DIGITALEUROPE

23 JANUARY 2023

DIGITALEUROPE's recommendations for a more ambitious EU Cyber Defence Policy

Executive Summary

DIGITALEUROPE welcomes the Joint Communication on an EU Cyber Defence policy, part of the Security and Defence package published on 10 November 2022.[1] Cyberattacks at the hands of state and non-state actors have increased exponentially in the past few years, having had serious political, financial, and economic consequences across Europe and beyond.

Cyber defence entered a new era on 24 February 2022. Russia's physical and digital attacks against Ukraine marked the age of the hybrid war. It was the first time that two cyber-powers fought each other online in wartime.[2] Cyberattacks targeting the critical infrastructure of all nation-states increased by 20% in 2022, up to a total of 40% compared to previous years.[3] Cyberattacks are becoming a threat to life itself as hospitals find themselves more and more under increasing attacks. A recent study surveying more than 600 healthcare facilities found that mortality rates increased by 25% following a ransomware attack.[4] According to data from the CyberPeace Institute, the average cyberattack on a healthcare system leads to 19 days of patient care loss. In one case, a cyberattack led to around four months of disrupted medical care.[5]

Cyberattacks have significant consequences in other areas such as banking, defence, energy and media. Most recently, hackers have disrupted access to the websites of Denmark's central bank and seven private banks in the country.[6] Still in Denmark, the train network saw a major breakdown as a result

[1] European Commission (2022), *Joint Communication to the European Parliament and the Council: EU Policy on Cyber Defence*, <https://www.eeas.europa.eu/sites/default/files/documents/Comm_cyber%20defence.pdf>.
[2] The Economist (2022), *Why Russia's cyber-attacks have fallen flat*, <https://www.economist.com/leaders/2022/12/01/why-russias-cyber-attacks-have-fallen-flat>.
[3] Microsoft (2022), *Microsoft Digital Defence Report 2022*, <https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report-2022>.
[4] Ponemon Institute (2022), *Cyber Insecurity in Health Care: The Cost and Impact on Patient Safety and Care*, <https://www.proofpoint.com/sites/default/files/threat-reports/pfpt-us-tr-cyber-insecurity-healthcare-ponemon-report.pdf>.
[5] CyberPeace Institute (2023), *Cyber Incident Tracer #HEALTH*, <https://cit.cyberpeaceinstitute.org/explore>.
[6] Reuters (2023), *Hackers hit websites of Danish central bank, other banks*, <https://www.reuters.com/technology/denmarks-central-bank-website-hit-by-cyberattack-2023-01-10/>.

DIGITALEUROPE
Rue de la Science, 14A, B-1040 Brussels
T.+32 (0) 2 609 53 10 / www.digitaleurope.org / @DIGITALEUROPE
EU Transparency Register: 64270747023-20

of a hacker attack on an IT subcontractor's software testing environment.[7] Oil shipments from the Amsterdam-Rotterdam-Antwerp oil trading hub and 11 German terminals were significantly delayed after cyber-attacks.[8] Even media companies find themselves affected by ransomware attacks.[9]

To address the increasing number and the changing nature of digital threats in the new geopolitical context, DIGITALEUROPE set up a dedicated Executive Council. DIGITALEUROPE's Resilience Executive Council provides in this paper a response to the Joint Communication highlighting the current and potential contribution of the private sector to the efforts of Member States, the European Commission and relevant EU institutions, bodies and agencies (EUIBAs) on cyber defence.

Our Executive Council strongly believes that the public and private sectors need to work closely for a more ambitious EU Cyber Defence Policy in the new European security context. Moreover, we agree that it is beneficial to partner and address common challenges. The global community needs to cooperate and collaborate closer, exchange information and interact more. Our global digital economy risks being more and more vulnerable to cyberattacks if nation-states, global industry, and experts do not increase international cooperation on definitions and solutions around cybersecurity. The recommendations below correspond to key areas such as the governance of the EU Cyber Defence Policy, procurement, standards, and skills. DIGITALEUROPE's Resilience Executive Council recommends:

Action 1: Create a Joint Public-Private Advisory Council on Cyber Resilience ('the Advisory Council')

The Advisory Council would support and facilitate strategic cooperation and preparedness to achieve a high common level of network and information systems security in the European Union. Multiple models of public-private cooperation already exist for inspiration, in sectors and in other countries.

Action 2: The Advisory Council should play a crucial role in defining the proposed EU Cyber Solidarity initiative and cyber reserve

[7] Reuters (2022), *Danish train standstill on Saturday caused by cyber-attack*, <https://www.reuters.com/technology/danish-train-standstill-saturday-caused-by-cyber-attack-2022-11-03/>.

[8] Reuters (2022), *Oil shipments in European oil hub delayed after cyber-attacks*, <https://www.reuters.com/world/europe/oil-shipments-european-oil-hub-delayed-after-cyber-attacks-2022-02-04/>.

[9] BBC (2022), *Guardian newspaper hit by suspected ransomware attack*, https://www.bbc.com/news/technology-64056300.

The Advisory Council would suggest criteria for cybersecurity certification schemes for trusted private providers (the 'cyber reserve') and how to develop them. Common public-private exercises are crucial to ensure the necessary level of preparedness, including a common knowledge base and understanding of cyber defence.

Action 3: The upcoming European Defence Investment Programme should include provisions for the joint procurement of digital and cybersecurity technologies while ensuring faster and more agile procurement processes.

We need to ensure that the upcoming regulation prioritises digital and cybersecurity as core components of our efforts to increase the security of EU citizens, after consultations with relevant stakeholders in the digital industry. Procurement processes must be faster and more agile.

Action 4: NATO's DIANA model should be duplicated at the EU level to drive SME innovation in cybersecurity.

EU Member States could draw learnings from NATO and the new SME accelerator programme DIANA, which supports SME innovation and cross-border contracting amongst NATO allies. While avoiding competition, a similar bureaucratically agile and streamlined model replicated at the EU level could spur more SME innovation in cybersecurity.

Action 5: The Advisory Council should work with the High-Level Forum on European Standardisation to promote and develop hybrid civil/defence standards.

Interoperability will be critical for our cyber defence. Our governments need to look closely at industry-based standards and become an adopter of standards, notably of private sector standards in terms of innovation and defence. The Advisory Council should have the specific knowledge to contribute industry expertise to establish a strong common ground in standardisation. The Advisory Council could also cooperate with the High-Level Forum on European Standardisation.

Action 6: The Advisory Council should be an integral part of the initiative on a Cyber Skills Academy

The Advisory Council can contribute to outlining the framework for the Cyber Skills Academy. For example, DIGITALEUROPE is already coordinating similar

programmes such as Women4IT. We encourage both the EU and NATO to pool resources, investments, and capabilities in developing this initiative.

Table of contents

Introduction

Digital technologies could enhance our resilience while at the same time being weaponised and used against us. Digital has no borders and only through collective efforts with like-minded nations and partners, we can effectively address the risks associated with cyberattacks.

About DIGITALEUROPE's Resilience Executive Council

DIGITALEUROPE is the leading trade association representing digitally transforming industries in Europe. We stand for a regulatory environment that enables European businesses and citizens to prosper from digital technologies. We wish Europe to grow, attract and sustain the world's best digital talents and technology companies.

Together with our members, we shape the industry policy positions on all relevant legislative matters and contribute to the development and implementation of relevant EU policies, as well as international policies that have an impact on Europe's digital economy. Our membership represents over 45,000 businesses that operate and invest in Europe. It includes 100 corporations which are global leaders in their field of activity, as well as 41 national trade associations from across Europe.

DIGITALEUROPE's Resilience Executive Council is an advisory board acting as a trusted advisor to international organisations i.e., European Union, NATO, United Nations. The Executive Council puts forward recommendations on addressing and preventing digital threats in the new geopolitical context in Europe. It gathers senior executives and experts in their field from the private sector. The main topics covered are cyber defence and security, connectivity and infrastructure, disinformation, skills, investment, as well as supply chains. Members of the Executive Council are part of private organisations coming from NATO countries and EU Member States.

Our Executive Council held several high-level meetings, the recent ones being dedicated to critical digital technologies as well as to the resilience of supply chains. Members of DIGITALEUROPE's Executive Council who contributed to this paper:

- **Izabela Albrycht**, Director of the Cybersecurity Center, AGH University of Science and Technology, PIIT representative
- **Bjarke Alling**, Group Director of Liga and Member of the National Danish Cybersecurity Council
- **Jonathan Davis**, Senior Director, Cybersecurity Policy & Awareness, VISA
- **Vincent Defrenne**, Director of Cyber Strategy & Architecture, Nviso

- **Gavin Henderson**, VP and Chief Security Officer Europe, MasterCard
- **Andrew Lee**, VP of Government Affairs, ESET
- **Marina Nogales Fulwood**, Global Head Cyber External Engagement, Grupo Santander
- **Peter Sund**, CEO, Technology Finland
- **Eva Telecka**, Executive Director, Regional CISO, MSD

1. GOVERNANCE

Why the private sector must play a bigger role, and how.

- The cumulative consequences of malicious cyber activities can have a major strategic impact on our societies. The private sector is best placed to prevent, detect, and respond to significant cybersecurity incidents. DIGITALEUROPE welcomes this acknowledgement in the Joint Communication. At the same time, we draw attention to the lack of specific governance in the Joint Communication on collaboration with the private sector. We believe that it is imperative for the public and private sectors to cooperate and collaborate to ensure the resilience and resolve of our societies in the new European security architecture.
- The collaboration between the Military Computer Emergency Response Team Operational Network (MICNET), the Computer Security Incident Response Teams (CSIRT) network and the Computer Emergency Response Team (CERT-EU) – as mentioned in the Joint Communication – needs to involve the private sector in relevant information-sharing and incident response efforts. While we support the initiative of Security Operation Centres (SOCs), we also see a vital role for the private sector in the activities of SOCs. In addition, the Network and Information Systems Directive[10] establishes a Cooperation Group composed of representatives of the Member States, the European Commission and the European Union Agency for Cybersecurity (ENISA). However, real cyber resilience cannot be achieved without the involvement of the private sector. We see that there is a complex web of institutional structures in the overall cyber defence model as outlined in the Joint Communication, which could affect the EU's ability to react and serve efficiently. A joint public-private governance structure would bridge the work of the many existing initiatives at the EU level with the relevant initiatives from the private sector. It is also important to

[10] European Commission (2016), *DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union*, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32016L1148>.

streamline the number of organisations and clarify roles and responsibilities when implementing the EU Cyber Defence Policy.

Action 1: Create a Joint Public-Private Advisory Council on Cyber Resilience ('the Advisory Council)

- DIGITALEUROPE recommends setting up a Joint Public-Private Advisory Council on Cyber Resilience ("the Advisory Council") in order to support and facilitate strategic cooperation and preparedness with a view to achieving a high common level of security of network and information systems in the European Union. The Joint Public-Private Advisory Council on Cyber Resilience could be set up by the European Defence Agency as part of its role to ensure that MICNET collaborates with the CSIRT and the CERT-EU as well as the private sector. We would see the outline as follows:

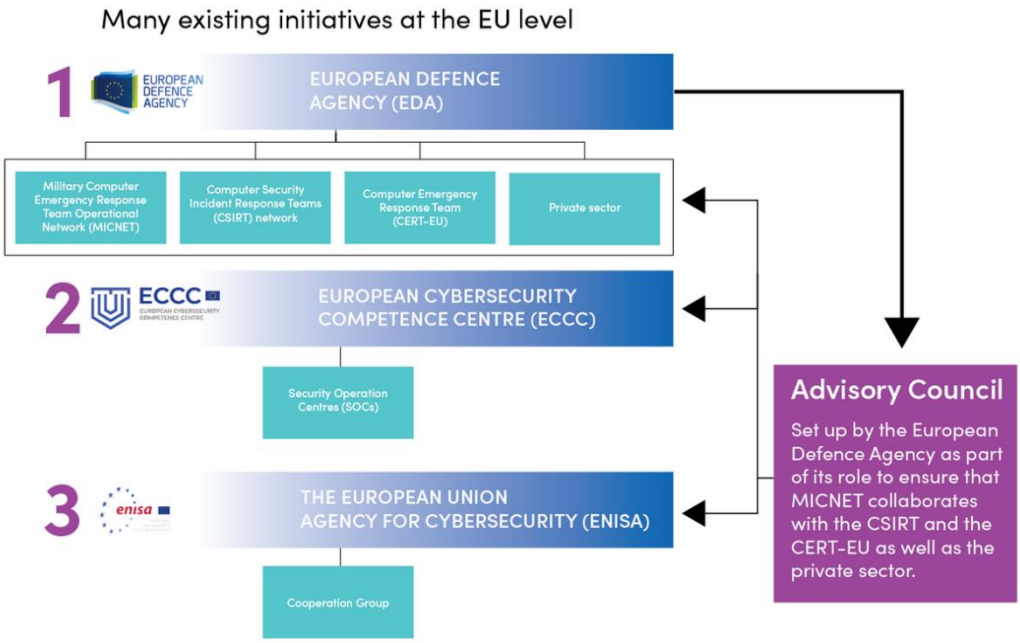

Figure 1: The Advisory Group in the current institutional setting

- The private sector owns and operates a substantial amount of critical infrastructure. It can provide subject matter expertise in vulnerability workarounds as well as software-related updates and fixes. Moreover, the private sector has knowledge of best practices and current cyber threat intelligence (CTI). Consequently, we need a joint framework for sharing CTI, risk mitigation and other vital information and resources with the public sector. This approach needs to go beyond the request to share information unilaterally, as foreseen in the Network and Information Security Directive (NIS2). As such, the private sector part of this joint framework should have access to relevant information and activities in the defence area at the national and European levels.

Private actors often use CTI sources and tools similar to the ones used by national defence ministries.

Action 2: The Advisory Council should play a crucial role in defining the proposed EU Cyber Solidarity initiative and cyber reserve

- DIGITALEUROPE welcomes the idea of the EU Cyber Solidarity initiative, which could support the gradual set-up of an EU-level cyber reserve with services from trusted private providers, including the possibility to develop cybersecurity certification schemes. This should be aligned with existing schemes to avoid duplication. In addition, we would already recommend setting up discussions with industry partners to define what trusted private providers are. The Joint Public-Private Advisory Council on Cyber Resilience should play a crucial role in suggesting criteria for cybersecurity certification schemes and developing them. We provide several examples of similar certification schemes here below for reflection.
- The Advisory Council can also input into the framework to set up the EU-level cyber reserve. Common public-private exercises are crucial to ensure the necessary level of preparedness. To have a common knowledge base and understanding of the cyber defence, we should pool together best practices and practical examples as well as joint training. We provide examples of public-private cooperation in our section dedicated to Skills.[11]

Examples of information-sharing models

- ISACs – European Union
  - For a more efficient approach, we encourage the information sharing between private and public sectors to be sector-specific e.g., finance, healthcare, telecommunications, energy etc. A sector-specific approach could reduce noise and confusion to improve situational awareness across sectors, as well as make it simpler for private sector organisations to participate, which will in turn drive greater participation among more organisations. For example, ISAC communities collaborate with ENISA to exchange information.
- Critical emergency response group – United States
  - Another example is the critical emergency response group in the United States. Before Russia invaded Ukraine, the group saw tensions mounting and got together to discuss potential solutions to critical cybersecurity situations. When the war started, information was disseminated across the US to tackle

[11] Please see page 9 in this document.

misinformation on cyber-attacks to calm the public. The groups' calls are set based on need and urgency.

- Katakri - Finland
  - Finland uses Katakri,[12] an auditing tool that assesses the ability of an organisation to protect classified information coming from a national or local authority. The tool ensures that the organisation has adequate security arrangements to prevent the disclosure of classified information in all the environments where the information is handled. It can be used for domestic and international projects.

2. PROCUREMENT

How to ensure Europe has access to the best cybersecurity technology

- Digital technologies are becoming a game-changer in defence. Emerging and disruptive technologies, cybersecurity, and 5G are key for defence critical systems. Defence strategies and capabilities cannot be thought out without the digital component. To be able to stay at the forefront of the growing competition in this area, the European Union needs to think of agile procurement strategies that prioritise innovative digital solutions to counteract digital threats, including cyber threats.
- DIGITALEUROPE welcomed the proposal to commit €500 million of the EU budget for common procurement of urgently needed defence products.[13] However, we call on the European Commission to ensure that at least 20% of these funds are spent on innovative SME-cyber solutions. This will boost digital resilience. In addition, the procurement of tools to train and develop skill sets should also be considered.

Action 3: The upcoming European Defence Investment Programme should include provisions for the joint procurement of digital and cybersecurity technologies while ensuring faster and more agile procurement processes.

- We also believe that it is very timely for the European Commission to work on a proposal for a European Defence Investment Programme (EDIP) as an anchor for future joint development and procurement projects of high common interest to the security of the Member States and the Union. DIGITALEUROPE calls on the European Commission

[12] Ministry of Foreign Affairs of Finland (2022), *Information security auditing tool for authorities – Katakri*, <https://um.fi/information-security-auditing-tool-for-authorities-katakri>.

[13] European Commission (2022), *Defence industry: EU to reinforce the European defence industry through common procurement with a €500 million instrument*, <https://ec.europa.eu/commission/presscorner/detail/en/IP_22_4491>.

to include relevant provisions for the joint procurement of digital and cybersecurity technologies in the upcoming proposal for a European Defence Investment Programme (EDIP) after consultations with relevant stakeholders in the digital industry. We need to ensure that the upcoming regulation prioritises digital as a core component of our efforts to increase the security of EU citizens. At the same time, we encourage the European Commission and Member States to direct funds to procure innovative solutions from SMEs, thus leading to more digital resilience.

- We also encourage European and national institutions to find ways to move faster and become more agile in terms of procurement. Today, it takes ten years between prototypes and phases of approval, which is too long in cybersecurity and cyber-defence. Member States need to take the lead while ensuring a collaborative approach instead of a domestic one. An example is the mutual recognition of the definition of "secure solutions". This would boost the scalability of SMEs developing cyber technologies in the European Union. Currently, we have a high number of SMEs in Europe, but they are not in a position to scale across borders because – amongst others – we lack a common application of "secure solutions". The development of cybersecurity certification schemes for trusted providers should tackle this challenge for SMEs.

Action 4: NATO's DIANA model to be duplicated at the EU level to drive SME innovation

- EU Member States could draw learnings from NATO and the new SME accelerator programme DIANA, which supports SME innovation and cross-border contracting amongst NATO allies. While avoiding competition, a similar bureaucratically agile and streamlined model replicated at the EU level could spur more SME innovation. Generally speaking, DIGITALEUROPE would advise against duplicating efforts already underway at the NATO level.

- Hence, DIGITALEUROPE encourages the European Commission and the relevant EUIBAs to work together with the private sector, academia and Member States to establish a similar framework at the EU level bringing together trusted cybersecurity innovators amongst start-ups, scientific researchers and technology companies. Over the past years, the European innovation programmes have helped technology champions emerge and form a European ecosystem that is yet to be formalised. Efforts in this sense could be led by the European Defence Agency (EDA). This framework could facilitate the joint procurement of digital and cybersecurity technologies between Member States while allowing emerging players to become more aware of EU programmes for innovation in the area of digital defence. The efforts to establish an EU-level cyber reserve could benefit from this approach.

3. STANDARDS

Ensuring interoperability to enhance our cyber defences

Action 5: The Advisory Council should work with the High-Level Forum on European Standardisation to promote and develop hybrid civil/defence standards.

- The Advisory Council welcomes the recommendation in the Joint Communication for more cooperation between the EU and NATO on common standards. In particular, more focus is needed on Command-and-control standards, Emergency Management standards, Cyber Threat Intelligence standards and other key areas. The Advisory Council stands ready to contribute industry expertise to establish a strong common ground in standardisation.
- The European Commission is currently setting up a High-Level Forum on European Standardisation (the Forum) to identify standardisation priorities in support of EU policies and legislation on green, digital and resilience.14 It is imperative for the Forum to ensure that cyber and AI standards are at the top of the agenda. DIGITALEUROPE is a member of the Forum and will support this work. It is therefore our recommendation that the Advisory Council and the High-Level Forum on European Standardisation cooperate on standards to enhance our cyber defence.
- Interoperability should be an absolute priority. The future is collaborative, with data playing a massive role. We are aware that the European Commission aims to present a plan to promote the use of existing hybrid civil/defence standards and the development of new ones. Our recommendation is to involve the Advisory Council throughout the entire process.
- It is paramount that we can operate together – public and private – in an interoperable manner. Our governments need to look closely at industry-based standards and become an adopter of standards, notably of private sector standards in terms of innovation and defence. With key technologies becoming off-the-shelf and accessible, interconnection and cooperation between countries and with industry are key.
- Cybersecurity defence and cybersecurity standards, supported by legislation, should when necessary, use common assessment methodologies which are grounded in widely used frameworks and

[14] European Commission (2022), *High-Level Forum on European Standardisation*, <https://single-market-economy.ec.europa.eu/single-market/european-standards/standardisation-policy/high-level-forum-european-standardisation_en>.

standards to ensure even application across jurisdictions. In addition, eIDAS2 is equally important, as government services are expected to work seamlessly and cross-border in the near future. The NIIS Foundation is a good example of a platform for countries that use similar interoperability mechanisms. Here below is an example of certification aimed at increasing trust between governments and critical infrastructures:

- Example: The Cyber Trust mark in Singapore

  - The Cyber Trust mark is a cybersecurity certification developed by the Cyber Security Agency of Singapore (CSA).[15] It serves as a mark of distinction for companies to prove that they have implemented good cybersecurity practices and measures that are commensurate with their cybersecurity risk profile. The Cyber Trust mark rates participating organisations on a five-level scale (i.e., supporter, practitioner, promoter, performer, advocate) across 22 critical control areas. This voluntary certification of companies, which is not as heavy as ISO certifications and can be assessed in a relatively short period will set a level of cyber maturity transparently and thus help to increase the level of trust from governments towards critical infrastructure entities. This might play an important role in future cyber defence processes. CISA is considering launching a similar certification program.

4. SKILLS

Pooling common resources, investments, and capabilities to ensure a skilled workforce

- Companies large and small report difficulties in finding people with the right skill set. Europe lacks between 350,000 and one million cyber specialists.[16] Skills are of paramount importance to improve the resilience and resolve of our societies. The public, private and academic sectors need to collaborate closely to solve this situation.
- As previously mentioned, DIGITALEUROPE welcomes the idea of a gradual set-up of an EU-level cyber reserve with services from trusted private providers. The EU-level cyber reserve must be a result of joint private-public collaboration, with the private sector playing a key role.

---

[15] Cyber Security Agency of Singapore (2022), *Cybersecurity Certification Centre*, <https://www.csa.gov.sg/Programmes/certification-and-labelling-schemes/cybersecurity-certification-centre>.

[16] DIGITALEUROPE (2019), *A Stronger Digital Europe – our call to action towards 2025*, <https://www.digitaleurope.org/policies/strongerdigitaleurope/>.

This initiative can explore opportunities to make inroads with academic sectors, tech-savvy experts and junior talent.

Action 6: The Advisory Council should be an integral part of the initiative on a Cyber Skills Academy

- While the proposed Cyber Skills Academy aims to act as an umbrella initiative, the European Commission and the relevant EUIBAs need to involve the Advisory Council in outlining the framework for the Cyber Skills Academy. We encourage both the EU and NATO to pool resources, investments, and capabilities in developing this initiative. It needs to benefit each EU Member State and address the lack of vital cybersecurity skills undermining resilience in Europe.
- DIGITALEUROPE is already coordinating similar programmes such as Women4IT.[17] Our project trained 900 young women from seven European countries in job-relevant digital skills while receiving employability mentorship. Based on the experience stemming from the Women4IT project, DIGITALEUROPE is ready to work closely with the European Commission and the Advisory Council to create a similar programme on cyber skills.
- Below are some other examples that could serve to roll out the Cyber Skills Academy.
- Example: NATO's Locked Shields exercise
    - European policymakers could also draw inspiration from other institutional initiatives, such as NATO's Locked Shields exercise – the largest and most complex international live-fire cyber defence exercise in the world.[18] Such a pan-European exercise could bring together specialists from the public, private and academic sectors to hone their skills and experience on both sides while creating an informal network across Europe and the US between national specialists.
- Example: EU Network of Cybersecurity campuses
    - DIGITALEUROPE also recommends the creation of a network of Cybersecurity Skills campuses across Member States to support local training activities. The recently established Campus Cyber[19] in France is an example that could be used at the EU level. Member States must draw from their national recovery and resilience funding and invest in CAPEX for the set-up of their campuses. Coordination of the Network should fall on

[17] Women4IT (2022), <https://women4it.eu/>.

[18] NATO (2022), *Exercise Locked Shields 2022 concludes*, <https://shape.nato.int/news-archive/2022/exercise-locked-shields-2022-concludes>.

[19] Campus Cyber (2022), <https://campuscyber.fr/>.

the Commission to ensure campus specialisation where reasonable across the EU, in the interest of resource maximisation. It can take advantage of existing academic networks across the European Union. Campuses should cater first to SMEs operating in sensitive sectors for Europe's economy and society. They should prioritise specialist areas like threat-led penetration testing and compliance to equip businesses with cyber-prevention capabilities and meet strict, upcoming regulatory requirements. They should cover, partially or fully with public money, OPEX such as training equipment, coaching and mentoring for employer-sponsored individual training.

- However, upskilling existing IT professionals is not enough. Long-term cyber resilience requires a complete rethinking of curricula in primary and secondary schools as well as higher education and academic centres. The EU must increase from 12 to 24 by 2025 the number of Member States with compulsory computer science in their national primary or secondary education. They should also support upgrading knowledge and expertise in cybersecurity curricula across the academic sector. To speed up progress on this target, the Commission should explore monetary reward and incentive schemes for those EU countries that make their curricula digital-proof. In addition, we should look at the upskilling of other industry sectors when it comes to cybersecurity. Even the existing IT workforce would equally benefit from upgrading their cybersecurity skills. The private sector is eager to collaborate with European and national authorities to shape such curricula as they would benefit society and businesses.

- The lack of focus on critical security skills in western democracies stands in sharp contrast to countries like China and India which have had a focus on science, technology, engineering, and mathematics (STEM) as well as tech skills for the past 20 years. For every cybersecurity graduate in the EU every year, there are 12 such graduates in China.[20] 2023 is the European Year of Skills and the public, private and academic sectors have the chance to use this momentum to collaborate to develop the much-needed cyber specialists in Europe.

Conclusion

- In the new geopolitical context, defence and security are becoming key priorities for national governments. With the rise of cyber armies and

[20] South China Morning Post (2022), *China's demand for cybersecurity talent will exceed supply by over 3 million in five years, says education ministry report*, <https://www.scmp.com/tech/tech-trends/article/3191781/chinas-demand-cybersecurity-talent-will-exceed-supply-over-3>.

information warfare, the European Union, its member states, as well as NATO and its allies face growing digital security challenges, demanding increased cooperation. Cooperation between the public, private and academic sectors is of uttermost importance and will remain so. We all need to work together and ensure there is the right clarity and commitment towards peaceful settlements of international cyber disputes to avoid greater militarization of cyberspace.

- To ensure that the cooperation between the public and the private sectors yields the best results, DIGITALEUROPE suggests the recommendations above and remains ready to support the European institutions and NATO.