TECH 7

ITALY 2024

JOINT DECLARATION

Rome, April 11th, 2024

AFNUM · Anitec-Assinform · bitkom · DIGITALEUROPE · ITI · JEITA · numeum · TECHNATION CA · techUK

TECH ITALY 2024 7

Summary

1. Scenario 5
1.1. Current geo-political picture 5
1.2. 2024: a year of worldwide elections 6
1.3. Strengthening economic security through digital resilience 6
1.4. Trade cooperation 7
Recommendations 8
2. New Emerging technologies 9
2.1. Digital public infrastructure 9
2.2. Artificial intelligence (AI) 10
2.2.1. Balancing competition and cooperation 11
2.2.2. Advancing the G7 Hiroshima principles 11
2.3. Quantum computing & quantum secure communications 12
2.4. 6G 13
Recommendations 14
3. Digital skills and education 16
3.1. Basic and advanced digital skills 16
3.2. Cybersecurity professionals and awareness 17
Recommendations 18
4. Cybersecurity 19
4.1. Regulatory harmonization and convergence 19
Recommendations 20
5. Digital Transformation 21
5.1. SMEs & competitiveness 21
5.2. Digital health 21
Recommendations 22
6. Digital trade and data flows 23
Recommendations 23
7. Sustainability and green transition 25
7.1. Climate change and resource efficiency 26
7.2. Supply chain and procurement 26

TECH ITALY 2024 7

1. SCENARIO

1.1. Current geo-political picture

We are arguably in the most economically transformative period in decades and cooperation between countries is key to navigating this transformation.

The year 2023 was marked by the war in Ukraine and the Middle East crisis that polarized international politics and caused heightened geopolitical tensions and energy and commodity shortages.

Trade barriers, rising protectionism and escalating international tensions are changing the long understood global order and have the potential to undermine economic growth, innovation, global development and competitiveness.

Climate change, manifested through extreme weather events, is currently disrupting trade routes and causing damage to infrastructures. This risk poses a significant threat to economic and national security and global stability.

Considering this, persistent energy security concerns are a serious threat to the global economy, increasing social, economic and political challenges for governments. New international crises (including health emergencies) could also further weaken national and international supply chains and stop production and exports, fueling global shortages.

Cybersecurity is an intricate geopolitical risk factor. Cybersecurity breaches pose a significant threat to people, organizations and national security and can cause significant harm to business continuity, public services as well as economic viability, thus undermining confidence in economic, political, and social institutions. In turn, the increasing international instability could produce significant repercussions in terms of target and effects in the cyber domain, as tool used by hostile actors to achieve their strategic objectives.

Given the extent of interaction between these geopolitical risks, the strategy to tackle them should be comprehensive. Achieving significant progress in climate transition, cybersecurity, energy security or international conflict management requires deeper collaboration and dialogue between countries and their respective industry stakeholders. Importantly, the technologies that our industry develops can provide a crucial contribution in addressing many of these challenges.

The global economic ecosystem benefits through the enhancement of international relationships among nations and the respect of the same regulatory frameworks by business and industrial partners worldwide. It is imperative to promote collaboration among countries in order to support partnerships in industry, research and development, and to avoid detrimental changes in trade policies.

The new economic landscape requires a transparent level playing field, one where all economic actors play by the same rules and where the rules are applied evenly and equally, regardless of where companies are based.

Open trade flow is key to fostering growth globally, and it is in the interest of all to ensure an effective, business-friendly customs process for importers and global exporters.

Embracing the international rules-based order and utilizing international standards is crucial to fostering the development of advanced technologies. This approach will provide access to expertise and innovations from diverse corners of the globe, allowing businesses to tap into cross-border resources and data and improving security and trust.

Additionally, it will instill confidence among users in terms of data protection and privacy, fostering a conducive environment for more equitable economic and social development.

1.2. 2024: a year of worldwide elections

In 2024, 62 countries with a combined population of four billion will hold elections. This is just under half of the whole of humanity: from the EU, the United States to India, and the U.K., for presidential, legislative or administrative elections, 16 African, 11 Asian, 22 European, 9 American and 4 countries in Oceania will vote.

Uncertain outcomes of different elections, together with current geopolitical instability, wars and crises, risk creating increased unpredictability for businesses, global trade, and economic security will have a significant influence on the economic and the political scenarios.

In this global scenario, G7 countries and their allies should further increase their digital and economic innovation and resilience through collaboration. Given complex and highly integrated global supply chains, this cannot be achieved in isolation, but only through increased cooperation among partners.

The future of our society is more closely linked than ever to the future of its industry and especially its ability to demonstrate digital and technological leadership.

1.3. Strengthening economic security through digital resilience

Previous G7 Presidencies played a crucial role in driving forward an international economic security agenda. Therefore, it is essential to maintain momentum and continue this work.

We urge the G7 to ensure that cooperation with each other and with like-minded partners is implemented before, during, and after the development of economic security policies.

We also reiterate the importance of resilient supply chains. Expanding trade collaboration through new commitments and enhanced enforcement of existing rules is key to ensure the free flow of data and combat challenges related to forced localization that undermine global supply chain resilience. Removing unjustified tariffs and non-tariff barriers with like-minded partners also promotes mutually beneficial supply chain integration by making it easier for companies to work, manufacture, and do business in the other parties' markets; also, cooperation on critical technologies is a must to ensure digital resilience and economic security.

In order to secure diverse trading partners, G7 countries should lead the discussion to maintain and strengthen the free trade system on a regular basis, for instance, expand the

scope of goods and economies covered by the Information Technology Agreement of the World Trade Organization (hereinafter, WTO-ITA) and its member countries and regions.

Moreover, aligning G7 export controls would be a win-win option in order to ensure these controls are as effective as possible and avoid the risks to economic harm that can stem from unilateral export controls.

Digital resilience also includes actions empowering private and public organizations to manage their own digital risks. Important policy actions include, implementing measures required to protect communication networks and information systems, their data, users, and other relevant individuals from events or activities that can harm the aforementioned or adversely affect them.

1.4. Trade cooperation

Digital trade and trade in technology products affects almost every business and its customers, not just large corporations or technology companies, which is why it is so important for governments to enact trade-enabling policy approaches. Micro, small, and medium-sized enterprises (MSMEs) in every sector—from medical professionals and services providers to farmers and manufacturers—rely on data flows and digital services to reach customers, conduct R&D, maintain supply chains, and otherwise facilitate daily operations. Digital trade enables companies to be "born global" in that they can reach customers in a global marketplace from day one and provides access to technologies that facilitate trade and enhance productivity, such as the digitalization of business operations and customs procedures, that benefit all exporters.

This trade cooperation underpins future innovation and economic growth and contributes to many of the other goals listed in this document; it is also a major part of the modern economy. UNCTAD estimates that global digital trade totaled nearly 4 trillion $ last year, which was more than half of all services exports.

G7 countries should deepen cooperation to advance digital trade and trade in technology products this year by pursuing new international agreements and collectively addressing barriers to trade in third markets. In particular, G7 countries should pursue outcomes in the World Trade Organization, including through agreement on a robust and meaningful outcome in the Joint Initiative on E-commerce. These negotiations offer a unique opportunity to help realize the promise of cross-border access to technology and the trusted movement of data for all economic sectors and across regions. To enhance certainty and economic opportunity, the agreement should aim to achieve high standard provisions ensuring data flows across borders. A permanent moratorium on customs duties on electronic transmissions - including electronically transmitted contents, non-discrimination of digital products, prohibition of disclosure or transfer of source code or algorithms, and disciplining discriminatory data localization policies, in particular, the requirement to install computer-related equipment within the country- has to be provided as a condition for conducting

business. The agreement should respect the right to regulate where necessary and be guided by principles of non-discrimination, transparency, and interoperability among legal frameworks.

Also, G7 countries should lead the discussion of further expanding the product coverage, membership countries and regions for WTO-ITA, which plays a significant role in maintaining and continuing negotiations on a plurilateral basis, given the difficulty of reaching an agreement among all WTO Members.

Recommendations

- G7 countries and their allies should further increase their digital and economic resilience and collaboration. Given complex and highly integrated global supply chains, this cannot be achieved in isolation: only through increased cooperation among partners we can achieve significant progress in climate transition, cyber security, energy security or international conflict management.
- G7 countries should deepen cooperation to advance digital trade and trade in technology products this year by pursuing new international agreements and collectively addressing barriers to trade in third markets.
- G7 countries should pursue tangible outcomes in the World Trade Organization, including through agreement on a robust and meaningful outcome in the Joint Initiative on E-commerce.

2. NEW EMERGING TECHNOLOGIES

Digital transformation supports continued social and economic prosperity of our countries in the current scenario.

We, the Tech7, ask the G7 to recognize the role of digital technologies into maximizing digital transformation, digital trust, and economic security and the importance of regulatory harmonization in support of innovation; in particular, we believe that G7 countries should encourage investments into key technologies such as AI, cybersecurity, quantum technologies, cloud computing, data centers, 6G, space technologies and other technologies that enable and extend the benefits of the internet and digital innovation.

Therefore, research and innovation should be a strategic priority.

Each G7 country should strive to mutually align on strategies for advancing the development and implementation of emerging technologies that considers multiple components - research, industry, education, skills, and economic issues. G7 countries must also advance efforts to increase information sharing and jointly collaborate to meet both individual and shared goals. Establishing digital trust will also be important as G7 countries balance the need for the free flow of data to advance these new and emerging technologies against challenges relating to privacy, security and data protection. It is thus important for G7 countries to utilize the Data Free Flow with Trust workstream to agree upon an international framework for digital trust.

Given that "96% of commercial code contains open source" (Synopsis report '23) and for every 10% increase in open-source contribution boosts GDP by 0,4-0,6% (EU report '21), further collaboration across the open-source ecosystem is vital to both economic growth, system and data interoperability as well as driving open innovation.

2.1. Digital public infrastructure

Digital Public Infrastructure (DPI) is an emerging policy trend in several key forums, including the G20 and the United Nations. Governments seek to harness DPI to reshape their digital economies and drive progress on Sustainable Development Goals, including financial and digital inclusion.

Rising interest in DPI has also highlighted the importance of developing strong safeguards to curb government overreach, protect consumers and citizens, and enable private sector innovation and competitive markets. Absent safeguards, the rollout of DPI potentially risks crowding out private sector players and could generate new privacy risks to citizens.

With the G20 recognizing the need for safeguards and the United Nations leading a DPI safeguards initiative, the G7 has a unique opportunity to shape the debate by forming its own high-level position on DPI safeguards, which should emphasize strong principles that preserve good governance and market disciplines.

On developing national DPI strategies, we suggest the G7 countries plan their digital transformation, measure the impact of digital public infrastructure and track digital

transformation projects in a coordinated way: exchange of best practices, development of open standards and sharing track of KPIs would be welcomed and will help the process. The G7 should also request the OECD to study and develop a position on DPI safeguards, drawing on its long history and contributions to corporate governance for state-owned enterprises as well as its good practice principles for public service design and delivery.

2.2. Artificial intelligence (AI)

The rapid development of artificial intelligence (AI) marks a pivotal moment in human history, offering unparalleled opportunities for progress and innovation across industries and societies. As we enter this technological revolution, it is crucial to recognize the continued transformative potential of AI and its profound impact on global productivity, development and innovation which includes enhancing human creativity and accelerating scientific discovery.

A pro-innovation policy framework in AI that supports the deployment of AI models to the benefit of citizens and consumers is critical. Countries should, therefore, continue to pursue a risk-based approach to regulation to ensure that AI can deliver for citizens, whilst respecting their fundamental rights.

Amidst the vast potential of AI innovation, there lies a pressing need for international collaboration, transparency, accountability, and alignment. AI is developed across a global ecosystem, including a significant open-source component, with value chains that are integrated around the world. No single nation can tackle the challenges and opportunities presented by AI in isolation. It is imperative for the international community to develop an interoperable risk-based and consensus-driven approach to AI governance that enables responsible AI practices to scale globally and facilitates trade and wider adoption for the benefit of humanity. Furthermore, given the rapid development of AI, it is crucial to prioritize the development of AI governance and policy tools, that can be flexibly adapted and reflected according to technologies being innovated.

To that end, any national governance approach should be based on international standards, where they exist, in line with WTO principles. We urge the G7 to uphold the advancements made in industry-led international standardization, in particular through ISO and IEC and other globally relevant standards including those developed by 3GPP."

We urge the G7 to uphold the advancements made in private sector-led international open standardization, particularly through bodies like ISO, IEC or 3GPP, while adhering to WTO principles for international standard setting.[1]

Our goal should be to foster a worldwide landscape for the development and utilization of safe, secure, and trustworthy AI, where adherence to policy and regulatory standards, as well as interoperability across various implementation frameworks, can be achieved without

[1] WTO | Principles for the Development of International Standards, Guides and Recommendations

stifling innovation and utilization. As a concrete step in support of this goal, G7 countries could support a joint roadmap on the development of shared standards and, in case of development and recognition of international standards, in trade agreements.

2.2.1. Balancing competition and cooperation

Finding the balance between global competition and cooperation is paramount in harnessing the full potential of AI. Encouraging international collaboration and convergence to spearhead transborder AI projects aimed at addressing global challenges is essential for fostering innovation and sustainable development. As a concrete step in support of this goal, G7 countries should consider working with the Global Partnership on AI – a G7 founded initiative - to establish intergovernmental AI taskforces on shared international challenges. For example: G7 countries should support the development of international standards for public sector datasets to facilitate the use of interoperable, large-scale datasets for beneficial AI applications.

2.2.2. Advancing the G7 Hiroshima principles

In the pursuit of AI advancement for the global good, establishing a set of principles to guide the development and deployment of the most advanced AI systems is imperative. Building upon the groundwork laid by initiatives like the G7 Hiroshima Principles, strengthening dialogue with industry stakeholders is essential to ensure the practical applicability and feasibility of proposed frameworks.

We believe that the G7 Hiroshima initiative was a significant first step to fostering consensus on a set of baselines guiding principles important to consider in the context of the most advanced AI systems. However, we also believe the G7 can continue to take steps to update, refine, when needed, and raise awareness on the guiding principles and encourage their implementation, both within the G7 across industry and research institutions, and potentially beyond.

Continuing dialogue and partnership with industry and with multilateral organizations like the OECD will be crucial to achieve these objectives.

Most importantly, the Hiroshima AI initiative should facilitate common understandings between countries, including developing countries and emerging economies, of key terms and concepts, to ensure compatibility and, as much as possible, alignment between the growing number of regional and national frameworks for AI governance. It is important to pursue a common understanding across nations of key definitions and shared taxonomies, such as the concept of 'advanced AI systems,' and foundational issues to effective governance such as risk thresholds, evaluation, benchmarks, fairness and bias and privacy.

Standards play a vital role in defining and clarifying key terms, practices, and taxonomies in actionable ways for businesses everywhere, helping support the goal that governance

approaches should be interoperable. The G7 should leverage international standards in order to encourage global trade and cooperation.

The G7 can also act as a forum for like-minded partners and stakeholders to discuss key AI issues worthy of being brought to the consideration of international standards bodies.

Finally, the principles must be tailored to each stakeholder's role in the complex AI value chain; recognizing the diverse roles within the AI value chain is essential. Tailoring the application of principles accordingly would enhance their effectiveness in promoting responsible AI governance and innovation.

2.3. Quantum computing & quantum secure communications

Quantum computing is another area where G7 countries should work together to ensure that the technology can be adopted successfully, and that challenges are addressed. For example, mutual recognition of existing and to-be-built computing infrastructure, streamlining supply chains and facilitating common access to computing resources will be key to supporting cooperation and research across economic sectors from health to financial services; together with the necessary specified know-how to develop dedicated applications it will represent a competitive advantage.

Furthermore, a highly focused education plan is pivotal to the growth of competitiveness in this area, considering that new skills as Quantum Scientist, Quantum Engineer, Quantum Developer are needed.

On the other hand, Quantum secure communications are already under development and application.

Quantum Key Distribution (QKD), which allows to transfer a cryptographic key with the guarantee of confidentiality, and Quantum Random Number Generation (QRNG), which helps making robust cryptographic keys through the generation of random numbers, are two quantum technologies with a high level of maturity which are able to create solutions of the highest level of security, even superior to the capabilities of the quantum computer.

Moreover, there is great interest in Post Quantum Cryptography (PQC) from National authorities[2], as well as the European Union Agency for Cybersecurity (ENISA)[3] have published reports on preparing for the implementation and deployment of PQC. The US Cybersecurity and Infrastructure Security Agency (CISA) established a PQC Initiative to unify and drive agency efforts to address potential threats posed by quantum computing.[4] For an effective

---

[2] https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/Quantum_Positionspapier.pdf?__blob=publicationFile&v=4

[3] Post-Quantum Cryptography: Current state and quantum mitigation — ENISA (europa.eu)

[4] https://www.cisa.gov/news-events/news/cisa-announces-post-quantum-cryptography-initiative

transition towards PQC, efforts should be synchronized ensuring the roadmaps are aligned, with concrete timelines for every transition step.[5]

PQC and QKD could also be combined to obtain solutions with different levels of flexibility and security suitable for different use cases and contexts: for example, using QKD for physical layer security and PQC for higher application levels and for authentication.

G7 countries should strengthen cooperation in this field, especially around the support for international standards on post-quantum encryption and on the creation of a geographic network for the distribution of cryptographic keys as a security service and should support the development and mutual recognition of trustworthy and of quantum proofed infrastructures.

A tailored approach is in fact necessary, since a one-size-fits-all solution will not work. When addressing technologies with different opportunities & risks, and at different stages of development, public-private sector cooperation is vital. Investment, building competence, and upskilling in critical tech can take us one step closer to the desired goal.

2.4. 6G

A prosperous digital economy is built on trusted digital infrastructure that enables digitization of all industry sectors. Accelerated deployment and adoption of 5G is also a critical steppingstone on the journey to 5G Advanced and then on to 6G once all the standards will be consolidated.

Advanced connectivity achievable through the development of 6G technology paves the way to new and promising scenarios for all production sectors, and for the whole society. 5G technology has already opened new frontiers to improve business productivity, reduce the environmental impact of human activities, increase safety for people, provide society with more efficient services, and allow us to consider technological advances enabled by the network.

Digital services and skills enabled by advanced connectivity also play an important role in addressing socioeconomic inequalities and promoting gender inclusion and in allowing the most disadvantaged social categories to freely access information and services related to education, improve health and welfare, as well as better job conditions.

6G is expected in the 2030 timeframe, through even higher technical performances, wider adaptability to different application areas, such as virtual human twins and autonomous mobility, and integration of new features, will further develop these opportunities, with an extraordinarily positive impact for the global community. Therefore, G7 countries should promote the development of, not only technologies related to 6G, but also application that is expected to be realized in 6G.

[5] https://digital-strategy.ec.europa.eu/en/library/white-paper-how-master-europes-digital-infrastructure-needs

G7 countries should aspire for global technology leadership in 6G and to this end have already taken steps in national programs that can be future leveraged by well-coordinated international cooperation.

In particular:

- build on progress such as the EU-US TTC[6], EU-Japan DPA[7], and Principles for 6G[8];
- increase international cooperation in research and development activities, as well as on international 6G standards development aligned with WTO principles for international standardization, which includes encouraging and facilitating broader collaboration between industry, research organizations and standardization bodies;
- remove any potential regulatory barrier to the adoption of new network technologies;
- enhance common development models, in particular open source, that support the broadest collaboration among all market operators in the digital communication and services sectors;
- promote the security and trust of network infrastructure and communications and data traversing networks regardless of underlying technology.

Recommendations

- Moving from G7 Hiroshima initiative, G7 should agree to develop a responsible governance with interoperability, which will help to foster AI awareness and will balance competition and cooperation.
- Promote AI awareness and competence, also in the public sector to enhance its internal processes and policies through the responsible use of data and AI technology.
- On developing national Digital Public Infrastructure strategies, we suggest the G7 countries plan their digital transformation, measure the impact of digital public infrastructure and track digital transformation projects in a coordinated way.
- We believe that G7 countries should encourage investments into key technologies such as AI, cybersecurity, quantum technologies, cloud computing, data centers, 6G, space technologies and other technologies that enable and extend the benefits of the internet and digital innovation and to promote the alignment of the related regulations and the development and use of international standards.
- G7 Countries should promote the sharing of both computing and network quantum infrastructures.
- G7 Countries should promote the use of enabling technologies to safeguard welfare systems.

[6] 6G outlook | Shaping Europe's digital future (europa.eu)

[7] 最終版-jp-eu-digital-partnership-clean-final-docx.pdf (europa.eu)

[8] Joint Statement Endorsing Principles for 6G: Secure, Open, and Resilient by Design | The White House

- G7 countries should aspire for global technology leadership in 6G and to this end have already taken steps in national programs that can be future leveraged by well-coordinated international cooperation. In the development of 6G, it is necessary to promote the development of technologies and applications, such as virtual human twins and autonomous mobility, that will be realized on 6G in parallel.

TECH 7 ITALY 2024

3. DIGITAL SKILLS AND EDUCATION

3.1. Basic and advanced digital skills

A robust digital economy, fueled by citizens equipped with both basic and advanced digital skills, is crucial for fostering innovation, employment, and competitiveness. Basic digital skills are the backbone for the social and economic advancement of nations. Achieving this goal requires systemic policies that specifically target vulnerable and underrepresented groups, including young and older people and minorities and enabling learning opportunities for continuous upskilling and reskilling.

Also, since skills are important to all our economies, proper migration policies can help respond to the growing demand for highly skilled digital professionals and mirror the fact that a one percent increase in migration would result in a two percent GDP growth for the receiving countries[9] .

It is essential that digital skills are developed to address both the skill mismatch typical of the social and labour transition, and to become a proficient digital citizen to best utilize the benefits that new technologies provide. Digital education shall be considered the starting point for this virtuous path and a pre-condition for democratic citizenship.

Collaboration among G7 countries will be important to:

- promote digital literacy and citizenship;
- bridge the digital skills gap;
- develop AI literacy, referring to understanding the fundamentals of AI, including its application, implications, and limitations;
- offer the most vulnerable and disadvantaged all the opportunities of digitalization;
- define common tools to acquire and recognize the acquisition of the skills necessary for social life and the labour market.

Considering the increasingly pervasive diffusion of digital technologies is shaping a new labour market, influencing the demand for specialized skills necessary for the growth of the production system.

Digital training and education tools (Edtech) shall be accessible to all and validated technically and pedagogically to achieve relevant impact for learners. Continuous orientation and adoption of digital tools in formal and informal education, collaboration between academia and private companies to integrate high-profile skills into university (and doctoral) programs, and support for R&D activities are necessary actions to fully exploit the opportunities offered by digital transformation.

It is important that we do not consider digital skills and training as a school age phenomenon. The commitment to training must be lifelong.

[9] Source: The International Monetary Fund

Easily accessible digital training and education programs and hands-on learning opportunities, continuous orientation and digital education in schools, collaboration between academia and private companies to integrate high-profile skills into university (and doctoral) programs, and support for R&D activities are necessary start point actions to fully exploit the opportunities offered by the digital transformation. We also want to encourage better recognition and reskilling validation of industry-led certification to make labour markets more inclusive and aligned with market reality.

This must continue through a citizen's life.

3.2. Cybersecurity professionals and awareness

Similarly, in the area of cybersecurity, skills play a central role in safeguarding sensitive data and responding to significant cybersecurity incidents. While cybersecurity working for public, private and third sector are called upon to develop and implement strategies to protect systems, networks and data, it is also important that citizens are aware of and taking steps to increase cybersecurity awareness.

This is why in cybersecurity skills are more than a priority. Security depends on:

- the protection of sensitive information and the prevention of privacy breaches;
- the security of critical infrastructure in core sectors such as energy, TLC, healthcare, finance and utilities and in essential and important entities, services and sectors;
- the prevention of detection and response to cyber-attacks that can cause significant damage to organizations and their operations;
- the regulatory compliance of organizations based on international security standards and mutual recognition of standards and certification between allies;
- the management of increasingly advanced emerging threats;
- the coordination among institutions and among polices at national level and the enhancement of international cooperation including private sector.

The success of the digital economy, safety and prosperity of citizens, and the achievement of various objectives in areas of AI, quantum, etc., will all require a strong and sustained focus on cybersecurity.

Investing in cybersecurity skills, especially to professional level, will help to provide an effective line of defense against cyber-attacks and malicious actors. Digital literacy, basic and advanced training, continuous updating of knowledge, collaboration between experts, and the promotion of ambitious public-private partnerships, and the exchange of information between the public and private sectors are essential to ensure information security in the digital society.

When addressing the workforce issue in cybersecurity, attracting new talent is as important as re-skilling and upskilling professionals.

To attract new talent, G7 countries should lead the way by joining forces with the private sector and academia in this shared challenge to develop a globally scalable youth cyber education pathway. Harmonizing the way cybersecurity roles are viewed globally can help make these roles more attractive, ensure mobility of professionals and improve our coordination ability during incidents. This is primarily achieved by creating alignment, starting from the G7, on key concepts. The NICE framework in the US[10] is a good example of harmonizing the descriptions of cybersecurity work and workers regardless of where or for whom the work is performed.

It would be impactful for G7 countries to support the establishment of government-sponsored national cyber academies. There are not enough cybersecurity professionals and this talent gap is only widening. Closing this gap at scale requires sustained investment and support from governments and private sector stakeholders.

To ensure preparedness of employees that work on critical functions, public and private sectors need to create upskilling pathways in the learning management system. With governments being often targets of sophisticated attacks, it is important that governmental officials are constantly upskilled to be able to defend against such attacks. G7 countries should work closely in this regard with private companies that already offer trainings to provide professionals the opportunity to deepen their cyber skillset in key future growth areas.

Recommendations

- G7 countries should track the most on-demand digitalization level in various sectors, focusing on continuous orientation, streamlining educational paths, and monitoring the gaps to be addressed.
- G7 countries should invest in programs to support digital education of population and to train, attract, and retain talent in the ICT sector.
- Collaboration among G7 countries will be important to bridge the digital skills gap, which affects both social life and the labour market, promote STEM education and reduce gender gap.
- G7 countries should lead the way by joining forces with the private sector and academia to develop global education programs focused on emerging technologies such as AI, cybersecurity, quantum technologies, 6G and facilitate the adoption of new digital solutions in companies by fostering "on-the-job" continuing training through initiatives that promote the adoption of frontier technologies.

[10] https://niccs.cisa.gov/workforce-development/nice-framework

4. CYBERSECURITY

Cybersecurity is an area where governments have a huge responsibility in ensuring that organizations of all sizes have access to and use state-of-the art technologies crucial to their cybersecurity and cyber resilience. Cloud computing and the latest developments in artificial intelligence can significantly boost organizations' ability to successfully defend their systems and G7 governments should promote the development and adoption of these technologies.

Ensuring convergence is particularly crucial for effectively bolstering defenses and prevention. Given the global nature of cyber threats, it is imperative for G7 countries to foster policies that advance interoperable approaches to cybersecurity, particularly in key areas such as incident reporting, product cybersecurity, and vulnerability management. Such collaboration is crucial for enhancing global cybersecurity, benefiting both the private sector and government entities, which often face sophisticated threats with limited resources and time. More specifically, G7 countries should increase cooperation on cyber threat information sharing, securing networks, cloud services and digital infrastructure.

Additionally, it is crucial for G7 countries to integrate cybersecurity considerations into every phase of regulatory development and implementation. Cybersecurity considerations can no longer be an after-the-fact consideration or separated from the substance of regulatory proposals. Rather, it should be an integral part of the assessment at every stage of the legislative process. This is to ensure that in the efforts of complying with other regulatory frameworks, cybersecurity is not compromised or de-prioritized.

4.1. Regulatory harmonization and convergence

Our global digital ecosystem is becoming more interconnected than ever before. Organizations are regularly operating across geographies, jurisdictions, and regulatory schemes. The further apart regulatory environments are in different countries, the harder it is to secure systems and respond to incidents. During an incident involving multiple jurisdictions, the varied regulatory environment takes time and energy away from response. Given the impact such attacks can have on the security of our people and our economies, the G7 countries should follow this issue very closely.

One way to address the fragmented regulatory ecosystem is through mutual recognition agreements among like-minded countries and the use of globally recognized standards. Standardization plays a fundamental role in the harmonization effort. As much as possible, rules should take into account existing standards, such as ISO/IEC that offer guidance on information security, cybersecurity and privacy protection.

The tech industry is doing its part, but governments have an important role to play as well. This includes cooperation and dialogue on cybersecurity threats, mitigation measures, and policy approaches. It also means ensuring that attention is paid to threats across the entire hardware-software stack — from network infrastructure and cloud to devices, operating systems, and applications.

Importantly, convergence also requires a fundamentally new approach to regulation more generally. Cybersecurity considerations cannot be an after-thought or "add-on" to regulatory initiatives; rather, they must be central to the development of all regulatory proposals and impact assessments at the outset. This requires that governments adopt a mindset of "cyber-proofing" ensuring that relevant cybersecurity experts and agencies are properly equipped and consulted in the development of laws and regulations affecting the technology sector.

We ask G7 countries to support the mapping capabilities across countries, identify common gaps in areas like security awareness and compliance.

Recommendations

- G7 countries should foster policies that advance interoperable approaches to cybersecurity including the development and use of international standards.
- G7 countries should increase cooperation on cyber threat information sharing, securing networks, cloud services and digital infrastructure.
- It is crucial for G7 countries to integrate cybersecurity considerations into every phase of regulatory development and implementation and to harmonize regulations.

5. DIGITAL TRANSFORMATION

5.1. SMEs & competitiveness

Digitalization is hugely revolutionizing every sector of our society. Among the digitalization applications, online marketplaces can significantly enhance the competitiveness of SMEs by providing global reach with a platform to reach a global audience; this helps to extend their customer base beyond local or regional boundaries, allowing them to tap into new markets and customer segments that might be otherwise inaccessible.

Online marketplaces offer a cost-effective way to promote products and services. The marketplace itself often invests in marketing and traffic generation, reducing the individual SME's marketing and advertising expenses.

Online marketplaces also provide a ready-made infrastructure, including payment gateways and logistics support, saving SMEs time and resources. Online marketplaces often provide analytics tools that help SMEs understand customer behavior, preferences, and market trends. This data can be invaluable for making informed business decisions and tailoring products or services to meet customer demands. Being part of an online marketplace allows SMEs to observe and learn from competitors. It also opens up possibilities for collaboration with other businesses on the platform, fostering a network that can lead to partnerships and mutually beneficial relationships. Online marketplaces often embrace new technologies and trends quickly. SMEs within these marketplaces can benefit from innovations, stay competitive, and adapt to changing consumer preferences more efficiently. Finally, online marketplaces may assist SMEs in navigating complex regulatory environments. They often have mechanisms in place to ensure sellers comply with legal requirements, easing the burden on SMEs and ensuring a level playing field.

On the other hand, the widespread use of digital solutions increases the cyber security challenges and vulnerabilities faced by SMEs, which usually lack of cyber skills, awareness and organizational cybersecurity culture. Cyber-attacks could seriously impact SMEs competitiveness and disrupt the entire value-chain. In this vein, SMEs need to be supported to improve their cybersecurity posture, identify key cyber security risks and enhance cybersecurity awareness, with regular security assessment, resources and training. Promoting and implementing cybersecurity measures for SMEs through public-private collaboration could foster their productivity, processes and related infrastructure, and the efficiency of the industry as a whole.

5.2. Digital health

Digital solutions can provide the means to support the transformation of health systems and ensure that patients have access to improved healthcare. Digital technologies (such as AI, virtual human twins and wearables) and the (re)use of data have immense potential to improve patient care, manage health systems, develop public health policies, and facilitate health R&I. To support these developments, policy measures should enhance the use of data and new enabling technologies in health systems and health R&I, improve digital health literacy and skills, increase trust through multi-stakeholder collaborations, and ensure that all related

funding and allocated resources advance digital transformation in healthcare. In terms of regulatory requirements, there are needs to be consistent: implementation of privacy, data protection and cybersecurity requirements, utilizing to the fullest extent possible international standards to improve interoperability, effective IP protection to incentivize R&I in digital health, recognition of the ubiquitous, cross-border and international data flow needs of digital health ecosystems.

Recommendations

- G7 countries should support digital sector not only as an enabler and growth factor for economic actors, but also because it brings positive impacts on social welfare, public services, and the environment.
- G7 countries should foster digital transformation of SMEs by simplifying and better explaining regulations which will help to foster their productivity.
- G7 policies and measures on digital health should encompasses strong funding programs which give special attention to cloud-based and software driven ICT solutions.

6. DIGITAL TRADE AND DATA FLOWS

Data flows are critical to global priorities including economic growth, climate change, cybersecurity modern economies, supply chains, and public health. We urge the G7 countries to strengthen its commitment to a comprehensive data strategy that relentlessly promotes and enables secure and responsible data flows and maintains high data protection standards and bolsters innovation.

This includes accelerating work on the Data Free Flows with Trust (DFFT) initiative to drive greater alignment and interoperability across different national data protection frameworks, maintaining high data security standards, and moving towards a more flexible, risk-based approach to the use of data transfer mechanisms and certifications taking into account existing regulations such as GDPR.

The seamless movement of data is the backbone of trade, research, and development (R&D), innovation, and operational activities across various sectors. It sustains the advancement and operation of the products and services crucial to our everyday lives[11].

Achieving a clear global approach to trusted data flows is also critical to the growth of AI and other emerging technologies. Imposing unfounded limitations on data flows, including any form of data localization, should be avoided as they tend to stifle innovation, impede cross-border collaboration, and obstruct the seamless flow of information, undermining the potential for global connectivity and shared advancements.

Data, when harnessed responsibly, holds the transformative power to drive positive societal and economic shifts. It serves as a catalyst for innovation, unlocking boundless potential for progress. To fully realize this potential, it's imperative for the G7 countries to show continued leadership in advancing safe, secure and interoperable data frameworks, respectful of IP rights and trade secrets at a global level.

Recommendations

- We urge the G7 countries to build on Data Free Flows with Trust (DFFT) and continue to work towards a comprehensive global data strategy built on evidence-based criteria and internationally recognized risk-based standards to establish trustworthiness between governments and industry partners.
- G7 countries should also develop shared principles for trusted digital infrastructure such as cloud computing, facilitating trust-based cross border data flows, and promoting interoperable data governance systems.
- The G7 countries should prioritize the implementation of the OECD Declaration on Government Access to Personal Data Held by Private Sector Entities, considering that

[11] For example DIGITALEUROPE's Data flows and the Digital Decade Study

achieving a clear approach to trusted data flows is also critical to the growth of AI, other emerging technologies, trade and economic security.

- G7 countries should address the issue of data interoperability in a coordinated manner by promoting the creation and implementation of interoperability codes/models, with a particular emphasis on key sectors such as healthcare and social policies. Interoperability is in fact a crucial element to ensure that data can flow between different state entities, simplifying the exchange of information at the cross-border level and creating a fertile ground for innovative solutions.

7. SUSTAINABILITY AND GREEN TRANSITION

Climate change and environmental degradation are increasingly affecting people's lives, disrupting economies, and transforming ecosystems. Technology will play a key role in helping address these issues.

Technological investments and digital solutions can foster new economic opportunities and ensure a sustainable green transition. This green transition will create a climate-resilient economy, one that can withstand or recover quickly from climate impacts in the short and long term.

Countries should have ambitious goals on sustainability and on the promotion of a green transition. Countries around the world are promoting the transition to a green economy with a wide range of policy and regulatory interventions in the climate, energy, and environmental fields. It is thus crucial to aim for alignment of these objectives at the international level to help companies navigate in a less burdensome and more investment-friendly business environment.

Policy approaches should be harmonized to ensure competitiveness and developed through a collaborative approach with all stakeholders involved in the transition. It is particularly important to incentivize the green transition (e.g. UN's OSPOs for good[12]) by focusing on attainable results, using a technology-neutral approach.

Critical raw materials are indispensable for industry and the development of clean technologies, and excessive dependencies on third countries can create supply security risks. Without lithium and rare earths, there will be no energy transition (e.g., wind farms), electric mobility (e.g., batteries), digitization (e.g., semiconductors), and industry 4.0, but also no expansion of infrastructure and no effective defense industry. G7 countries should cooperate with each other and work with industry to minimize these risks, boost supply chain resilience and work on resource efficiency.

The G7 countries should acknowledge the significance of digital technologies, especially in fostering decarbonization and circularity through aspects like connectivity, sustainable networks, digital infrastructure, AI/machine learning, product passports, software-as-a-service and cross-border and cloud-based services.

G7 countries should increase investment in R&D funding programs, facilitating greater cross-border cooperation and participation by expanding funding resources and involving more stakeholders and organizations.

Some countries lack the necessary skills, connectivity infrastructure, and equipment to effectively deploy and utilize such technology for adaptation efforts. Digital solutions for risk management and disaster prevention should be incentivized to provide aid and support to countries most at risk of climate change.

[12] https://www.un.org/techenvoy/content/ospos-good-2024

7.1. Climate change and resource efficiency

Digital technologies are pivotal to accelerating climate action, helping reduce emissions in the energy, transportation, and manufacturing sectors. Innovation and digital solutions are essential to achieve the 2015 Paris Agreement's goals, as well as to decouple resource consumption needs.

With the potential of increasing energy needs for emerging technologies, it is ever more important that companies are encouraged and incentivized to use renewable energy sources for operations. Technology companies have already started the transition to renewable energy use, paving the way to a new vision on energy and material consumption: consuming more renewable energy and investing more in resource efficiency.

Governments should be able to finance and promote the greening of the digital sector through policies that facilitate the acceleration of a pragmatic energy transition and support businesses to implement new renewable goals.

The next step would be bringing digital and sustainability goals together by integrating climate and circularity considerations into digital policies, sustainably addressing the digital divide, and strategically incorporating digital technologies into green sectoral strategies to exploit their enabling potential.

7.2. Supply chain and procurement

Procurement can play an important role in boosting demand for sustainable solutions. To tap into this potential, G7 countries should encompass a broader spectrum of awarding criteria, such as sustainability, accessibility, and environmental impact into procurement decisions, which today are often dominated purely by price considerations.

G7 countries should commit to use purchasing preferences for socially and environmentally preferable goods or services which have a lesser or reduced impact on the life cycle when compared with competing goods or services serving the same purpose.

Technology can boost transparency throughout the supply chain to inform business decisions on supply chain environmental sustainability. This would help designers in generating more sustainable products that meet customer needs while reducing product environmental impact.

In this scenario, G7 countries should look to consensus-based international standards and ecolabels to identify these goods and services and strengthen cooperation with each other and other like-minded partners to develop aligned and coordinated approaches to prevent regulatory fragmentation.

Recommendations

- G7 countries should facilitate the development of large-scale pilots on digital traceability of products, building on existing technical solutions.

- G7 countries should adopt green digital strategies, at least, across the key economic sectors.
- G7 countries should acknowledge the significance of digital technologies, especially in fostering decarbonization and circularity.
- G7 countries should ensure citizens access to high-quality communication services and digital infrastructure, regardless of geographical location and social and economic conditions.
- G7 Governments should be able to finance and promote the greening of the digital sector.
- G7 countries should promote the creation of concrete relationships and investment plans to bridge the digital divide and especially the AI divide between Global North and Global South. It is important that the Global South fully benefits from digital transformation, as AI applications hold the potential to effectively address economic and social challenges.

Notes:

Notes:

Notes:

TECH ITALY 2024 7

TECH 7

ITALY 2024

Created by:

AFNUM Alliance Française des Industries du Numérique

Anitec-Assinform

bitkom

DIGITALEUROPE

ITI

JEITA

numeum

TECHNATION CA

techUK