economy while our economic influence is diminishing.

However, **we should not be naive about the risks we are facing**. And I would like to focus on the question of data. Europe has pursued a persistent and consistent strategy to protect personal information on behalf of its citizens, but one blind spot we have still is the commercial data. This means that **although we have all the legal remedies and the institutions required to protect personal information, this is not necessarily the case in terms of commercial data**. Not all valuable information is personal. Also not all paths to protecting data are legal, which means that we cannot necessarily just regulate in order to protect the data in our economy. This is of course very clear.

As I highlighted before in my opening statement about the commercial risks as more and more information is moved online, this has a direct impact on employment. We are looking at almost 290,000 jobs being at risk from different types of cyber theft. I will also add that particular risk is the coercion of various governments. Many of the so-called APT groups we know are state sponsored. And of course, if you are looking at every attack across the supply chains that we have seen in the past, very few entities actually have the resources and the persistence to undertake such an operation in order to damage Europe's strategic advantages as we have seen.

And I will highlight two examples. One is actually the United States, where there is the US Cloud Act that has actually an ability to coerce corporations to collaborate with its government. However, the United States does not necessarily pose a strategic threat or at least not from an existential point of view. Also, there are effective legal remedies and effective methods [in the US] to basically scale back on potential abuse. The other example we have seen in the past year is China. **Under the Chinese National Intelligence Law that was enacted this year, the Chinese government has actually the ability – under penal sanctions – to require Chinese citizens, organisations and even their equipment to collaborate with the Chinese national intelligence**. And in that regard, I think it is evidently clear that the threat goes across the entire infrastructure, and what is really vulnerable is all the data.

Ann Mettler: Thank you so much. Next is Mr Särekanno please.

Uku Särekanno: Yes, thank you very much. The question is about the identification of critical dependencies and I would put it in a way as the head of our R&D department did last year. The biggest challenge that he described in the field of cyber security, he named it monoculture. He meant with that basic dependence that not only the public institutions but also the private sector has from very few software and hardware solutions. I mean if you look around and take for example Estonia. I would say that 90 percent of the market is using Windows or Microsoft products. If you take the processors that are used in different hardware equipment, there is a very short list of producers there. And what we have seen throughout the last few years and earlier as well, but it has become a particular issue this year, are the vulnerabilities that tend to emerge with the technology that we are all using in a very widespread manner. So the SPECTRE case for example, which was linked to Intel processors. This had a huge impact particularly in a global scale.

Coming back to the matter that I mentioned earlier: what we learned from the last year, basically, we had a supply chain issue with our ID cards. We had a theoretical case where someone with pretty good knowledge, with a good expertise, misusing the malfunctioning chip and the cryptographic algorithm or the combination of two and with enough calculation power could falsify your electronic identity, enter with your identity to some bank or even vote on elections etc. So there was this theoretical case. We managed to avoid any incidents, we managed to take things under control. But we had only very bad scenarios on the table. I mean, one option was that we would simply say that 800,000 cards that we have at our disposal or which are used by our citizens will be simply not meant for using any electronics services anymore, which did not seem to be a good option because there were so many services depending on the authentication of digital signatures provided by the card. And the second option was that we would switch to another cryptographic algorithm, update the software on 800,000 cards and fix the problem. That is the road that we took. It took several months to fix the problem. In the end of the day, we had around 500,000 cards updated with the new software, providing safe and sound and secure authentication. And in the case of 300,000 cards we had to simply close the access to electronic services.

So what did we learn from that? One option would be to simply blame the companies who are producing chips and saying that it is a supply chain issue, that we would need to opt for any other provider etc. The key lesson for us was that you have to diversify the technology. If we are using for authentication ID cards, we need something next to that as well. We had already mobile ID. Now we have smart ID as well. But when it comes to the ID card, we should use different chips with different technological solutions when it comes to encryption etc.

So I also tend to agree that the best way out from the state of play is not trade barriers, but to advise different governments to diversify the technology that they are using and the options that they are using. And last not least, I see on a daily basis that **there is a growing pressure for the agencies like ours to start really blacklisting some of the products which are available at the internal market on the basis of the security concerns.** And this is something which **needs to be addressed in a more coordinated manner in Europe.** I am not going to enter into detail on the discussions over the 5G networks, but that is one example. And if you take account, for example, of the Estonian market, we have three operators. They are all Scandinavian companies. So it is clear that whatever decision is made, this needs to be coordinated at least among the three countries who are operating or where the companies are operating their technology. So yes, that is probably a road where some EU regulation or at least some coordination is needed in the future. Thank you.

Ann Mettler: Thank you very much. Next is Mr Castro please.

Daniel Castro: The combined forces of digitalisation and globalisation have created supply chain vulnerabilities for virtually every firm. There are three main threats that the EU should address.

First, there is the problem of **Chinese acquisition of EU firms.** In 2017, Chinese foreign direct investment in the EU reached €30 billion up from €700 million nine years before. Some of the motivation for this investment is commercial. A good portion is supported by Chinese state-owned enterprises. Moreover, it is likely that **much of that investment is guided and supported by the Chinese government, specifically targeting sectors that are strategically important for EU strategic**

interests including national security and economic leadership.

As China ramps up its indigenous innovation strategy, designed to slow down foreign companies in China and enable Chinese-owned firms to take global market share in advanced industries, there is **a growing tech trend for China to have its firms acquire foreign technology companies – including in the EU – in order to acquire much needed knowhow, compress innovation cycles and develop indigenous supply chains for particular sectors.** At the same time, China restricts EU investments in many sectors and treats foreign companies – including European firms – under different rules. Many foreign firms consistently report being treated unfairly compared to their domestic counterparts. As such, policymakers should be under no illusion that many of these acquisitions are in the service of an overarching strategy to accomplish one important goal: take European technology capabilities so the Chinese firms can gain global market share at the expense of their foreign competitors.

Second, the EU should be concerned about the threat that, as **China seeks to displace European technology firms** with its 'Made In China' policies, it will undercut the competitiveness of EU firms. Of particular concern would be those **firms with dual-use technologies**, as a decline in European competitiveness among these firms **would weaken the European defence industrial base.**

Third, there is a **risk of vulnerabilities in the software and hardware EU firms acquire from abroad.** Many of the major data breaches over the past few years, including Cambridge Analytica, can be traced back to vulnerabilities in suppliers. Vendors' or partners' vulnerabilities such as the Heartbleed bug can affect millions of commercial systems and software flaws in major platforms such as the Magento e-commerce platform can put terabytes of business and consumer data at risk. Given the prevalence of open source software in particular, it is unfortunate that there is relatively little government support for securing this code – even though open source projects are often integrated into many commercial and government systems. Moreover, reports from earlier this year – while contested – suggests that **attacks on hardware suppliers to major technology companies remain an area of interest for nation states who wish to introduce vulnerabilities in the systems and networks of foreign adversaries.**

The EU therefore has a strong interest in addressing supply chain vulnerabilities for hardware and software, especially for those that could affect critical infrastructure. China in particular should be a prime concern for the EU, as law enforcement officials have identified Chinese hackers as being responsible for a number of major cyber-attacks, including the recent Marriott data breach. Moreover, Chinese hackers steal not only intellectual property for state-sponsored corporate espionage but also military secrets. In the United States, for example, a recent report found that Chinese hackers have been engaged in widespread targeting of government contractors both large and small, as well as universities, to steal highly sensitive classified information about advanced military technology from the U.S. Navy, including everything from ship maintenance data to missile plans, prompting the Navy to launch a top-to-bottom review of cybersecurity threats.

One important reason **hardware and software vulnerabilities are so prevalent is because most countries have a fundamentally broken approach to cybersecurity policy.** Most countries want to be able to defend themselves against digital attacks while successfully executing these same attacks on foreign adversaries. This policy is unrealistic for today's global networks. There is a substantial amount of shared technology and thus shared vulnerabilities. Cyber superiority is a misguided policy goal – when one system is susceptible to an attack all users foreign and domestic are threatened. It is this contradiction that is at the heart of most cybersecurity policies. This philosophy of relative security rather than absolute security is the reason that law enforcement intelligence agencies typically oppose measures that would improve security for everyone such as expanding the use of end-to-end encryption or disclosing new vulnerabilities immediately because they hope to exploit these weaknesses against others. Unfortunately, the main result of this policy is that all systems remain insecure. Until we **create a new cybersecurity policy that prioritises defensive capabilities and resiliency over offensive strength** and advocates for this new vision among global allies, the fundamental cybersecurity challenges will remain unchanged.

Ann Mettler: Thank you. Lukas Kello, please.

Lucas Kello: I think the organisers of this hearing are right to draw special attention to supply chain risks. And that is what I will focus my next comments on. **The globalisation of technology production cycles over the last few decades means that vital infrastructure increasingly relies on off-the-shelf and offshore manufacturers for other components which has introduced significant vulnerabilities into the supply chains**. This is an important point when one looks at the historical context of globalisation, which is qualitatively different to economic interdependence in the sense that today it is not just about growing commercial flows across national frontiers but also about the globalisation of the production cycles themselves, in terms of the manufacturing of our technological products.

The resulting vulnerabilities present major challenges to infrastructure defenders. They amplify the situation that I have written about quite extensively: offense superiority, which means that there are many advantages that possessors of advanced weaponised code enjoy when faced with actors who must defend against its use. The most worrisome prospect I think is the scenario where foreign agents or private contractors preload software or hardware components with malware whether for attack or exploitative purposes. We have a number of instances on the record, notable ones, where this concern has been expressed. Apple security experts for example are worried that their company's cloud services like cloud have been compromised by vendors who installed a backdoor for government spying purposes. In 2012, the US House of Representatives Intelligence Committee warned that machine parts supplied by Huawei, the Chinese company founded by no less than by a former officer of the People's Liberation Army, could be used to exfiltrate data from US government machines and in 2009 – closer to home – Britain's Joint Intelligence Committee warned that Chinese cyber components of British telecoms and phone network could be preloaded with zero day vulnerabilities, giving Beijing the ability to interrupt the country's power and food supplies.

A more specific scenario that I find worrisome and which merges this technological reality with geopolitics is one where sleeper payloads are remotely inserted and activated to achieve a preferred outcome in a future diplomatic or military crisis that is unfolding outside of cyberspace. Indeed, I cannot conceive of a future crisis involving the world's large powers – for instance over maritime sovereignty in East Asia or over the situation the intensifying conflict in Ukraine – that does not involve at least periodic – perhaps sometimes mysterious – crashes of vital infrastructure as a form of punishment, signaling or even just inadvertent escalation in the crisis. Now it is important to note that supply chain risks were also a concern of Western adversaries. Chinese government for example recently banned the use of Windows 8 operating system in some of its computer infrastructure out of similar concerns of supply chain risks. What this means, then, is that supply chain security is an area of common concern among nations, which makes up room for limited international agreement.

Supply chain risks magnify the basic problem that all technologically advanced nations face, and it is to purloin a phrase from former British Prime Minister Stanley Baldwin speaking in the 1930s about strategic air bombers: **Malware will always get through.** This situation represents a major reversal of the classical security paradigm, the traditional objective of which was to keep your adversary outside of your prized home terrain and if your adversaries penetrate the perimeter well then you – according to this classical paradigm – have failed. **Today, it has to be the starting assumption of security policy, that at least your most sophisticated adversaries, your advanced persistent threats, are already living inside your vital infrastructures without you even knowing it, possibly until it is too late to neutralise the threat.**

And I have to my left a CISO and I know that if someone in that capacity were to go to his or her boss and say 'I promise that the computer systems were perfectly secure, no malware has been detected in the systems', that individual probably does not deserve his or her job right. Because as I said, the starting message should be: 'we have not detected any advance threats yet, but we have to assume that at least those high-end players are already on our systems.' This has a very important implication for security thinking, which I think this group of individuals has to consider very seriously: the main challenge of infrastructural protection in face of these growing supply chain risks is not how to keep your enemy outside of your systems but rather how to diminish their ability to inflict harm from within.

Question 4: Drivers affecting Europe's present and future capabilities in digital technologies

Lewin Schmitt: Thank you. We now move to core question three: **Which drivers are affecting Europe's present and future capabilities and digital technologies? To what extent are they defining Europe's level of strategic autonomy?** You will have four minutes for this question, and we start with Hosuk Lee-Makiyama, please.

Hosuk Lee-Makiyama: Thank you. Europe has enjoyed a small window of manufacturing services supremacy in the last century, while much of the rest of the world – and in particular Asian economies – has been underperforming due to artificial policy constraints, poor governance or misallocation of resources. From that perspective, it is perhaps only a question of time where the competitors will catch up with Europe. The fundamental problem is perhaps that the certain economies – emerging economies – are catching up faster than Europe transitioning to higher value added. And it is due to not just natural competitiveness and restoration of market economy, but also the state-administered market economy as well as mercantilist policies are helping them on the way. This is something that has been prevalent not just with the recent emergence of China, but also – at least the mercantilist aspect – has been a dominant feature in the rise of other emerging economies as well.

But the fact is that Europe's loss of relative competitiveness is not just due to the fact of other economies engaging in state-market fusion. It is also due to the fact that **European industrial policy engaged in a policy gamble in the last 20, 30 years that has not come out too well.** And one of the fallouts of this is that **we cannot reward basic R&D or commercialisation and innovation to the extent that will make it actually profitable in our own home market.** From that point of view, FDI coming into Europe is not – at least for an economist – a problem in itself. We need foreign investments when our own companies refuse to invest in our economy and prefer to invest overseas, it is welcomed. You can even argue that if emerging actors, including state actors, actually come through the front door rather than the back door to actually pay for our R&D – at least for an economist – it is not necessarily a problem. Well, as long as the back door is closed, and as long as there is a transparency about who we are engaged in business with. This transparency is an important part, because transparency is not always the norm outside of Europe.

The other problem is due to the fact that the **forced technology transfer** that we see is mostly happening through investment and foreign equity caps (FECs) that are still enforced in much of the rest of the world. Joint-venture requirements are basically instruments to not pay for our R&D, which is the underlying problem.

And aside from FECs and joint-venture requirements, we also have an increasing **proliferation of cybersecurity barriers**, and these are raised both in the West as well as in the East. But notably, if you look at the recent events around 5G, we can see that there have been raised by countries who do not have domestic industries to protect. These are not your typical run-of-the-mill protectionism. And when it comes to what we see in the emerging economies, and especially in China, they [cybersecurity barriers] seem very disproportionate, demanding very hefty and wide safety margins. They are not just an expression of the risks they are exposed to – actual existential risks – but also the fact that they are very decentralised entities where regulations are necessarily enforced fully within their own economies.

Lewin Schmitt: Thank you. Mr Särekanno, please.

Uku Särekanno: Thank you very much. Well, three key drivers affecting the capabilities in digital technologies in Europe – skills, investments, and regulation. First, the skills and know-how: we are running a very heavy competition at the moment with the rest of the planet and we have so many different growing economies stepping in. And we see how China is growing, how focused their policy has been in developing different – especially cybersecurity-related – products. We see the global competition between US and China when it comes through to new technologies so I mean skills is probably one of the key challenges which each and every head of agency or person in my position will tell you that this is one of the key drivers or key challenges that we have.

Second element is the investments: **we see a lot of foreign investments coming in, affecting the critical infrastructure that we are using.** How to draw the line? Where do we need foreign investments and where do we need to be a bit more careful? I think this needs a bit longer reflection.

Thirdly, last not least, there is the question of regulation. We should be aiming in the internal market for a regulation where we have set **standards for some core elements of the e-governance system and this should not be the minimum common denominator** that we are able to agree. But this should be following the best standards and practices available. And I would say that this is a particular concern from the Estonian point of view. For example when it comes to electronic identity management, the different cryptographic methods used there, we are afraid that the EU regulation might define too low standards. We might lose the high level of security that we have gained at the moment if we go for the lowest common denominator. This is not what we are aiming at. And this is something that we need to understand in Europe as well. If you go for regulation, we need to really focus on the key cornerstones of the critical infrastructure where the regulation might provide some added value and there we should not stick to that lowest common denominator.

Lewin Schmitt: Thank you, and Mr Castro.

Daniel Castro: Thank you. There have been many important steps for the past 30 years in digital technologies. After the 1980s with the emergence of the personal computer, the 1990s and the early 2000s saw the rise of the Internet economy, as firms used new global networks to innovate with new business models and supply chains. **Over the last decade or so, the world moved into the data economy as firms increasingly used data to drive improvements in products and services with analytics.**

Europe's success in the Internet economy and the data economy has been somewhat muted especially compared to the United States. There are many reasons explaining why more European firms did not capture significant global market positions, including a **lack of understanding about how new ecosystem based business models worked** – thus, for example, the reason Apple started gaining market share from Nokia was by creating this unique customer experience that is based on the product-service combination – **a focus on mechanical engineering at the expense of software capabilities**, and finally the **lack of an integrated EU market that would have enabled firms to gain scale quickly** – something that is at the core of success for digital firms. Notably now some EU Member States such as Denmark, Finland and the Netherlands have done much better than others in the data economy.

The Center for Data Innovation analysed a broad set of metrics across three key areas of the data economy to understand some of these national differences. We looked at three areas. First, data including the availability of usable data and the effectiveness of government policies promoting the supply and use of data. For example, some countries have made more progress in data sharing in healthcare with government Open Data. Second, the technology, particularly the availability and use of key digital infrastructure and systems, such as the Internet of Things, e-government services and broadband. And finally, people and firms, such as the use of data driven technologies by firms and the prevalence of digital skills and training opportunities.

All of the metrics vary significantly by country but the EU will need to effectively address all of these factors to succeed economically as well as reduce its exposure of the cyber threats. For example, the EU is more vulnerable to cyber-attacks if it lacks workers with the necessary skills and training to identify and respond to threats. **The EU will also need to address the uneven technology adoption across Member States. Attackers go after the weakest links and in some cases, these weakest links will be within Europe.**

The global economy is changing once again with the rise of the algorithmic economy in which firms' success directly correlates with their ability to automate processes using AI. To prepare for the shift you should consider two broad goals. **First, the EU should focus on the industries and technologies of the future, not of the recent past.** As hockey star Wayne Gretzky famously said, 'skate to where the puck is going, not to where it has been.' As the past shows, the shift in digital technologies has led to different firms and nations seizing a competitive advantage. This trend will likely continue. In other words, the winners of the algorithmic economy, where new technologies like blockchain, robotics, 5G, and the

Internet of Things will be paramount, are not preordained, and current competitive advantages do not assure a future advantage. Remember that IBM's leadership in mainframes did not translate into the PC era, and Microsoft's leadership in PCs did not translate into leadership in social media. As such, Europe should focus on winning global market shares in these emerging technologies.

Second, the EU should build on existing core competencies. Many of the emerging technologies involve cyber physical systems: the combination of digital technologies with physical objects and services such as smart manufacturing, smart agriculture, smart cities and smart grids, not to mention autonomous vehicles. This **opportunity plays well to Europe's considerable strengths in engineering but will also require Europe to improve and expand upon its software capabilities.** Thank you.

Lewin Schmitt: Thank you. Lukas Kello.

Lukas Kello: On the question of drivers affecting Europe's capabilities in digital technologies and this broad theme. I want to draw attention again to geopolitical and other forces underlying cyber threats. So the record of harmful incidents reveals that the most significant events – you take your pick, Estonia, Georgia, Stuxnet, Moon, Sony Pictures – occurred at the confluence of geopolitics and technological vulnerability. And let us recall that international cyber conflict originated in Europe, in Estonia in the spring of 2007. Before then, it would have been quite rare for international relations specialists or a national security planner to devote much time or attention to cyber threat. Cybersecurity was not really a thing in the public perception but it certainly exploded up the national international security agenda thereafter. And it was that particular incident. I mean, any student of the history and politics of the continent will understand the non-technological origins of the conflict very well.

So two main factors will ensure that Europe remains a central theatre in the intensification of cyber conflict. The first concerns what one might call the demand side of cyber threats, by which I mean the opportunities to cause harm technologically. **Europe's inordinate and increasing reliance on computer technology across the economy, society and government creates new vulnerabilities that opportunistic adversaries can and will exploit.** Estonia was easily targeted because of the prevalence of cyberspace in its core governmental and financial functions. Perhaps no other European nation or society relies so heavily on computer technology. And Europe has broadly followed the digital path of Estonia and perhaps no other continent relies so heavily for its security and prosperity on the protection of vital computer infrastructure. So all signs indicate – especially in the context of the ambitious Digital Single Market – that the demand side of cyber threats, the opportunities to cause harm with zeros and ones will continue to grow in this part of the world.

A second set of factors are involved, what I call the supply side, and this concerns the world outside of cyberspace: **the convergence of cyberspace and forces beyond it that provide the motives for adversaries to exploit Europe's state of digital dependence for some political strategic or ideological purpose**. So dependence will either remain the same or – as I am suggesting – will grow larger, but the underlying motives will vary. These growing geopolitical and ideological tensions in the region and beyond supply motives for states and other actors to carry out harmful cyber activity, and here we must emphasize – even if there is no time to elaborate – the salience of one major adversary on our geopolitical doorstep which is Russia, a country that increasingly uses cyberspace to disrupt the internal affairs of Western liberal nations.

Let me emphasise that the Russian threat has acquired a new emphasis in the ways that it has. The Russians have seized damaging political information which they have then revealed about a popular public official organisation which they then revealed in a way that was timed specifically to influence and possibly alter the shape of a nation's foreign policy or even government as a form of activity which I refer to, and others, as Kompromat, which is a very interesting and worrisome evolution in the use of intelligence gathering in the cyber domain. **It used to be that if you stole our secret information you wanted to not reveal that fact to the victim because that would defeat the purpose of intelligence gathering. Increasingly what we are seeing is that the Russians are stealing information in order precisely to make it public in a way that produces a disruptive political impact in order to reduce the foreign policy assertiveness and internal political cohesion of its**

Western liberal adversaries, including of course many member states of the European Union.

Lewin Schmitt: Thank you. Mrs Kenyon, please.

Bridget Kenyon: So the question of whether the EU is lagging behind other economies, behind other countries in its capabilities and digital technologies. You have to bear in mind the amount of willpower that each government is putting behind the need to innovate, and the need to apply the brakes when the innovation actually can cause more harm than good. In the US, for example there is the Silicon Valley, a long established hub of digital transformation. In Israel, as another example, one of the major political goals is to become a global cyber power and citizens (who mostly have to do national service) are given the opportunity to be part of the cyber military. The very first PhD in cyber security was available from Israel, to give another example. Israel is not the only area where the military and academia are very closely related. **In China, for example, there is a strong relationship between the government and academia, which can direct activities outside their borders such that academics from China may be sponsored to go and liaise with other countries.** And as one of my colleagues just said: as long as this is happening transparently – great. If it is not so obvious what the purpose is and what the intentions are of the collaboration, that's when it gets very dangerous and very interesting.

A major driver is the need to catch up with everyone else. I think everyone in this room feels that there is a need to innovate, a need to progress and to be the best in digital transformation and as I have said a second ago, **that tends to come at the expense of risk management**. So, for example, a company will run an industrial control system, will decide that they are going to innovate – they are going to bring in whatever they need to make things faster and more exciting. They are going to put their aircraft on standard Ethernet, rather than something special that was designed for the aircraft in the first place. In the enthusiasm to move to commercial off-the-shelf products, the suitability of those products for the use cases are not always fully considered, such that you end up with systems that have significant security issues being brought into operation in environments that they were never intended for. Thus, you have a situation where someone can (for example) connect the flight entertainment system to the flaps on an aircraft. That is something we all would rather prefer it did not happen. But it is a distinct possibility, once you start running everything through exactly the same technology.

Finally, **a metatrend, again it is the sharing and blending of personal and work worlds**. The lack of understanding of the implications of decisions, the enthusiasm for new things and almost a fear of the future: what is going to happen? Let us try and make it. Let us try and get there first, so that when we get there we can make our position solid. And when everybody else gets there, we are safe against them. Encryption is a good example, actually: **one way to break encryption is to steal the data that has been encrypted and wait.** All you have to do is wait **for someone to find a flaw in the algorithm**; for someone, for example, **to get a better quantum computer, which can break encryption very quickly**. A lot of security is just about time. You add time to security – you can often break it.

Question 5: Recommendations for EU policy responses

Ann Mettler: Thank you so much. We now come to a core question four, pertaining to recommendations for the EU. **How should the EU respond to these developments in digital technologies? What would be effective and sensible measures and policy responses both in the short and in the long term?** You have four minutes in this round and we start with Mr Särekanno please.

Uku Särekanno: Thank you. To say what we are lacking, I think we have to look what we have at our disposal first. And if you look around it is not so bad. I mean we have the NIS directive in place since this year. We have the GDPR framework in place. We have the different capabilities in the field of cyber security developed over the years in all Member States. You might of course question how capable are they and whether they are comparable, but they exist. We have a toolbox for cyber-attacks which was developed during the Estonian presidency of the EU, which is basically on essence about the attribution and how the EU should respond in case of a cyber-attack. And we have now the compendium on how to secure elections. So there is a long list of legal and political documents available.

The key issue at the moment to my view is enforcement. And I think here the Commission and the EU institutions should play their part to make it really meaningful, to make it really understandable, for example for the essential service providers and different member states that these papers need to be followed and these recommendations need to be addressed. And as regards the toolbox for example, It is just paper and it might rest as a paper but we were speaking about this meddling with the elections, how we have seen state actors intervening in different democratic processes and so forth. I mean this is something which needs to be put in practice and brought to the attention of ministers. During our presidency, we tried to organise an exercise on the matter and then the ministers of defence were playing through different scenarios on cyber security matters. But I think this needs a proper follow up because the problem with the attribution at the moment in Europe is that we are not very convincing.

Secondly, what we have seen internally is that **more awareness-raising is needed**, especially at the level of top managers. It is a very serious problem, because not all managers are aware about the cyber security risks. Basically the learning is coming through incidents. We see incidents on a weekly basis and it is not ok that we are so reactive. So what we have done back home is that we have offered with the EU and government funding penetration tests for some of the essential service providers in order to raise the awareness of the management board. We have set up sensors in collaboration with key essential service providers to reflect their network traffic for analyses to our CERT-EE for providing an extra shield of protection for them. We have tried to raise the awareness on the average users introducing different platforms of digital testing and so forth just to improve the overall ecosystem. So I think we have a very solid legal framework in place. In fact, the NIS directive reflects very well what was developed over the years in Estonia: different capabilities, different practices, different standards that need to be developed not only in Estonia. Many other countries are following this as well. So I think now is essential really to focus on the enforcement and also awareness raising.

Ann Mettler: Thank you very much. Next is Mr Castro please.

Daniel Castro: There are three broad sets of measures the EU should take to respond to the concerns we have been discussing. **First, the EU should implement stronger measures to stop Chinese firms from acquiring European advanced technology companies. China's indigenous innovation strategy is focused on unfair trade-distorting policies such as forced technology transfers, standards manipulation, subsidies, intellectual property theft and more. At its core, China's strategy is designed to replace foreign technology leaders with Chinese owned ones.** Naturally, not all Chinese investment is strategic or related to China's indigenous innovation strategy. Some of it particularly some of the greenfield investments can even offer a net positive for the European economy. But while some Chinese foreign direct investment is neutral or positive, a significant share is harmful because it is not based on market forces or commercial interests but rather guided by a Chinese state that is intimately involved in directly shaping economic outcomes well beyond what any other major economy does. **The EU should therefore continue to welcome Chinese purchases of European made products and services but set limits on buying European companies. The European framework for screening foreign direct investments is a good step in that direction. The EU should also demand a level playing field and insist on mutual access to Chinese firms and fair treatment for EU firms operating in China.**

Second, the EU will be best placed to address these concerns if it leads the technology rather than merely regulating the technology. Put differently if the US and the EU collectively lose the global AI race to China then both will be heavily dependent on Chinese companies for this technology and have little recourse to deal with strategic threats particularly as it relates to the use of AI and related technologies in our defence systems. To accomplish this the EU needs to be more aggressively pursuing a digital agenda especially in major technology areas discussed such as AI, IoT, blockchain and others to invest in R&D, improve the workforce, and increase data availability.

Third, **the EU should take steps to improve cybersecurity.** The NIS Directive establishes some cybersecurity compliance reporting requirements for organisations. But these are unlikely to substantially reduce threats to the supply chain overall because as I noted earlier attackers only need to find the weakest link. It will be more important to pursue EU wide policies that promote collective cybersecurity such as disclosing known vulnerabilities and establishing bug bounty programs for open source code and other critical systems as well as pushing back on attempts by other nations such as Australia to restrict end-to-end encryption.

The EU should also work with allies to develop strong collective countermeasures for companies that knowingly introduce hidden vulnerabilities into the supply chain such as at the behest of a foreign government. The problem right now is that companies are getting banned from certain markets sometimes publicly and sometimes discreetly because of potential ties to foreign governments. Recent examples of this include Huawei and ZTE because of potential ties to the Chinese government, Kaspersky Labs because of potential ties to the Russian government. US firms too have also been excluded for similar reasons. It is unclear if these bans are warranted. In every case and companies that are banned have little recourse, as it is hard to prove a negative, is hard to prove the absence of a vulnerability. To have a well-functioning global market for digital technologies rather than a segmented market, countries should come together and establish a collective agreement to allow companies that meet certain requirements to have access to their markets. How these countries can collectively agree that if a company's products or services are later discovered to have back doors or other intentional security vulnerabilities they will all implement a ban on that company's products for a set period of time. The goal is to set a high enough penalty that the costs of cheating would be too high to bear. Thank you.

Ann Mettler: Thank you very much. Mr Kello, please.

Lucas Kello: So Europe, and the West more broadly, face a glaring punishment problem when it comes to major cyber actions, and this is where I will focus my prescriptive recommendations. So **there is a persistent failure in this part of the world to counter the adversary's preferred form of aggression, which involves non-violent, but highly damaging attacks against economic infrastructures and the integrity of democratic institutions. I categorise this activity as acts of un-peace.**

This is a concept I develop in my recent book 'The Virtual weapon and international order' and un-peace denotes 'activity that is not war like in the traditional sense of a large scale physical destruction and loss of life', but nor is it peaceful rivalry in the sense that it is broadly tolerable and accepted. Repeatedly, Western leaders warn about the gravity of technological threats. Estonian officials in 2007 compared the Internet attacks to terrorist activities. Britain's MI6 warned that the manipulation of social media by foreign powers in the lead up to the Brexit referendum represented a fundamental threat to the nation's sovereignty. And, yet, **repeatedly Western nations fail to deter or punish the offenders.** In both cases that I just referenced there was little or no national or regional punishment. At least no major punishment, which is observable in the public domain. It is of course possible that some form of court activity took place.

Our response has largely focused on the preferred methods of Western diplomacy, which is the fostering of laws and norms of international conduct. European diplomats stress the importance of existing international law and institutions to curtail hostile conduct. They emphasise the value of forums such as the UN Group of Governmental Experts, which is tasked with adapting existing legal conventions such as the UN Charter principles to the regulation of cyber and prevention of hostile cyber actions. They stress the real reasonableness of prevailing norms, a term that one hears repeatedly in the chancelleries of Europe, as if the transgressors in Moscow, Beijing and Pyongyang had failed for all these years to grasp the norms and self-evident validity. The problem is that the main reason for Western inaction concerns precisely the limitations of the current legal and normative framework. It is not fit for the ends that policy-makers ascribe to it, because it does not provide clear grounds to seriously punish actions that fall short of the recognisable criteria of war. But they would witness a true act of cyber war which meets the criteria of traditional war, that in fact will be, perhaps somewhat paradoxically, an easy situation to deal with, because we will simply revert to our conventional response doctrines and manuals.

So contrary to common opinion, **contemporary problems of cybersecurity are not primarily normative or legal but rather doctrinal. The challenge is in figuring out how to punish hostile action which the traditions of law and security strategy do not ordinarily recognise as punishable.** Russian strategies commonly refer to the language of war, for example, some of the terms are next generation of non-linear warfare, but it is precisely because their actions are not overtly warlike that they appeal so much to the Russians. The Russians and other major adversaries understand two things doctrinally better than we do. First, they understand the severe economic, political, social harm that one can cause with computer technology. Secondly, and more importantly, they understand that so long as the harmful activity – no matter how harmful it is – does not rise to a recognisable level, warlike level, of physical destruction and loss of life, they will largely get away with it.

So I think that**, as a major regional and global power, Europe has enormous resources, economic, diplomatic, increasingly even military, at its disposal, to craft a more effective punishment strategy, if only we could correctly grasp the changing nature of threats and the roots of our failure to punishment.** And this regional response, I think, should be a central concern of our efforts to craft and implement strategic autonomy. And it could give institutional expression to Toomas Hendrik for a coalition of like-minded states in addressing evolving threats. And as I emphasise, in punishing them more effectively and credibly.

Ann Mettler: Thank you so much. Mrs Kenyon, please.

Bridget Kenyon: In terms of recommendations, let us look at something that has had a very significant effect – and we have all seen it – and that is the **General Data Protection Regulation.** Every organisation that I have interacted with knows what it is. They have all made changes, and those changes have not just been in the organisations themselves, it is been in communications with their customers and also with their supply chain. The organisation that I am in right now, Thales eSecurity, has been approached by customers saying 'We have completely new ways that we now deal with our supply chain, here are new things that we require from you'. And it is driven by GDPR, but it extends beyond that. Quite often, the customer will say 'Yes, I know this data that is included in our GDPR work, it is not personal data, but we have decided we want to treat it as carefully as we would personal data'. **So one recommendation might be to look at ways in which we could use that same approach that has worked for GDPR for intellectual property, as one of my colleagues has already mentioned.**

Another recommendation, going in a slightly different direction, is to bear in mind the impact of the choice of words. So GDPR, 'General Data Protection Regulation' – people can get to grips with that. As soon as you use the word 'cyber', at least half of your audience – maybe even 80 percent of your audience – will switch off, because what it means is technology. It means 'IT will save us'. And the first thing that happens is that everything that has 'cyber' in it goes to the IT department, and the CEO never wants to see it again. My recommendation is: **think carefully about the choice of wording for any policies or legislation, because it will determine which part of the organisation pays any attention** to what you have written.

Another item, obviously, funding. I do not know how many people have heard: 'Well, it is really important and I fully understand how absolutely vital it is, but I really just do not have the time'. Or: 'We are not going to be able to do that because we have got some really important things on today'. The message is, simply, it is not important, because we have chosen to deprioritise it. And when you want to see what a priority is, you look at where the budget is going. You look at where the funding is going. If you are not funding it, that is the message. It tells people it does not matter.

Supply chain security, I mentioned that briefly. We cannot stuff the genie back into the bottle – or to move slightly sideways: we have learned how to make fire. We cannot unlearn it. **We cannot disconnect our supply chain or say that it only exists within one country.** And, for that matter, we should not. We should not be trying to retreat into little country-limited caves, because we will lose the advantages that we have in the different capabilities that exist, within different organisations, within different countries. For that matter, if you are a multinational dividing yourself up like that, is at the very least painful.

And then the NIS directive was, well, I knew it existed, but pretty much nobody else I talked to does. GDPR completely eclipsed it, and it is just something to bear in mind. It is timing. It is what comes into play at the same time as something else.

And finally, get the basics right. **GDPR had a wonderful phrase – 'Secure by Design'.** Grab that and reuse it. It is powerful. It is something that is designed to be fit for purpose; and by fit for purpose, I mean adequately secure. Not completely. Adequately. Then you know exactly what you can do with it, and what you should not do with it. If you define what the appropriate purposes are for something that you are building, everybody knows what it is good for. That could be a basis for policy. Thank you.

Ann Mettler: Thank you so much. And the last one in this round, Mr Lee-Makiyama. Please.

Hosuk Lee-Makiyama: I start by saying, investment screening, which has been the focus of much of the attention recently, is not a silver bullet. Especially if you are an economy who fails to apply export control adequately and uniformly. Why buy a company when you just simply can buy the goods from one supplier in Europe? **It [investment screening] merely serves a trade friction and an irritant and a leverage to force our counterparties to come to the negotiation table to get rid of their own investment restrictions. For that purpose, it is helpful, but it has nothing to do with supply chain security.**

On the question of certification, I would say that it is a helpful first step, but once again it is not a silver bullet and, at worst, it is a regulatory red tape that basically just increased the competitiveness gap with countries or supplier from countries who do not apply similar certification scheme in their own home economies. In other words, it might actually erode our competitiveness through our own market barriers. And if you speak to the cybersecurity experts, **certification will not mitigate the real risk of backdoors**, especially [the risk] from resourceful players. I think these examples [of mitigating measures] are based on a misconception that there is something called trust towards vendors or certain vendors are trustworthy and some are not. Sure, there are trustworthy vendors from every country in the world. And there are probably not so trustworthy vendors from the same countries. But this question, **whether a certain vendor is trustworthy or not, is completely irrelevant: It is a question about extraterritorial, extrajudicial dependencies that vendors have or [or may develop] simply because they are forced to follow the legislation of their home jurisdiction.**

In other words, this is not a question about trust to vendors**: It is a question about trust between governments and between executives.** This basically means that there is nothing that a vendor can do – either to us, or to other governments – to prove that they are completely trustworthy. [Or for us to prove] they are not trustworthy. And this creates the policy space for disproportionate legislation.

Yet, I think that we can say that all governments spy. And, therefore, international treaties or 'no-spy agreements'... well, their effectiveness have been questioned. And in effect the only thing that seemed to have had an effect is active cyber defence as a deterrent, which means that **these [supply chain] risks will persist, and which also means that governments – not just here in Europe, but also others – will respond by creating 'Supply Chain Security Areas' between trusted government that can provide legal and constitutional safeguards** that I mentioned in the previous question.

And also within that framework, between a group of allied countries, you can have free market rules and open data access and apply a holistic approach to data protection. And this is also one of the reasons I think that – although the 5G was developed amongst the global group of industry stakeholders – I believe **6G will be developed within a closed group of like-minded countries.**

So, as a final point, aside from basic re-territorialisation or regionalisation [of supply chains] into plurilateral groups of like-minded countries that form 'secure areas' of supply chains, I think it is also important to address some of the multilateral questions. I addressed already the question of export control, but also the importance to address national security exception in trade – and especially in the context of WTO – that are currently being abused by the disproportionate safety margins that has been demanded by certain countries in the face of their risks. Ssimply because the standards will be set by the most disproportionate country, as all the other economies will be forced to respond in kind. Thank you.

Question 6: In a nutshell – message to the European Commission

Lewin Schmitt: Thank you. As the hearing comes to a close it is time for final remarks and key takeaways. So you will have two minutes each to address the last question which goes: **In a nutshell, your message to the European Commission. What should or should not be done to ensure an adequate level of European strategic autonomy in the digital age?** And we will start with Daniel Castro.

Daniel Castro: Thank you. To protect strategic European interests, **the EU should pursue policies to address supply chain vulnerabilities, in particular, targeted threats from Chinese foreign direct investment and unaddressed and emerging cybersecurity risks.** All of these issues pose daunting challenges to EU strategic autonomy.

However, strategic autonomy for the EU should not be defined as regional autonomy. The goal should not be to replicate the 'Made in China' policy with a similar 'Made In Europe' policy. Instead**, the goal should be to establish a coalition of interdependent liberal democracies that share the EU's goals of reducing vulnerabilities in the global supply chain of digital technologies.** By working together for this common end, the EU can create an environment that enables strategic autonomy. This does not mean that the EU should not aggressively pursue technological leadership in the emerging algorithmic economy. **There is a global race for AI and the countries that emerge as the winners will be able to shape the development of this technology and mitigate many potential threats.**

It is worth noting that **the EU-US disputes over policy issues like privacy, anti-trust, and taxes, undermine the strategic cooperation we should be pursuing on cybersecurity, digital, trade and foreign investment.** One particular risk is that some of the EU's regulatory efforts around competition and data protection may serve mostly to weaken US technology companies, paving the way for Chinese counterparts to take over. This outcome would only weaken the EU's strategic autonomy. I will close on that final remark. And thank you again for the opportunity to be here today.

Lucas Kello: In my concluding remarks, I want to elaborate a bit further on my preceding comments about the failure to punish. The roots of Western policy paralysis in the face of growing technological aggression lie I think in a failure to grasp the changing tides of modern conflict. Traditionally, war has been the principal force of change in international affairs. **In the 21st century, however, the relevance of war to geopolitical competition and transformation has diminished**. War no longer alters history or moves geopolitics as it did even in the recent past. In fact, when major war does occur, it mainly preserves international order rather than challenging it, as in NATO's air campaign against Libya's Gadhafi and the case to stop its violent suppression of civilian disturbances. So relative to the rich history of warfighting in the past century, the most distinctive feature of modern conflict is the silencing of guns among the large powers. That is because the consequences of major war would be economically and politically ruinous, as leaders around the world understand this quite well. But also, as I have been stating, because **new technologies make it possible for nations to achieve some of the core political and other objectives of war without firing a single gun**. My sense is that Western policy makers fail to grasp the central truth, or at least fail to grasp it as well as our main adversary, which is that much of modern interstate rivalry fits neither the destructive criteria of war nor the acceptable boundaries of peaceful competition. It is, as I labelled it, un-peaceful activity. And yet the rigid thinking about war and peace prevails Western security policy, operates strictly within the bounds of these two binary notions. As I discussed earlier, this policy response approach has produced severely flawed results, which manifest primarily in the form of policy and **institutional paralysis in the face of growing technological aggression**. In closing, in case there is any doubt about the tone of my comments today, let me end on a pessimistic note.

The quandaries of strategy and doctrine will be long lasting. We are still very much in the first generation of international and national security level cyber threats. We certainly will not be the last to grapple with its persistent problems in thinking about these issues. It will be, I predict, a permanent technological revolution, in the way that perhaps no other era of technological change has witnessed. **The underlying technologies will continue to evolve far more rapidly than our development**

of security doctrines to address them. With the advent, for example, of artificial intelligence and with the growing expansion of the Internet of Things. Moreover, our reliance on the technologies will also become more complex and difficult for security thinkers to grasp. **So as a result, our policy axioms and understandings will continue to lag behind rapidly changing technological realities**. What this means, I think, for our efforts looking into the future, is that our main investment should be where our adversaries invest, which is in the development, precisely, of new modes of thinking, principles of offense and defence, in order to not, as I suggested, close the gap in thinking, but rather to ensure that we do not fall behind as quickly.

Lewin Schmitt: Thank you and Miss Kenyon is next, please.

Bridget Kenyon: We are getting an increasingly hostile environment on the Internet. Once upon a time it was a couple of people in a pair of universities communicating with each other, I think it was CERN. And now everybody is there. **The digital world is a reflection of all that is good and bad about every one of us. Organised crime exists there**, espionage exists there. And yet it is strangely unregulated on a global scale. We have what is, in essence, very similar to the American Wild West. And we are using it for everything, including managing medical devices, such as pacemakers. You combine these two facts together and you come up with a future that looks a little bit exciting, for want of a better word, because we are not at the end of the innovations.

We can see many things on the horizon – there are other things we cannot see, and the obvious ones, AI, which have been mentioned and quantum computing. These are two edged swords, and when it comes to picking up a sword like that, the question is not can I wield it, but should I, and on whom. Pretty much **every one of our technologies that we currently develop can be used for offensive and defensive capabilities, as well as simply for commerce**, and there are entire economies, as I mentioned, which are based around the notion that everything can be turned to an offensive purpose. I would not recommend the EU go that way. But using technology and knowing what the implications are, designing things to be secure, ab initio, these are the principles that we should apply as a community of like-minded and sane countries. Finally, I would mention the need to make sure that lawmakers are fully aware of the implications of their decisions. And I would thank you very much for inviting me to this event.

Lewin Schmitt: Thank you, and Mr Lee-Makiyama, please.

Hosuk Lee-Makiyama: Thank you. The EU is exposed. Our expertise in light manufacturing is where the emerging economies usually challenge us. If you look at 'Made In China 2025', in the 10 sectors that China has singled out [for prioritisation], Europe is the leading actor in all these 10 sectors. Digitalisation is affecting these manufacturing sectors in a larger scale. Currently we do not have a strategy in order to transition into higher value-added. Also, we do not necessarily have means to scale back the national security measures that are on the rise. Which basically means that we will be organising our supply chains into, not necessary regional, but plurilateral alliances. But the question is, whether these alliances can sustain the large over-capacities in the EU economies.

In other words, the eco-sphere must be much bigger than Europe in order to sustain our employment, as well as our future capabilities. And on that note, I will maybe point out that **if the Single Market is going to be sustainable, and if the EU is continuing to be a relevant factor, we need to be agile and think beyond the silos that we have created around commercial policy and foreign policy.** In other words, the response of digitalisation needs to be holistic, and approach to data – and the risks posed to our data – must be holistic. Thank you.

Lewin Schmitt: Thank you. And Mr Särekanno, please.

Uku Särekanno: Thank you very much. To conclude, first recommendation: focus on the enforcement of existing legal framework, do it in a meaningful and convincing manner and try to raise the awareness. The 2007 cyber-attacks in Tallinn were nothing else than awareness raising exercise. We had cybersecurity capabilities in place already earlier, we had standards in place earlier, we had CERT in place earlier. Our financial sector was following the best recommendations. It demonstrated that we had the resilience, we could cope with the attacks at that time, but it was kind of a change of the mindset for politicians because they recognise somehow that it is not a science fiction anymore. It has a real impact on the ground, on the way average citizens are living their lives, and it has state security interest involved. Awareness raising is a key issue here.

I think the Commission should be very forceful when it comes to the enforcement of the existing legislation. Go for the infringement procedures, go for higher penalty fees. GDPR was very successful and was very understandable for entrepreneurs thanks to the fact that it had very high penalty fees foreseen. But the NIS Directive is something which has a bit disappeared from the mindset of an average CEO. Try to raise the awareness, try to get kind of a mindset change there.

Secondly, **coordinate blacklisting when it comes to the national security issues.** It is not a technical matter, it is a political matter, and technicians really do not like this topic. They recognise that **each and every technology has some vulnerabilities,** but you have to understand the context, who is using these vulnerabilities, when they are using these vulnerabilities, whether there is a meaningful suspicion that this will be used by some state actor or non-state actor. This is a political decision, and we have internal market, we have regulations for all the products that we have, we have certificates for the products which are circulating on the market. If we would like to skip something out of the market, it is a political decision, and more coordination is needed there.

And last not least, **work together with NATO and try to build a meaningful deterrence**. That goes along with the recommendations that we gave when it comes to the like-minded coalition and when it comes to the cyber-attacks orchestrated by third countries and meddling with the elections. So we would really have to work out some sort of a meaningful counter measures that would be convincing to any third country not to intervene in the democratic process. Thank you.

Ann Mettler: Thank you very much. I just want to warmly thank all of you for sharing your insights and your expertise with us today. This concludes this hearing and we will still be serving refreshments outside the room. I assume many of my colleagues will want to have a word with you, so now is an opportunity to do so. But before I finally close, may I ask my colleagues to give a warm round of applause for our speakers today. Thank you so much.

European **Political**
Strategy Centre

Disclaimer
The views expressed here are those of the experts speaking at the Hearing. They do not necessarily correspond to those of the European Commission.