OECD publishing

ENCOURAGING DIGITAL SECURITY INNOVATION

GLOBAL FORUM ON DIGITAL SECURITY FOR PROSPERITY

OECD DIGITAL ECONOMY PAPERS

November 2020 **No. 298**

OECD
BETTER POLICIES FOR BETTER LIVES

This document contains a summary of the discussions held at the second annual event of the OECD Global Forum on Digital Security for Prosperity ("Global Forum") held on 14-15 November 2019 at Plexal, Here East, London, United Kingdom. It was discussed by the OECD Working Party on Security in the Digital Economy (SDE), and declassified by the OECD Committee on Digital Economy Policy by written procedure on 2 October 2020.

Note to Delegations:

This document is also available on O.N.E under the reference code:

DSTI/CDEP/SDE(2020)7/FINAL

This document, as well as any data and map included herein, are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area. The statistical data for Israel are supplied by and under the responsibility of the relevant Israeli authorities. The use of such data by the OECD is without prejudice to the status of the Golan Heights, East Jerusalem and Israeli settlements in the West Bank under the terms of international law.

Foreword

This report provides a summary of the second annual event of the OECD Global Forum on Digital Security for Prosperity ("Global Forum") held on 14-15 November 2019 at Plexal, Here East, London, United Kingdom. It was drafted by Laurent Bernat and Matthew Nuding, of the OECD Secretariat. Speakers and moderators reviewed the draft and provided input and corrections.

This event was sponsored by the United Kingdom Department for Digital, Culture, Media and Sports (DCMS) and TÜV SÜD. It gathered 160 experts and 30 speakers from governments, business, civil society, the technical community and academia. The report includes an executive summary, an overview of the key points made during the discussion and a detailed summary of each session. The annex contains the event's agenda. Speakers' biographies can be found on the Global Forum web site.

The event organising team included Matthew Nuding, Laurent Bernat, Ghislain De Salins and Alice Weber, of the OECD Secretariat.

The Global Forum was launched in 2018 to foster sharing of experiences and good practice on digital security risk and its management, mutual learning and convergence of views on core thematic issues related to digital security for economic and social prosperity. Its outputs feed OECD policy discussions and can lead to the development of analytical work, principles and international policy recommendations. Events are proposed by OECD delegations and organised by the Secretariat in co-operation with the host.

More information about the Global Forum and its events is available at https://oe.cd/gfdsp.

Table of contents

Executive summary

The second annual event of the OECD Global Forum on Digital Security for Prosperity (“Global Forum”) was held on 14-15 November 2019 in London, United Kingdom. It gathered over 160 participants from 22 governments as well as experts from the business, technical, and civil society communities to discuss how to encourage digital security innovation. The event took place at Plexal, the East London innovation centre hosting the London Office for Rapid Cybersecurity Advancement (LORCA).

Participants highlighted that we are at the early days of digital security innovation. All stakeholders still have a lot to learn about the role they should play to further stimulate innovation.

While there is a huge potential for digital security innovation, there are also many obstacles. However, funding does not seem to be the major challenge as digital security innovation can attract a lot of capital, although this may vary across countries.

Governments can play a key role to remove obstacles and foster digital security innovation through a mix of policy tools ranging from tax incentives to acting as an early customer for innovative products. In addition, regulation can play an important role to stimulate demand if it is flexible and outcome-based.

However, the most important component of a strategic approach to digital security innovation is the creation of a digital security innovation ecosystem, a process which takes time and should build upon an overarching strategic vision for digital security. An ecosystem brings together different stakeholder groups, generally in a dedicated geographic location to facilitate synergies between them (e.g. Be’er Sheva in Israel). While it is useful for governments to learn from successful models of innovation ecosystems, it is not possible to simply copy an ecosystem development strategy from one country to another and expect the same outcome.

International co-operation on digital security innovation is also needed. For example, Global Epic is an international initiative for co-ordinating digital security innovation ecosystems and facilitating co-operation between them. International organisations such as the OECD can also play a key role to support co-operation and provide opportunities for stakeholders to collaborate and share information on a sustainable basis.

Human capital is another major factor in fostering digital security innovation. To succeed as entrepreneurs, digital security experts need to venture outside their area of expertise and acquire business management, marketing and communication skills. The current digital security skill shortage can be partly addressed through further educational efforts, upskilling and reskilling, as well as by providing support to disadvantaged groups to take advantage of hidden talents. Governments could also give underground “hackers” a chance to move to the legal side and become innovative entrepreneurs .

Governments can encourage digital security by design in innovation more generally. Examples include Israel’s integration of digital security at the core of its countrywide smart transports initiative, Japan’s combination of Internet of Things (IoT) regulation and industry-based guidelines, and the United Kingdom’s procurement policy which requires small- and medium-sized enterprises (SMEs) and supply chain actors to comply with the Cyber Essentials scheme to become a government supplier.

Key points

This section provides an overview of the key points raised during the discussion.

1. Encouraging innovation in digital security

An innovation ecosystem is a condition for innovation to take off

- While it is useful for governments to learn from successful models of innovation ecosystems, they should be aware that it is not possible to simply copy an ecosystem development strategy from one country to another and expect the same outcome. There is no silver bullet to create an innovation ecosystem.
- Creating a digital security innovation ecosystem takes time and should build upon a long-term strategic digital security vision.
- To create an ecosystem, important lessons can be learned from successful innovation ecosystems in other areas. Innovation ecosystems are not a digital security specificity, but have common features. It is not necessary to reinvent the wheel.
- Bringing together different stakeholder groups is fundamental. The key ingredients of a successful innovation ecosystem include: entrepreneurs, corporations, academia, risk capital, and government. Additional stakeholders for a digital security ecosystem include telecommunication operators, cloud and other digital service providers, lawyers, digital security governmental agencies, and "hackers".
- A connector or facilitator is also essential to bind these stakeholders and keep them focused on responding to the market. The connector must understand both the strategic intent of the different stakeholders and the technology. Connectors are usually energetic, passionate and committed people who continuously maintain the links between stakeholders.
- People are at the centre of innovation. A successful ecosystem is a place where they can connect, talk and listen to each other, exchange, partner, etc. Good communication between stakeholders is key to maximise synergies and realise the full benefits of the ecosystem. This is particularly important for digital security, given its global nature and the level of interconnectedness and interdependence between actors.
- The physical gathering of major stakeholders in the same location is essential, such as Be'er Sheva in Israel, although it can seem counter-intuitive in the age of connectivity. Such a gathering of stakeholders requires a mutually beneficial, "win-win", situation between them.
- Ecosystems' leaders are needed to help start up the community. They need to listen to the ecosystem carefully to understand the problems faced by stakeholders, and facilitate their resolution. However, it is unclear how to identify, cultivate and mentor leaders.
- The government should focus on co-ordinating and enabling rather than seeking to control the ecosystem.
- Collaboration between competitors is necessary to foster digital security innovation, even though it can be challenging. However, with time and through experience, businesses can learn to collaborate on digital security rather than only approach it as a competitive advantage.

Co-operation between ecosystems can bring many benefits

- There is a growing opportunity for stakeholders from different ecosystems to form an “ecosystem of ecosystems” whereby they can learn from each other and collaborate to bring down costs, such as by sharing testing technologies and equipment. However, this requires building deep connections between local ecosystems.
- Global Epic is an example of an international initiative for co-ordinating digital security innovation ecosystems.
- Connectors, which are needed to bind together stakeholders within an ecosystem, can also connect ecosystems and create synergies across different regions.
- In order to learn about another ecosystem’s best practices, stakeholders need to meet in person to discuss and compare their frameworks.

Human capital is a major factor in fostering digital security innovation

- To succeed as entrepreneurs, digital security experts need to venture outside their area of expertise and acquire business management, marketing and communication skills.
- The digital security community needs leaders with sufficient understanding of policymaking, law and ethics to contribute to public discourse.
- There is a significant skills shortage in the digital security industry, which can be partly addressed through further educational efforts, as well as upskilling and reskilling. There are also hidden talents amongst those who do not have sufficient access to the technological revolution. The government can provide support to disadvantaged groups in order to both reduce inequality and tap into this potential of hidden talents to increase the country’s innovation potential.
- There is also a large potential of talents in the cybersecurity underground. Every skilled and innovative person choosing the attack side is a lost resource for the defence side. Governments could aim at creating conditions for these talents to turn away from illegal activities and give them a chance to become innovative entrepreneurs.

There are many ways that governments can support digital security innovation

- Countries need to have a coherent national digital security strategy prior to investing in digital security innovation.
- Governments can play a key role to support innovation, as shown in Silicon Valley and entrepreneurial start-up nations like Israel. However, they sometimes approach innovation by promoting national champions within their own sovereign territory, which could lead to a patchwork effect. As an alternative, organisations like the OECD can help find common approaches.
- Digital security innovation requires an “openness by default” mind-set and a culture of agility. However, it can be challenging for government agencies that have a national security role to both adopt and credibly promote such an agenda.
- Governments need to engage in a dialogue with industry in order to identify the concrete needs of the innovation ecosystem’s stakeholders.
- A mixed approach is needed to support innovation through a combination of “carrots and sticks”, with flexible and agile regulation and innovative policy tools such as sandboxes, recognising that entrepreneurial activity often moves at a different pace to policy making.
- Regulation can support demand for innovative digital security products.
    - Policy makers should aim to improve the effectiveness of existing regulations rather than just adding more regulatory layers and constraints on businesses, in particular for entrepreneurs.
    - Principles-based, outcomes-oriented regulations with clear metrics for success is much more effective than checklists and other prescriptive compliance frameworks. Flexible regulation that focuses on the “what” without prescribing the “how” (such as the General Data Protection

Regulation (GDPR) in the EU) generally drives businesses to address digital security more dynamically and strategically, and to take a more agile and pragmatic risk management approach.

- Other means governments can use to foster digital security innovation, in addition or apart from regulation, include:
    - Creating a conducive environment through regulatory sandboxes;
    - Acting as a connector between innovative companies and their potential customers;
    - Performing a broker role in the digital security ecosystem, by acting as a neutral body that can lead on innovation without a commercial agenda. Universities can play a similar role;
    - Taking on some of the risk for early stage companies and innovators by acting as an early customer, although this requires changes in the public sector culture which is generally risk averse because failure is rarely tolerated in government;
    - Assisting early stage companies through tax incentive schemes for entrepreneurs and the provision of seed capital;
    - Facilitating access to funding by civic tech and non-profit innovation models which typically struggle for resources;
    - Working together across borders to solve common problems. However, governments are likely to place a number of conditions with respect to innovation-related cross-border collaborations.

2. Fostering Digital Security in Innovation

- Digital security is one among many challenges that entrepreneurs are facing.
- Many innovative companies often perceive digital security as a cost and an obstacle that will increase their time to market. They often do not perceive that digital security can be a valuable asset and a market differentiator.
- Different firms have different objectives and relate to digital security risk differently.
- A positive relationship between technical experts and business leaders, in small and large firms, is needed for digital security to be approached as an opportunity rather than a burden.
- There is a paradoxical cultural gap between the innovation and digital security risk cultures. Risk is at the core of an entrepreneur's culture. However, technical security professionals are not always able to relate digital security to business risk, in order for entrepreneurs to integrate it in their overall business equation. In turn, entrepreneurs are often not sufficiently aware and educated about digital security risk to proactively take it into account in their business strategy.
- Innovation is everywhere, in start-ups but also in academia, government, and large corporations. To encourage digital security by design, policy makers need to address all the places where innovation can take place across the different stakeholder groups.
- Education and training of both entrepreneurs and digital security professionals should evolve. Security professionals should have a better knowledge of the business culture and entrepreneurs should understand digital security to be able to proactively manage digital security risk as part of their business decision-making process.
- Governments can combine different approaches to support digital security by design. For example:
    - Israel's digital security agency (INCD) is adopting a security by design approach to support its ambitious countrywide digital transformation policy initiatives such as in the smart transports area.
    - Japan adopted a combination of regulation and industry-based guidelines to keep up with technological change and dynamic threat while not stifling innovation.
    - The United Kingdom's government uses its procurement policy to encourage SMEs and supply chain actors to enhance their digital security.

- Awareness raising and education of users and vendors are essential. Balancing digital security measures and requirements with usability is also key.
- Governments should engage with civil society when designing digital security policies as digital security can easily affect human rights and fundamental values.

Detailed Summary

This section provides a summary of each session. The concluding session brought the sessions' moderators together for final remarks. These remarks have been included in a "Concluding points" at the end of each session's summary below. The annex contains the event's agenda. Speakers' biographies can be found on the Global Forum web site. Italicised text highlights some of the key points.

Strategic Initiatives for Digital Security Innovation

Israeli National Cyber Directorate (INCD)

The Israeli approach to encourage digital security innovation is based on the recognition that the government should be part of the solution rather than part of the problem. For the Israeli government, a start-up nation must adapt to dynamic and global challenges, risks and opportunities. It is therefore essential to have a coherent national digital security strategy prior to investing in digital security innovation. The government identified three key priorities to develop a vibrant innovation policy: i) address the lack of knowledge and shortage of digital security professionals and teachers with digital security skills, ii) address the market failure that generates thousands of IoT products without enough digital security, and iii) prioritise efforts and innovation according to a map of risk and damages.

In addition to establishing a national cyberspace campus in Be'er Sheva[1]**,** the government uses its purchasing power to support start-ups. For example, the government changed its tendering process to encourage innovation. In some areas, it switched the tendering selection principle from lowest priced to best pioneering product. Furthermore, in Israel, start-ups often have difficulties finding their first large customer rather than finding investments. Therefore, instead of a traditional tender process, which typically favours large companies, the government invites innovators to respond to a challenge, letting ten start-ups take the lead. They develop proof of concepts (PoC) for which they are paid along during 3 to 6 months, regardless of their PoC's success. The government then choses the three best PoCs and continues to work with these start-ups. If they are successful, they become an official government supplier. The government also holds a start-up day to facilitate connections between young innovators and large companies.

The government also stimulates demand for innovative products by creating a supportive environment to promote a culture of digital security, and encouraging companies to implement voluntary standards for digital security risk assessment. For example, in 2020, Israel will give priority for public sector tenders to companies that apply the cyber national certification. The INCD also released a free tool to manage a company's digital security risk and controls.

[1] http://cyberspark.org.il

The United Kingdom National Cyber Security Centre (NCSC)

UK's National Cyber Security strategy is based on three pillars: defend, deter and develop. Initiatives to encourage digital security innovation implement the third pillar.

In addition to the London Office for Rapid Cybersecurity Advancement (LORCA)[2], where the Global Forum event took place, *the UK runs a number of programmes to encourage innovation while at the same time assessing in which areas the private sector is best placed to lead*. These include a small business boot camp, early start-up incubators and a program encouraging academics to turn research into products.

Furthermore, GCHQ, the home of the UK National Cybersecurity Centre (NCSC), learned from its past experience of discovering asymmetric cryptography but missing the opportunity to leverage its potential for economic and social prosperity. *The agency explored how its intellectual property could benefit a broader prosperity agenda* than the narrower intelligence mission it was intended for in the first place. For example, it now collaborates with the Turing Institute, which applies to medical records data analytics initially developed for intelligence purposes. Furthermore, *the UK national cybersecurity strategy enabled GCHQ to engage more proactively with innovation*. It launched the NCSC Cyber Accelerator, part of the Cheltenham Innovation Centre[3], which had supported 30 companies as of November 2019. This Centre's location near GCHQ allows for a close relationship between start-ups and GCHQ's experts who can support their products' development. The Centre is slowly evolving into an ecosystem with some firms staying in the area after leaving the accelerator. GCHQ however only provides expertise and relies on a private partner to provide the mentoring and other business support to entrepreneurs. *This experience is challenging the agency's national security culture*.

The UK recognises that *there is a fundamental difference between innovation in digital security and innovation in other areas*. Digital security is generally about protecting systems that may not have been well designed, deployed or configured, from attacks. Whereas, innovation, particularly for start-ups, is about developing a new idea and rapidly delivering to the market. This often requires a trade-off between time-to-market and design quality. Addressing a digital security challenge with a product that itself is not very robust or is not very well built actually aggravates rather than addresses the overall digital security challenge it is expected to mitigate. *A digital security solution has to be built upon a solid foundation, which is particularly difficult for smaller companies.* More generally, it is a major challenge for both digital security and other start-ups, to develop "secure by design" products that can scale, and to continue to improve their security practices over time.

The French National Cybersecurity Agency (ANSSI)

ANSSI places a strong emphasis on innovation. Ten percent of the agency's staff are researchers and have time to attend conferences, develop new ideas, and publish in journals. This is both an important motivation for them and a way to evaluate how innovative and successful they are. ANSSI also encourages former employees to create start-ups based on their experience at the organisation.

ANSSI also places a strong focus on collaboration with the security community and supports a principle of "openness by default". This means that any new tool, detection mechanism or threat intelligence system it develops will be shared with the community, often through open source. For example, ANSSI developed an analysis tool, Open CTI (Cyber Threat Intelligence)[4] that it shared online. This is often at odds with the

[2] www.lorca.co.uk

[3] www.ncsc.gov.uk/information/cyber-accelerator

[4] www.opencti.io/en/

culture of secrecy of the national security community and is therefore sometimes challenged. However, the openness principle focuses on the tools rather than on the information and data.

The agency can work with non-governmental stakeholders in a traditional way such as through public procurement contracts. *But it can also operate in a more agile and innovative way*. For example, when the European Commission launched the European Cyber Security Organisation (ECSO) as a public-private partnership (Cf. Box 2), ANSSI faced legal difficulties to join it as a public entity but swiftly moved to participate as a private entity instead, saving time and increasing efficiency. Another example is the preparations for the 2024 Olympics where the agency is working on a mega project with many partners to manage the event's security, promote stakeholders co-ordination and benefit digital security in France more generally.

France is planning to develop a cyber-campus, similar to Be'er Sheva, where it can bring stakeholders together to innovate, train, develop research, etc. The usual way for governments to develop such an initiative is to pay the private sector to do it. This time, France will ask companies to pay to get involved because they will benefit from the initiative, which will bring them together with research institutions, universities, schools, and the State.[5]

The Australian Cyber Security Growth Network (AustCyber)

Created in 2017, AustCyber[6] is an independent organisation, funded by the government, which provides a link between the industry and the government. There are around 300 digital security companies in its ecosystem, with 40 cutting edge ones. AustCyber maintains a network of digital security representatives in every Australian state and territory in order to foster adequate cooperation across the country. Its most important role is to *identify the digital security challenges specific to a set of key growth sectors (e.g. agriculture, health, mining) and advise digital security companies in the ecosystem on how they can address them*. It engages with accelerators and incubators and can represent industry without being an industry association. It can lobby the government while working closely with many government partners such as the Australian National Cyber Security Centre, sectoral regulators, the Australian federal scientific research agency (CSIRO), and the Department of Industry, which is responsible for the growth of small businesses.

AustCyber has three objectives:

1. Grow the digital security ecosystem, including by encouraging the government, which tends to be risk averse, to buy sovereign products;
2. Help start-ups to grow, including by encouraging the government to fund start-ups (currently AUD 50 M for 15 projects) and working with industry to provide start-ups with an environment in which they can test and learn. AustCyber also helps start-ups scale to a wider and international customer base including by better understanding cultural and economic differences across countries in the Asia-Pacific region and adjusting strategies accordingly; and
3. Promote education, research and development, for example, by connecting industry with research institutions best positioned to answer questions such as ethics and AI.

AustCyber works with schools, tertiary education providers, universities and organisations to bridge the digital security skills gap with the objective of doubling the digital security workforce by 2025. By collaborating with universities on STEM curricula, it ensures that universities are creating good quality courses.

[5] www.ssi.gouv.fr/agence/cybersecurite/un-campus-dedie-a-la-cybersecurite/

[6] www.austcyber.com

The European Commission

At the European level, digital security firms, in particular SMEs, interested in selling certified digital security products in the EU market used to face two obstacles: they had to request certification in each EU member and again in each non-EU country they wanted to trade in. *The Cybersecurity Act aims to address this market fragmentation issue by introducing voluntary EU-wide digital security certification schemes* and enabling mutual recognition agreements of certification schemes with non-EU countries. This aims to be an enabler for SMEs and small industries.

In addition, the *European Commission proposed the creation of a European Cybersecurity, Industrial Technology and Research Competence Centre and Network of National Competence Centres*. This initiative would facilitate co-ordination of national capacity building as well as research and development projects, and of research and innovation efforts of national cybersecurity centres. It would also help develop capacities at national level by providing funding to national cybersecurity centres, who, in turn, would transfer it to national public and private stakeholders. The Centre would help develop a co-ordinated response to the evolving risk landscape related to emerging technologies, such as 5G, Artificial Intelligence, the Internet of Things and blockchain. The first step in this competence network is the formation of the community. The Commission launched four pilot projects to test the idea, the Concordia, Cybersecurity for Europe, ECHO and SPARTA. They are bringing together more than 160 partners from 26 EU members.

The EU has a large number of funding opportunities for innovation initiatives in areas such as resilience in evolving IoT systems, digital security and privacy for citizens and Small and Medium Entreprises (SMEs), cybersecurity in the electrical power and energy systems, Artificial intelligence and security, etc. It also has contractual public private partnerships, such as the European Cyber Security Organization (ECSO) that is more focused on the research and innovation dimension (cf. Box 2Box 1).

Concluding points

There is a tension between digital security and innovation (i.e. product robustness vs time to market), and no easy solution to address it, in particular with respect to IoT devices.

A mixed approach is needed to align the incentives, using a combination of carrot and stick, flexible and agile regulation, and other policy tools.

Government has always played a key role in innovation, it should play a role in digital security innovation as well. This may require reframing digital security from a cost to an investment or benefit, introducing trust labels, and developing a more positive narrative around digital security rather than focusing on threats and damages.

Calls for government to take a share of the risk often contradict the public sector culture, which is generally risk averse because failure is rarely tolerated in government. Public procurement can certainly help set and stimulate the market.

Governments sometimes approach innovation by promoting national champions within their own sovereign territory. This could lead to an unhelpful patchwork effect. Instead organisations like the OECD can help find common approaches.

Opportunities and Challenges to Enable Digital Security Innovation

While lack of capital may be an issue outside of the United States, *the idea that money is the only obstacle for digital security innovation is a myth*. Digital security innovation can attract a lot of capital, but capital must be accompanied by entrepreneurial capacity and, more generally, the presence of an ecosystem.

Nevertheless, there can be gaps where investors may not be interested in providing seed capital, in which case alternative options such as government grants can be useful.

What are the key ingredients of a successful "digital security innovation ecosystem"?

Why does digital security innovation happen in certain places and not others? In short, *an innovation ecosystem is required for innovation to take off*. However, the kind of ecosystem that is needed and the means to establish one vary significantly depending on the region. *There is no silver bullet approach and therefore it is not possible to simply copy an ecosystem development strategy from one region to another and expect the same outcome*. The fact that money, talent and capital exist in certain regions where innovation is not taking place demonstrates that these elements do not bring about innovation alone.

Creating a digital security innovation ecosystem takes time and builds upon a long-term strategic vision

One of the main lessons from the successful creation of Cyberspark is that creating such an innovation ecosystem takes time. Israel began planning it thirty years ago when the government started to view digital security as a strategic threat to its modern and connected way of life. Cyberspark was created as a component in a broader strategic geopolitical and economic vision where digitalisation was viewed as a core dimension of the country's future. *Although technological development and disruptive technologies are rising at exponential speed, it is time-consuming to build an effective ecosystem.*

Innovation ecosystems are not a digital security specificity and it is not necessary to reinvent the wheel. Important lessons can be learned from successful innovation ecosystems in other areas. For example, it took a century of co-operation of stakeholders in the aviation ecosystem to build an innovative industry that millions of people trust to travel by plane. The same kind of co-operation is needed for digital security. Some of these other ecosystems' methodologies and paradigms can be adopted and applied to digital security innovation ecosystems. There is a lot to learn, including on how they are dealing with technology, regulation, human capital development, etc.

A digital security ecosystem requires key stakeholders plus leaders and a connector

According to MIT,[7] *five key stakeholders must come together to form an innovation ecosystem*: entrepreneurs, corporate, academia, risk capital (e.g. Venture Capital, grants, etc.) and government. With respect to digital security innovation ecosystems, additional stakeholders are needed. The EU pilot program SPARTA[8] involves *telecommunication operators, technical cloud providers and other digital service providers, lawyers, security agencies and even "hackers"*, which it views as particularly important in a security context.

An ecosystem is like a set of jigsaw pieces, often partially already there, which need to be connected. Because these stakeholders often would not ordinarily talk to each other, *a connector or facilitator is also required to bind them and keep them focused on responding to the market*. Not anybody or any organisation can be the connector. It must understand both the strategic intent of the different stakeholders and the technology. Connectors are usually energetic, passionate and committed people who continuously maintain the links between stakeholders. The connector needs to adapt to cultural differences and changing players. For example, SPARTA's mission is to bridge a fragmented European ecosystem where excellent scientists, entrepreneurs and capital are in no short supply.

[7] https://innovation.mit.edu/assets/BuddenMurray_An-MIT-Approach-to-Innovation2.pdf

[8] www.sparta.eu

Ecosystem's leaders are also needed to help start up the community. They need to listen to the ecosystem carefully to understand the problems faced by stakeholders, and facilitate their resolution.

Lastly, rather than seeking to control ecosystems, *the role of government should be to co-ordinate, govern and enable*, as illustrated by CyberNB[9] in Canada.

The physical gathering of major stakeholders and good communication between them is crucial

The physical gathering of major stakeholders in the same location is essential, although it can seem counter-intuitive in the age of connectivity. Stakeholders gathered in Be'er Sheva, Israel, progressively, with university coming first, then industry, followed by human capital, after which the government decided to turn Be'er Sheva into the capital of cyber security.

Such a gathering of stakeholders requires a mutually beneficial, "win-win", situation between them. For example, when academics reside with industry, they can keep up with the industry's pace of change, and maintain their curriculum up to date. Meanwhile, industry players can hire more mature graduates who are in a better position to be operational in a work environment.

Good communication is key to maximise synergies and realise the full benefits of the ecosystem. This is particularly important for digital security, given its global nature and the level of interconnectedness and interdependence between actors. For example, the better the communication between stakeholders on what the market and government are looking for, the easier they can identify the problems that need solving, which helps investors direct their capital and universities and be more impactful. However, there is a concern that language and cultural references can be lost when speaking about issues across ecosystems. This loss of communication can happen between different regions. It can also happen within an ecosystem, for example between the federal government and local stakeholders. Face-to-face interactions, where questions can be asked and parallels can be drawn, are needed to ensure appropriate understanding across ecosystems and stakeholders' cultures. Virtual interactions are not sufficient.

Investors can play an important role in assisting entrepreneurs to truly focus on market needs and appreciate the market scale most appropriately, including at regional and global levels. For example, they can provide advice from experienced CISOs on how to deliver a product that has value on the market.

How can public policy support digital security innovation?

Industry can contribute to increasing demand and driving digital security innovation. For example, Siemens Australia holds a digital security awareness conference each year with all of the companies along their supply chain. Investors can also encourage companies to approach security as a business enabler, rather than a service blocker. But in addition to what businesses can do, there is a widespread recognition that *regulation and public policies can play a key role to foster the demand for more secure innovative technologies, and support digital security innovation more generally*.

Principles-based, outcomes-oriented regulation can support demand for innovative digital security products

While regulation can foster demand for digital security innovation, *policy makers should aim to improve regulation's effectiveness rather than just adding more digital security requirements*. Governments often tend to over-regulate businesses, adding new layers of regulation without removing older ones over time. Rigid regulation, which does not take into account the complexity and dynamic nature of digital security

[9] https://cybernb.ca

risk, can overly burden companies, impede their agility and impose costs that divert efforts from tackling digital security.

Principles-based, outcomes-oriented regulation with clear metrics for success is more effective than checklists and other prescriptive compliance frameworks. Flexible regulation that focuses on the "what" without prescribing the "how" generally drives businesses to address digital security more dynamically and strategically, and to take a more agile and pragmatic risk management approach. Furthermore, some experts believe that regulation can increase demand for more innovative security products by providing clear standards organisations should meet, and by punishing those who fail to adopt good security practices and processes. The *GDPR is a good example* of such a flexible principles-based and outcomes-oriented regulation with sanctions in case of non-compliance, which moved privacy protection from the technical to the board level. *Governments could also consider introducing a "duty of care" requirement* to clarify the responsibility of organisations and products makers to protect users from digital security threats.

Sectoral regulation can also help increase demand by requiring alignment with higher digital security standards in specific areas. For example, the Canadian national shipbuilding strategy includes a component asking for cybersecurity compliance and that alone will implicate 10 000 companies.

Government have many additional means to support digital security innovation

In addition to regulation, governments can also foster digital security innovation through tailored public policies, recognising that *industry moves at a different pace* than policy making or academic research. As a starting point, they need to *engage in a dialogue with industry in order to identify the concrete needs of the innovation ecosystem's stakeholders prior to intervene*. Based on Israel's experience, they may for example identify requirements such as loosening work permit regulation in order to facilitate exchange of knowledge providing, or providing means for smart transportation start-ups to test new networks (e.g. 5G). Another example is the incorporation of the next generation's needs into the education system, such as in Canada where the government views its ability to connect students to the industry as a winning formula and starts talent development very early by teaching programming and digital skills to children from a young age.

Governments can foster digital security innovation through at least the following means:

- *Creating a conducive environment through regulatory sandboxes*, which offer innovative companies a testing ground for new technologies, business models and processes.
- *Acting as a connector between innovative companies and their potential customers*. For example, the Japanese Ministry of Economy, Trade and Industry (METI) provides a platform through which SMEs and digital security product providers can connect, overcoming their lack of strong brand or reputation. Through this platform, the government bridges the gap between existing security providers and new and hidden digital security needs.
- *Performing a broker role in the digital security ecosystem*, by acting as neutral body that can lead on innovation without a commercial agenda. Universities can play a similar role, as they can also contribute to innovation free from the constraints of commercial incentives.
- *Taking on some of the risk* for early stage companies and innovators by acting as an early customer, which can enable the company's technology to be tested and can be a positive reference for other potential customers. However, entrepreneurs may not be familiar with the often complex and bureaucratic nature of government procurement.
- *Assisting early stage companies through tax incentive* schemes for entrepreneurs and the provision of seed capital. Many entrepreneurs will relocate their companies to the jurisdiction offering the most desirable financial schemes. For example, Mach37, based in Virginia, United States, and Cylon, based in London, United Kingdom, are government-supported accelerator programmes that offer such support to innovators.

Human capital is a major factor in fostering digital security innovation

Giving skilled attackers a chance to become innovative entrepreneurs

There is a shortage of digital security skills in most countries. When it comes to human capital, there is an asymmetry between attack and defence, whereby the attack side needs less resource than the defence side. Therefore *every skilled and innovative person choosing the attack side is a lost resource for the defence side. Public policy could aim at creating conditions for these talents to turn away from illegal activities*. It could provide innovative offensive hackers with the opportunity to cross over to the good side and make legitimate money by joining the digital security innovation ecosystem. By opening up the talent pool, this would enhance the innovative capacity of the ecosystem while reducing the resources of the attack side. Governments could also develop visa programmes to facilitate the inward movement of such talent from abroad.

Encouraging digital security experts to acquire communication and business skills

Digital security is often viewed as an isolated matter and the digital security community as being a closed group of experts speaking jargon that outsiders do not understand. Security experts are skilled at spotting "buffer overflows", but in order to empower themselves to innovate, *they need to venture outside their area of expertise and acquire skills in fields such as business management and marketing*.

Public policy can play a role in helping digital security innovators to develop the essential business and communication skills needed to succeed as entrepreneurs. Successful digital security innovation requires great technical security expertise combined with the ability to understand buyers' needs and constraints, as well as skills to build trust and engage with partners in the business community. Innovators need to be able to demonstrate a product's value to potential partners and buyers who, despite a desire to try innovative solutions, often lack the expertise to evaluate products solely in technological terms. Security entrepreneurs need to be able to convey the business benefits of their technology and explain how this might relate to the buyer's business objectives, rather than only promote products based on their technical ingenuity. They should speak in a language that everybody, including decision makers in non-ICT firms can understand, from a pacemaker manufacturer to any other firm in a traditional sector with legacy systems and devices which are not secure and will need to evolve to higher standards.

More generally, there is a need for *more leaders in the digital security community with sufficient understanding of policymaking, law and ethics to contribute to public discourse*. This would help raise all stakeholders' digital security awareness and increase demand.

Revealing hidden talents among disadvantaged groups

Lastly, while there is a significant skills shortage in the digital security industry, *there are also hidden talents amongst those who do not have sufficient access to the technological revolution*. For example, Elizabeth Friedman who was one of the most prolific code breakers in the United States history could have missed the opportunity to work in this space based on her gender. Today, people without broadband connection cannot develop digital skills, and among them, those with a potential for digital security do not often have an opportunity to realise it. *Governments can provide support to disadvantaged groups in order to both reduce inequality and tap into this potential of hidden talents.*

Concluding points

- The role of governments has been important even in Silicon Valley and entrepreneurial start-up nations like Israel. Governments and intergovernmental organisations should talk more to the other stakeholders, such as entrepreneurs, hackers, universities, risk capital provider and large companies.

- Governments can also add value in several ways, such as by identifying the challenges of the coming decade, taking into account the overall system complexity. For example, societies are going to find out that, like asbestos, some technologies implemented in the past are not good for our digital health. Governments have a role to clear up asbestos and help industries move on and deal with their legacy issues. How does that translate into digital security?
- Innovation is not always about a frontier horizon involving ground-breaking start-ups. It is also about incremental improvements in large enterprises, whether public or private.
- It is important to discuss concrete actions that can improve the situation and identify what the next steps should be.
- Leaders are needed in these digital security communities, but how to identify, cultivate and mentor leaders is unclear and should be discussed.
- People are the solution, but they need enough digital security skills. The skills challenge concerns both current employees and future generations.
- Some start-ups need funding and tax breaks, in particular in civic tech and non-profit models which typically struggle for resources.
- Innovation happens across many stakeholders (academia, research, government, industry, investors, etc.) operating at different pace. How can these differences be accounted for?
- Regulation should use clear metrics and avoid redundancies so that compliance does not induce unnecessary expenses.
- Product creators have a duty of care and should make products sufficiently secure by design. The government needs to have sticks, alongside the carrots.

Co-operation for digital security innovation

Co-operation between ecosystems can bring many benefits

There is a growing opportunity space for stakeholders from different ecosystems to learn from each other. However, this requires building deep connections between local ecosystems.

Global Epic[10] is an international initiative for co-ordinating digital security innovation ecosystems and facilitating co-operation between them (Box 1). It was created as ecosystem leaders from different countries realised that they had a lot to gain from sharing and comparing their experiences and discussing best practices. Ecosystems have strengths in different industry areas, e.g. mobile devices, or advanced manufacturing, or medical devices. Global Epic is exploring the challenge of how *ecosystems can collaborate to reduce cost, for example, by doing shared purchase of expensive equipment,* or making some pieces available to ecosystems that cannot afford them to level the playing field.

In order to learn about an ecosystem's best practices, stakeholders need to meet in person to discuss and compare their frameworks. Emails, web sites and other virtual means are not sufficient for co-operation between ecosystems to generate benefits. Innovation is a matter of people and so is co-operation.

Connectors, which are needed to bind together stakeholders within an ecosystem, can also connect ecosystems and create synergies across different regions.

[10] https://globalepic.org

Box 1. Global Epic, an international initiative for co-ordinating digital security innovation ecosystems

Global Epic (Global Ecosystem of Ecosystems Partnership in Innovation and Cybersecurity) is an organisation that co-ordinates co-operation between digital security ecosystems across the world. It began with leaders of ecosystems coming together to discuss best practices and, as of 2019, it had over 27 members from 15 different countries and 3 continents. Its members' ecosystems were formed through academia, local government, industry hubs, and sometimes a combination.

Through Global Epic, ecosystem leaders can compare one another's frameworks and figure out what ideas are worth taking to their own ecosystems. The Global EPIC Soft-Landing Program is a means to strengthen the ties between the ecosystems. It offers companies and entrepreneurs an opportunity to "soft land" for a trial period in the market of one of the Global EPIC ecosystems. It provides an easy and low risk entry trial to companies and entrepreneurs entering a new international market, accessing the resources they need to more readily tap into commercial opportunities. For example, a company which wants to open an outpost in another country can use this programme to get office space, mentors, and lawyers, and to address issues such as immigration issues.

Governments can work together to solve common problems

Governments can also work together to solve common problems as no country has a monopoly on innovation and there are many complementarities across countries. For example, the US Cybersecurity and Infrastructure Security Agency (CISA) has thirteen separate government-to-government cooperative agreements covering 30 digital security project with equivalent departments in other countries. However, in order to co-operate effectively, holding meetings or exchanging emails is not sufficient*: physical presence is needed*. For example, CISA has embedded analysts working in the UK alongside NCSC, and NCSC has staff working in Washington DC with CISA.

Nevertheless, governments are likely to place a number of conditions with respect to innovation-related partnerships. For example, they will assess the innovative technology being anticipated and the challenges it may raise; whether there is respect for intellectual property, a legal tradition of an independent judiciary, and respect for privacy in the location where it is being developed; as well as whether the entity developing the technology has ties to the government.

A key challenge is for businesses to simultaneously compete and collaborate on digital security

To innovate together in an ecosystem, stakeholders should see risk as being shared among them ("my risk as your risk and your risk as my risk") rather than viewing digital security as a competitive advantage. However, it takes time for different stakeholders, particularly business, to learn through experience that they can gain more from collaboration than from competition. In addition, it is not easy to reconcile the idea that businesses should collaborate extensively on digital security with simultaneously viewing it as an opportunity to differentiate themselves and build better products than the competition. Working around this issue requires a respect for diversity that recognises that some topics are in the purview of other groups. The European Cyber Security Organisation (ECSO) has been examining ways forward in light of this clash (Box 2).

Digital security innovation extends beyond developing new technology or software. It is also about being innovative when considering how to prepare the digital security workforce of tomorrow, strengthen supply chain risk management, address ethical issues, and support public-private partnerships. ECSO's experience also shows that digital security innovation should be approached holistically.

Box 2. The European Cyber Security Organisation (ECSO)

Initiatives such as ECSO show that it is possible to develop a common understanding of what different countries and stakeholders can do together.

ECSO is a three years old public-private partnership that coordinates the innovation roadmaps and investments in the EU, bringing many different voices in the discussion: academia, industry, SMEs and Member States. ECSO is an example of companies and other stakeholders coming together to enhance digital security. SMEs can learn a lot from ECSO's membership that would not have been available to them otherwise.

ECSO helps identify priorities at European level, building on European strengths and focusing on European issues and impacts. It co-ordinates and prioritises investments across many technical areas, such as Artificial Intelligence, quantum computing and blockchain, as well as non-technical ones such as SMEs, women in cyber, youth in cyber, etc. ECSO's European interactions have generated interest outside Europe and the Organisation is making outreach efforts to like-minded countries such as Japan, particularly around certification and women in cyber.

Concluding points

- Due to the complexity of the digital transformation, one of the best ways to tackle the digital security challenge at national, regional, and global levels is to build an effective "ecosystem of ecosystems".
- Digital security innovation is no exception to innovation ecosystems in general: physical presence of major stakeholders is essential, and coordinating hubs of facilitating bodies with committed people who are connecting the dots within the ecosystem, and between ecosystems, are necessary.
- People are at the centre of innovation. A successful ecosystem is a place where people can connect, talk and listen to each other, exchange, partner, etc. An ecosystem needs a common language and knowledge, as well as central place to bring people together.
- An ecosystem is a tool. Once an ecosystem has been created, it needs to be used, otherwise it is just an empty buzzword.
- International organisations can play a key role to actively facilitate connecting the different actors.

Fostering Security by Design in Digital Innovation

Digital security is one among many challenges that entrepreneurs are facing

Entrepreneurs and start-ups face many challenges and need to keep focus on priorities such as getting to market, beating the competition, and raising revenue. They need to figure out how to develop their technology and find the best partners to help them test it. They often have to work on fast deadlines, which can lead them to the wrong market strategy. But perhaps their most important challenge is a lack of resources. Start-ups are often more concerned with the existential threat posed by a lack of funding, and by other priorities such as time-to-market, than they are with digital security. *Most of start-ups will overlook security to save money and time.*

Many innovative companies often perceive digital security as a cost and an obstacle that will increase their time to market. They view it as hampering their ability to compete rather than as a providing them with a business advantage. *They often do not understand that security can be an opportunity and a valuable asset*, and that the customer trust it brings takes years to construct and is easy to destroy. Customers expect products on the market to be safe from all hazards including digital. Furthermore, it is difficult for entrepreneurs to strike the balance between short, mid and long-term objectives. Putting the product on the market is only the first step and a balance must be sought with long-term goals.

Different firms have different objectives and relate to digital security risk differently. A gaming start-up that needs to deliver its product before Christmas is likely to take a more lenient approach to digital security risk than a company in the nuclear, oil or another critical sector. Many SMEs have limited resources for security by design and bigger companies in their value chain or large customers they depend upon are likely to set the minimum standard.

There is a paradoxical cultural gap between the innovation and digital security risk cultures

Risk is at the core of an entrepreneur's culture. Every business must accept some level of risk to progress and survive. However, technical security professionals are not always able to relate digital security to business risk so that entrepreneurs can factor it in their overall business risk equation. And entrepreneurs are often not sufficiently aware and educated about digital security risk to proactively take it into account in their business approach. This gap can threaten the company's life and value. For example, if an innovative data driven company loses control of its data through a breach, or of its innovation through economic espionage, it can lose its competitive advantage.

Innovation also takes place in large and established firms where digital security professionals often lack the opportunity and/or ability to communicate about digital security risk in business terms to the board. Boards also do not necessarily inform digital security professionals of the business objectives for digital security risk to be managed in a manner that promotes the business. A positive relationship between technical experts and business leaders is needed for security to be approached as a business promoter rather than a burdensome obligation. Furthermore, leaders should ensure that security by design addresses both the technical level (software, hardware, architecture) and the company's processes, including product design, response to incidents, vulnerability management, etc.

Education and training of both entrepreneurs and digital security professionals should evolve. Security professionals should have a better knowledge of the business culture to communicate more effectively with business leaders about digital security risk. Entrepreneurs should also better understand digital security to be able to proactively manage digital security risk as part of their business decision-making process.

Governments can support entrepreneurs

Governments can combine different approaches to support digital security by design.

In Israel, the INCD is adopting a security by design approach to ambitious countrywide digital transformation policy initiatives, such as in the smart transports area (cf. Box 3). For example, the government requires 10-15% of its innovation research funding in automotive technology to be allocated to develop secure by design products in this area.

Box 3. Israel: Digital security policy “by design” for smart transports

The digital transformation is challenging digital security policy making by creating new areas such as 5G, smart health and smart transports, where factors such as the technology and business models are not yet mature, and the threat is not sufficiently well known. It is difficult to develop digital security policies to address such emerging areas without first precisely calibrating regulation in order to avoid stifling innovation and delaying adoption.

INCD is addressing this challenge by embedding digital security policy within specific digital transformation policy agendas. This multistakeholder approach aims to ensure that *i)* digital security is a facilitator rather than a showstopper for digital transformation agendas in specific sectors, and *ii)* digital security regulation is developed in parallel with the technological and standardisation progress rather than as an afterthought likely to delay adoption.

For example, in 2017, the government decided to pursue a smart transportation agenda as a major inter-ministerial initiative. This involved regulatory reform, new infrastructure and a comprehensive policy plan dealing with the emergence of a new digital market, in an area where the technologies, the business environment and the ecosystems are not yet mature. INCD decided to take part in this agenda by engaging with and incentivising the transportation industry, promoting the necessary digital security technologies, developing related methodologies and risk management schemes, creating and testing specific infrastructures, addressing new stakeholders (such as the Ministry of Transports and the transports regulator), and building new digital security communities.

INCD believes that it is important to connect all the silos (e.g. testing facilities, regulatory aspects, software components, research and development, etc.) by bringing them together into a physical focal point, namely the Digital Transportation Innovation Arena to be deployed in Be’er Sheva. It will consist of a PPP complementing the existing ecosystem with global automobile technology operators and manufacturers, which are currently not present in Israel, benefiting the needs of the Ministry of Transports, and enriching the existing start-up and cybersecurity ecosystem.

An important part of the smart transportation agenda is to facilitate access to public sector data by the automobile tech industry. This includes geolocation data held by the Ministry of Transports and municipalities. For INCD, this also means providing the relevant actors in the transports area with access to transports-related threat intelligence and threat expertise information.

In Japan, the government considers that a combination of regulation and industry-based guidelines is key to prevent stifling innovation while keeping up with technological change and dynamic threat. The government observed that half of the 212 billion digital security attacks in 2018 targeted IoT devices. It also recognised that consumers take the security of these devices as a given and therefore are unlikely to worry about it. This is why the government decided to compel IoT manufacturers to implement digital security by design requirements. It also introduced a certification system to ensure baseline security. The government encourages the industry to develop its own IoT certification scheme. One of these schemes includes a digital security label with stars indicating products’ security level, from basic to very good. The government also created a system where connected devices are tested against simple identifiers and passwords. When credentials are too weak on a device, the ISP is asked to notify the owner and invite him/her to strengthen them.

In the United Kingdom, the government uses its purchasing power to encourage SMEs and supply chain actors to enhance their digital security. Companies willing to become government suppliers need to implement the Cyber Essentials or Cyber Essentials Plus certification schemes. This approach promotes digital security without creating rigid compliance regulation that is likely to become outdated quickly and create burdensome requirements for business. When regulation is envisaged, it needs to be sufficiently flexible to match the dynamics of digital security. It is for example the case with the EU GDPR.

Awareness raising, education of users and vendors, as well as increasing the usability of security products are essential. If people do not understand the importance of security, they will never invest in it. It is also important to ensure that security enhancements are user friendly and do not undermine usability. There is often resistance against digital security measures in organisations because it increases inconvenience. Governments and the tech sector can play a key role to educate and raise awareness about the benefits of security as a means to change mindsets.

Digital security can easily affect human rights and fundamental values. Governments should therefore engage with civil society when designing digital security policies. For example, Access Now offers a digital security helpline for civil society actors, including journalists, NGOs and human rights defenders who are often both vulnerable and targeted by threat actors. It encourages other civil society groups to have their own digital security officer. Building the experience of groups such as Access Now, civil society can help governments better understand how digital security policies can support human rights. Civil society also co-operates with the private sector. For example, Access Now worked with WhatsApp to fix a vulnerability that involved spyware on human rights activists phones.

Concluding points

- Innovation is everywhere. Entrepreneurs and start-ups are of course important, but innovation also happens in academia, government, and large corporations. When we talk about building digital security by design, we need to talk about all of the places where innovation can take place across the different stakeholders.
- In addition to technology, innovation is also about people and processes.
- Market demand for security is a key requirement for innovators to increase security by design and for security to become a market differentiator. However, it is unclear whether consumers experience enough difficulties around their IoT devices to generate such demand. A major challenge is to educate consumers in a way that gets them to issue that demand.
- Large projects, such as the smart transportation initiative in Israel, can also generate demand for security by design to which the market is likely to respond if they include clear security requirements.
- Governments have a role to play. For example, they can set minimum requirements as in Japan. But beyond that, there is an ongoing discussion between those who think industry and the market should strike the digital security balance, and those who believe governments should be more proactive in this area.

Annex A. Agenda

Second Annual Event

ENCOURAGING DIGITAL SECURITY INNOVATION

14-15 November 2019 – Plexal, Here East, London, United Kingdom

https://oe.cd/gfdsp

The OECD Global Forum on Digital Security for Prosperity

- Aims to consolidate a global network of experts and policy makers;
- Facilitates regular sharing of experiences and good practice on digital security risk and its management, mutual learning and convergence of views on core thematic issues;
- Is an international multilateral, multi-stakeholder and multidisciplinary setting for all communities of experts to meet, network and influence digital security public policy making;

The Inaugural Event of the Global Forum took place in December 2018 and focused on "Roles and responsibilities of actors: governance of digital security in organisations, and security of digital technologies". The report can be found at https://oe.cd/gfdsp.

Purpose of the event

Innovation is a key driver of digital transformation, fostering job creation and growth. However, malicious actors are also increasingly innovative, engaged in a race for new ways to launch digital security attacks against businesses, governments and individuals. To win this head to head race against malicious players, the market should provide more innovative digital security tools. Innovative digital products, including IoT and AI-enabled devices, should also be designed with enhanced security from the outset ("digital security by design").

The second annual event of the OECD Global Forum on Digital Security for Prosperity will explore how public policy can best support digital security innovation and in particular:

- Foster successful innovation ecosystems for digital security start-ups to flourish and the digital security industry to grow;
- Encourage entrepreneurs to take digital security into account from the outset in their increasingly digital-intensive and digital-dependent products, without creating unnecessary burdens for them.

The event will facilitate dialogue and exchange of good practice between all actors involved in digital innovation and digital security, feeding into OECD work, and potentially leading to analytical work, principles and international policy recommendations.

Who will participate?

Key stakeholders from governments, businesses, civil society, and academia involved in digital innovation and digital security, including:

- Public policy makers in OECD member and non-member countries, from digital security and innovation agencies, ministries of economic development, higher education and research, and sectoral regulators.

- Digital security entrepreneurs, innovators, and experts;
- Investors, venture capital firms, angel investors as well as insurance, certification companies and other interested businesses;
- Digital security accelerators, incubators, hubs;
- Other experts and actors involved in digital security innovation.

AGENDA

DAY 1: Thursday, 14 November 2019

9:00 Registration

9:30 Welcome remarks

- Andrew Wyckoff, Director for Science, Technology and Innovation, OECD
- Saj Huq, Director, London Office for Rapid Cybersecurity Advancement (LORCA)

Keynotes

- Guillaume Poupard, Director General, French Cybersecurity Agency, ANSSI, France
- Ciaran Martin, Chief Executive Officer, National Cyber Security Centre (NCSC), United Kingdom

10:30 **Coffee Break (30mn)**

11:00 **Session 1 - Strategic Initiatives for Digital Security Innovation**

What are the most important national and international initiatives being spearheaded by Governments? What are the main challenges and the most important lessons learned?

An increasing number of governments and stakeholders are adopting a strategic approach to foster a thriving, innovative, digital security industry. Speakers will share their current vision and strategic initiatives to spur digital security innovation.

Format: Panel discussion including presentations of initiatives and dialogue with the audience.

Moderator: Andrew Wyckoff, Director for Science, Technology and Innovation, OECD

Speakers*:*

- Guillaume Poupard, Director General, French Cybersecurity Agency, ANSSI, France
- Prerana Mehta, Chief of Ecosystem Development, AustCyber, Australia
- Refael Franco, Deputy Director General, Robustness, Israeli National Cyber Directorate (INCD)
- Ioannis Askoxylakis, Cybersecurity Officer, European Commission
- Chris Ensor, Deputy Director for Cyber Skills and Growth, National Cyber Security Centre (NCSC), United Kingdom

12:30 **Lunch break**

14:00 Session 2 – Opportunities and Challenges to Enable Digital Security Innovation

What are the opportunities and challenges to foster digital security innovation? How can demand and supply-side policies and initiatives stimulate digital security innovation and help develop a vibrant digital security industry?

Format: This session will be interactive and will be divided in two panels including a 30min break. Discussants and all participants will debate on the above key issues.

Moderators:

- Phil Budden, Senior Lecturer, MIT Sloan School of Management
- Katie Stebbins, President, Global Epic, Vice President of Economic Development, University of Massachusetts

Panel 1 - Supply side issues and challenges (14:00 – 15:30)

- How can entrepreneurs gain access to capital and make the best use of skills?
- How can they gain access to and use data to enhance digital security innovation?
- How can sustainable interlinkages be built between stakeholders such as academia, industry, governments, entrepreneurs and financial actors to boost digital security innovation?

Panel 2 - Demand side issues and challenges (16:00 – 17:30)

- What policies are most likely to increase demand for innovative digital security products and services?
- How can start-ups best market their products and overcome the information asymmetries that limit demand and competitiveness for new security products?

Cross-cutting questions:

- What is the role of government, business, civil society, the technical community, academia, and actors such as accelerators?
- Aside from market-driven innovation, what role does open source innovation play in this area?
- In what ways do co-operation, partnerships and information exchange facilitate digital security innovation?

Discussants:

- Entrepreneurs
  - Rayna Stamboliyska, VP Governance and Public Affairs, Yes We Hack, France
  - Tyler Sweatt, Head of Special Projects, Calypso AI, United States
  - Elissa Shevinsky, CEO, Faster Than Light
- Venture Capital
  - Kenneth Pentimonti, Principal, Paladin Capital Group
  - Naama Ben Dov, Analyst, YL Ventures
  - Niloofar Razi Howe, Senior Operating Partner, Energy Impact Partners
- Key industry representatives
  - Sebastien Rummelhardt, Head of Digital Security Red and Blue Team Department, Airbus
- Governments, accelerators & hubs, and other initiatives
  - Josh Waite, Innovation & Workforce, Atlantic Canada Opportunities Agency (ACOA), Canada

  - Ko Ozaki, Deputy Director, Cybersecurity Division, Ministry of Economy, Trade and Industry (METI), Japan
  - Grace Cassy, Co-founder, Cylon
  - Florent Kirchner, Strategic Director, SPARTA
- Civil society and academia
  - Godfrey Gaston, Director, Centre for Secure Information Technologies, Queens University Belfast

17:30 **End of Day 1 - Reception**

DAY 2: Friday, 15 November 2019

9:00 **Session 3 – International Co-operation to Enhance Digital Security Innovation**

How can stakeholders best work together and co-operate across-border to enhance digital security innovation?

While innovation increasingly occurs across borders, national innovation policy initiatives often have a territorial development dimension. Speakers will discuss how different stakeholders in different countries and regions can work together in this area.

Format: Discussion between panellists and with the audience.

Moderator: András Hlács, Vice-Chair, OECD Committee on Digital Economy Policy (CDEP)

Speakers and panellists:

- Matthew Travis, Deputy Director, Cybersecurity and Infrastructure Security Agency (CISA), United States
- Roni Zehavi, CEO, RonTali Cyber Projects, Co-founder and Former CEO, Cyberspark
- Florent Kirchner, Head of Laboratory at CEA (Commissariat à l'énergie atomique et aux énergies alternatives), Board Member of ECSO (European Cyber Security Organisation)
- Katie Stebbins, President, Global Epic, Vice President of Economic Development, University of Massachusetts

10:00 **Coffee Break**

10:30 **Session 4 – Fostering Security by Design in Digital Innovation**

How can all startups (beyond security ones) better take digital security into account from the outset in the development of innovative digital products?

Start-ups usually value time-to-market, usability and cost-effectiveness over security. They “build first, patch later” because the market rewards the “first mover advantage” behaviour. As a result, many apps and IoT devices lack basic security features. However, with digital transformation, most products and sectors become digital intensive and dependent, and digital security incidents can have nation-wide economic consequences or affect safety.

Speakers will discuss how entrepreneurs, accelerators and investors approach security: as a minor detail, sunken cost, or increasingly important trust feature? How can policies and industry standards help to mainstream security-by-design in the start-up and digital innovation ecosystem, without creating unnecessary burdens? How could digital security become a differentiating factor on the market for innovative products?

Format: Discussion among panellists and with the audience.

Moderator: John Banghart, Senior Director, Center for Cybersecurity Policy and Law

Speakers and panellists:

- Roi Yarom, Director for Economy and Growth, Israeli National Cyber Directorate (INCD)
- Javier Diéguez, Director, Basque Cybersecurity Centre
- Reiko Kondo, Director of the Office of the Director-General for Cybersecurity, Ministry of Internal Affairs and Communications (MIC), Japan
- John Chapman, Chief Information Security Officer, Dell UK Public Sector
- Chris Gibson, Executive Director, Forum of Incident Response and Security Teams (FIRST)
- Melody Patry, Advocacy Director, Access Now

12:00 Conclusion

Moderator: Audrey Plonk, Head of the Digital Economy Policy Division, OECD

Moderators will be invited to share a brief summary of their respective sessions and discuss with the audience potential areas for future work.

12:45 End of the event

https://oe.cd/gfdsp

Global Forum Sponsor

TÜV SÜD