LCAMP

Learner Centric Advanced Manufacturing Platform

Cybersecurity

WPN° 3 Observatory

Co-funded by
the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

LCAMP partners:

TKNIKA – Basque VET Applied Research Centre, CIFP Miguel Altuna LHII, DHBW Heilbronn – Duale Hochschule, Baden-Württemberg, Curt Nicolin High School, AFM – Spanish Association of Machine Tool Industries, EARLALL – European Association of Regional & Local Authorities for Lifelong Learning, FORCAM, CMQE: Association campus des métiers et des qualifications industrie du future, MV: Mecanic Vallée, KIC: Knowledge Innovation Centre, MADE Competence Centre Industria 4.0; AFIL: Associazione Fabbrica Intelligente Lombardia, SIMUMATIK AB; Association HVC Association of Slovene Higher Vocational Colleges; TSCMB:Tehniški šolski center Maribor, KPDoNE: Kocaeli Directorate Of National Education; GEBKİM OIZ and CAMOSUN college.

Document summary

Document Type:	Public report
Title	Cybersecurity
Author/S	Hervé DANTON
Reviewer	Camille LEONARD
Date	December 2024
Document Status	Final
Document Level	Confidential until its publication
Document Description	This document describes the main features of the trends in advanced manufacturing and insights for VET
Cite This Deliverable As:	Danton, H. Cybersecurity (LCAMP4.0 Deliverable D3.2 Decembre 2024)
Document Level	Public

Version management

Version	Date	Action
0.1	2023-06-15	Draft version, lay out defined
0.5	2023-09-15	Draft version with partners contributions
0.8	2023-10-30	Final version for internal revision
0.9	2023-11-14	Final version for revision process
0.95	2024-11-10	Approval by the steering committee
1	2024-12-09	Version to be uploaded to the EU portal

GLOSSARY AND/OR ACRONYMS

AI - Artificial Intelligence

AM - Advanced Manufacturing

Cedefop - European Centre for the Development of Vocational Training

CoVE - Centres of Vocational Excellence

EAfA - European Alliance for Apprenticeships

EC - European Commission

ECVET - European Credit System for Vocational Education and Training

EntreComp - The Entrepreneurship Competence Framework

EQAVET - European Quality Assurance in Vocational Education and Training

EQF - European Qualifications Framework

ESCO - European Skills, Competences and Occupations

ETF - European Training Foundation

EU - European Union

HE - Higher Education

HVET - Higher Vocational Education and Training

I4.0 - Industry 4.0

KET - Key Enabling Technology

OECD - Organisation for Economic Cooperation and Development

SME - Small and Medium Enterprises

SWOT - Strengths, Weaknesses, Opportunities, Threats

TVET - Technical and Vocational Education and Training

VET - Vocational Education and Training

WBL - Work Based Learning

CONTENT TABLE

CONTENT TABLE 5

EXECUTIVE SUMMARY 6

1. INTRODUCTION 7

2. TOPIC: CYBERSECURITY 8

2.1 Main used sources 8

2.1.1 Context and limitations 11

2.1.2 Why relevant? 11

2.1.3 Main Data 11

2.1.4 Data Analysis 15

2.2 Findings 19

3. CONCLUSION 24

4. REFERENCES 29

5. INDEX OF TABLES 34

EXECUTIVE SUMMARY

Advanced Manufacturing (AM) and Higher Vocational Education and Training (HVET) need to update training, implement new technologies, and get quick access to data.

The causes behind these needs are technological factors (Industry 4.0), factors conditioned by education systems and education methodologies, social factors and environmental factors (the European Green Deal with its emphasis on the greening industry).

Under the CoVE initiative, the LCAMP project aims to support regional skill ecosystems and various stakeholders in providing new skills and implementing new or updated technologies in VET centres. LCAMP will tackle this by incorporating a permanent European Platform of Vocational Excellence for Advanced Manufacturing.

By collaborating across borders, LCAMP's goal is to support and empower regional Advanced Manufacturing CoVEs to become more resilient, innovative, and better equipped to train, upskill, and reskill young and adult students, to successfully face the digital and green transitions. We will help European regions and countries grow and be more competitive through their VET systems.

Therefore, the LCAMP OBSERVATORY is one of the services in the LCAMP platform. The observatory is led by the French cluster *Mecanic Vallée* and the French VET provider *Campus des Métiers et des Qualifications d'Excellence Industrie du Futur*.

This present document details the first results of the LCAMP Observatory, through the methodology that the LCAMP consortium used to set up and run the Observatory. We had set up a process cycle for the observation consisting of 5 stages:

- Stage 1: Diagnosis and priority
- Stage 2: Search and information gathering
- Stage 3: Information Analysis
- Stage 4: Creating value. Elaboration of LCAMP reports
- Stage 5: Dissemination and communication.

1. INTRODUCTION

The LCAMP observatory is one of the services of the LCAMP platform.

The LCAMP Observatory must be a reliable and easily accessible source of information and data for trainers, VET teachers, and professionals, updated on Digital / Advanced Manufacturing / Smart Industry, delivered through a multimedia and interactive platform -LCAMP platform-, that can be customized according to individual interests (Work in progress in WP8).

This observatory must feed other Work packages (WP), for instance, WP 5 on Learner Centric Training, or Open innovation Community in the WP4.

In a first document about methodology, are set up a process cycle for the observation consisting in 5 stages:

- Stage 1: Diagnosis and priority
- Stage 2: Search and information gathering
- Stage 3: Information Analysis
- Stage 4: Create value. Elaboration of LCAMP reports
- Stage 5: Disseminate-communicate.

Following this process cycle, are detailed the main aspects of the observation methodology:

- Identify reliable sources that we can find in Europe about Advanced Manufacturing.
- Classify and filter data gathered from different sources.
- Present several ways to collect data and to analyse them.
- Define the methods for the creation of annual reports.
- Validate process for those reports.

The observatory will publish periodical reports for VET and HVET target audiences about technology trends, labour market changes, skill needs, and occupations in Advanced Manufacturing. It is expected that SMEs, industry clusters and other associations will also find valuable information in the observatory.

The publication of a yearly report is planned.

- Report 1: June 2023,
- Report 2: June 2024,
- Report 3: June 2025.

This first annual report is gathering sub-reports written by around twenty different writers, from the main partners involved in the LCAMP project. 39 Topics were determined, and 22 TOPICS were analysed and worked on during this first period.

2. TOPIC: CYBERSECURITY

The purpose of this chapter is to present some of the development areas related to AM.

These are topics that concern all or some of the stakeholders

- CoVEs and VETs: teachers, trainers and heads of VET schools;
- Learners: students, active workers, job seekers;
- Companies;
- Policy makers and other stakeholders

2.1 MAIN USED SOURCES

Table 1 : Presentation and brief description of main sources

Identification [1]	Description	**Geographical** scope.	**Sectorial** scope	Links
PUBLIC SOURCES				
EFFRA	The European Factories of the Future Research Association (EFFRA) is a non-for-profit, industry-driven association promoting the development of new and innovative production technologies. EFFRA has been representing the private side of the manufacturing partnership with the EU Commission. Named under Horizon 2020, Factories of the Future to become Made in Europe nowadays under Horizon Europe	Europe	Multisector	https://www.effra.eu/
Groupe AFNOR	French national agency for standardization	International	Multisector	www.afnor.fr
OECD	2520 documents	World	Multisector	https://www.oecd.org/science/

Identification [1]	Description	**Geographical** scope.	**Sectorial** scope	Links
EUROPA		Europe	Multisector	
ENISA	European agency for cybersecurity	Europe	Multisector	
CORDIS	7587 documents	Europe		https://cordis.europa.eu/
TRAINING SOURCES				
MINALOGIC	European competitiveness cluster on mechanics	EU & Regional France	Aerospace	https://www.minalogic.com/
CETIM	French national agency for all mechanics subjects & Ind 4.0	France	Multisector	www.cetim.fr https://www.cetim-engineering.com/
FRANCE COMPETENCES	French National Center for technical learning	France	Industry and I 4.0	https://www.francecompetences.fr/
EFVET	EfVET is the European Forum of Technical and Vocational Education and Training	Europe		https://www.efvet.org/who-we-are/
industrial SOURCES				
BPi	French National Public Bank for development	France	Industry and I 4.0	https://www.bpifrance-universite.fr/formation/e-parcours-industrie-du-futur/
Usine Nouvelle	French national Newspaper for Industry	France	Multisector	https://www.usinenouvelle.com/
Journal du Net	8940 docs in trends cyber	France	iT	https://www.journaldunet.com/
Techniques de l'ingénieur	258 documents	National / international	Multisector	https://www.techniques-ingenieur.fr/

Identification [1]	Description	**Geographical** scope.	**Sectorial** scope	Links
Fraunhofer Institute of Optronics, System Technologies and Image Exploitation IOSB	The Cybersecurity Training Lab of Fraunhofer Academy is a cooperation between Fraunhofer and selected universities of applied sciences. Specialists and managers from industry and public administration receive a compact qualification in high-quality laboratories with up-to-date IT infrastructure. There, they simulate real threat scenarios, learn to recognise their significance and consequences and study suitable solution concepts in a practical manner in their use and efficiency.	Germany	Cybersecurity	https://www.iosb.fraunhofer.de
C4iiOT	C4IIOT will design, build and demonstrate a novel and unified Cybersecurity 4.0 framework	Europe	Cybersecurity	https://www.c4iiot.eu/
DELOITTE	Deloitte Consulting LLP's Supply Chain and Manufacturing Operations practice helps companies understand and address opportunities to apply Industry 4.0 technologies in pursuit of their business objectives. Our insights into additive manufacturing, IoT, and analytics enable us to help organizations reassess their people, processes, and technologies in light of advanced manufacturing practices that are evolving every day.	World	Multisector	https://www2.deloitte.com/content/dam/insights/us/articles/3749_Industry4-0_cybersecurity/DUP_Industry4-0_cybersecurity.pdf
PWC		World	Multisector	https://www.pwc.com/us/en/industries/industrial-products/library/assets/manufacturing-supply-chain-cybersecurity-feb.pdf
E&Y	EY purpose is building a better working world. The insights and services we provide help to create long-term value for clients, people and society, and to build trust in the capital markets.	World	Multisector	https://www.ey.com/en_ie/consulting/digital-manufacturing-technology
FORTINET	2022 State of Operational Technology and Cybersecurity Report	World	Multisector	https://www.fortinet.com/content/dam/fortinet/assets/analyst-reports/report-2022-ot-cybersecurity.pdf
ACM	Association for Computing Machinery	World	Multisector	https://doi.org/10.1007/978-3-030-95484-0_6
ATMS	Advanced Transportation Manufacturing Summit	World	Multisector	https://canada.ammeetings.com/images/downloads/Cybersecurity_for_Advanced_and_Intelligent_Manufacturing_Environments.pdf
EJBMR	European Journal of Business and Management Research	World	Multisector	https://www.ejbmr.org/index.php/ejbmr/article/view/1173

Identification [1]	Description	Geographical scope.	Sectorial scope	Links
i-scoop	Reporting on digital transformation, Industry 4.0, Internet of Things, and emerging technologies in context.	World	iT	https://www.i-scoop.eu/internet-of-things-iot/industrial-internet-things-iiot-saving-costs-innovation/cybersecurity-industrial-internet-things/

- All FIELDS are concerned and covered. **F1: Trends; F2: Impact on jobs; F3: Skills & Qualifications; F4: Future Skills**
- Language: English and French
- Already used in industry and in global transformation.

2.1.1 CONTEXT AND LIMITATIONS

The review was done on European, General and French sources, in French and English languages. So, the analysis will have to be completed in another step (in next report, next year), by extending the review at all National Sources we can gather.

2.1.2 WHY RELEVANT?

Relevant sources are ones mentioning the topic in their archives or documents. Some of our sources don't and are not relevant, even, if in general, they could be for other topics.

2.1.3 MAIN DATA

Table 2 : Presentation and brief description of DATA

Identification [1]	Topic name	Internet links
PUBLIC SOURCES		
EFFRA	ConnectedFactories CyberSecurity for Digital Manufacturing Pathway webinar	https://www.effra.eu/events/connectedfactories-cybersecurity-digital-manufacturing-pathway-webinar
EFFRA	ConnectedFactories	https://www.effra.eu/news/connectedfactories-final-event-presentations-and-recordings-available

Identification [1]	Topic name	Internet links
EFFRA	Cybersecurity workshop_Presentations and Recordings	https://www.effra.eu/events/cybersecurity-workshoppresentations-and-recordings
EFFRA	ConnectedFactories CyberSecurity for Digital Manufacturing Pathway	https://www.connectedfactories.eu/search/node/cybersecurity
EFFRA	Standards for digital manufacturing webinar:	https://www.effra.eu/news/standards-digital-manufacturing-webinar-recordings-and-presentations-are-now-available
EFFRA	SECOIIA	https://secoiia.eu/
EFFRA	COLLABS	https://www.collabs-project.eu/
EFFRA	INFRASTRESS	https://www.infrastress.eu/
Groupe AFNOR	Cybersécurité : ISO 27001, une norme devenue incontournable	https://www.afnor.org/actualites/cybersecurite-iso-27001-norme-incontournable/
CORDIS	Strengthening European efforts in Cyber Capacity Building	https://cordis.europa.eu/article/id/411432-strengthening-european-efforts-in-cyber-capacity-building
CORDIS	Making global supply chains cyberthreat-proof	https://cordis.europa.eu/article/id/442568-making-global-supply-chains-cyberthreat-proof
TRAINING SOURCES		
Bpi	La cybersécurité de ma PME : par où commencer ?	https://www.bpifrance-universite.fr/formation/la-cybersecurite-de-ma-pme-par-ou-commencer/
Bpi	Cursus Cybersécurité	https://www.bpifrance-universite.fr/formation/e-parcours-cybersecurite/
MINALOGIC	Minalogic lance son label "Sécurité économique"	https://www.minalogic.com/cybersecurite-comment-proteger-votre-entreprise/
CETIM	Introduction à la cyberesécurité	https://www.cetim.fr/formation/formation/industrie-du-futur/Transformation-numerique/IIOT/Collecte-et-stockage-des-donnees/cybersecurite-des-systemes-industriels-sie01
FRANCE COMPETENCES	Opérateur en cybersécurité	https://www.francecompetences.fr/recherche/rncp/34975/#ancre3
EFVET	REWIRE Cybersecurity Blueprint: The Future of Cybersecurity Education in Europe	https://efvet.org/rewire-cybersecurity-blueprint-the-future-of-cybersecurity-education-in-europe-online-event/
EFVET	How to train more Cybersecurity experts in Europe	https://efvet.org/ec-webinar-how-to-train-more-cybersecurity-experts-in-europe/
EFVET	DTAM: A new EU project to facilitate the digital transformation in advanced manufacturing	https://efvet.org/dtam-a-new-eu-project-to-facilitate-the-digital-transformation-in-advanced-manufacturing/

Identification [1]	Topic name	Internet links
INDUSTRIAL SOURCES		
CORDIS	Protect your company with a new cybersecurity self-assessment	https://cordis.europa.eu/article/id/418093-protect-your-company-with-a-new-cybersecurity-self-assessment
BPi	Formation : Autodiag Cybersécurité	https://www.bpifrance-universite.fr/formation/autodiag-cybersecurite/
Journal du Net	41.000 documents	https://www.journaldunet.com/cybersecurite/
Journal du Net	Cybersécurité : les tendances qui auront un impact sur vos applications en 2022	https://www.journaldunet.com/solutions/dsi/1507951-cybersecurite-les-principales-tendances-qui-auront-un-impact-sur-vos-applications-en-2022/
Techniques de l'ingénieur	L'industrie et les défis de la cybersécurité Publié en décembre 2022	https://www.techniques-ingenieur.fr/actualite/livre-blanc/lindustrie-et-les-defis-de-la-cybersecurite-118035/
CORDIS	Effective protection of Critical Infrastructures against cyber threats	https://cordis.europa.eu/article/id/429128-effective-protection-of-critical-infrastructures-against-cyber-threats
CORDIS	Cybersecurity risk management: How to strengthen resilience and adapt in 2021	https://cordis.europa.eu/article/id/429338-cybersecurity-risk-management-how-to-strengthen-resilience-and-adapt-in-2021
CORDIS	Dynamic cybersecurity management for organisations and local/regional networks based on awareness and collaboration	https://cordis.europa.eu/project/id/101069543
OECD	Analysing a New Generation of National Cybersecurity Strategies	https://www.oecd.org/digital/ieconomy/comparativeanalysisofnationalcybersecuritystrategies.htm
OECD	Recommendation of the Council on Digital Security Risk Management	https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0479
EUROPA	Digitising Industry (Industry 4.0) and Cybersecurity	https://www.europarl.europa.eu/RegData/etudes/BRIE/2017/607361/IPOL_BRI(2017)607361_EN.pdf
ENISA	Cybersecurity is a key enabler for Industry 4.0 adoption	https://www.enisa.europa.eu/news/enisa-news/cybersecurity-is-a-key-enabler-for-industry-4-0-adoption
Fraunhofer Institute of Optronics, System Technologies and Image Exploit	Cybersecurity Training Lab	https://www.iosb.fraunhofer.de/en/projects-and-products/cybersecurity-learning-lab.html
C4iiOT	European project	https://www.c4iiot.eu/
DELOITTE	Industry 4.0 and cybersecurity Managing risk in an age of connected production	https://www2.deloitte.com/content/dam/insights/us/articles/3749_Industry4-0_cybersecurity/DUP_Industry4-0_cybersecurity.pdf
PWC	Manufacturers ramp up cyber defenses as supply-chain bottlenecks – and vulnerabilities	https://www.pwc.com/us/en/industries/industrial-products/library/assets/manufacturing-supply-chain-cybersecurity-feb.pdf

Identification [1]	Topic name	Internet links
E&Y	Cybersecurity generalities	https://www.ey.com/en_ie/consulting/cybersecurity
NDIA	Cybersecurity for Advanced Manufacturing (CFAM)	https://content.ndia.org/-/media/sites/ndia/divisions/cybersecurity/ndia-cyber-div-cfam-ortiz-20170627-v5.pdf?download=1
FORTINET	2022 State of Operational Technology and Cybersecurity Report	https://www.fortinet.com/content/dam/fortinet/assets/analyst-reports/report-2022-ot-cybersecurity.pdf
ATMS	Cybersecurity for Advanced and Intelligent Manufacturing Environments	https://canada.ammeetings.com/images/downloads/Cybersecurity_for_Advanced_and_Intelligent_Manufacturing_Environments.pdf
EJBMR	The State of Cybersecurity in Smart Manufacturing Systems: A Systematic Review	https://www.ejbmr.org/index.php/ejbmr/article/view/1173
Lane Thames Dirk Schaefer	Cybersecurity for Industry 4.0 - Springer Series in Advanced Manufacturing - Analysis for Design and Manufacturing	https://www.researchgate.net/publication/291337650_Cybersecurity_for_Industry_40_Analysis_for_Design_and_Manufacturing_CALL_FOR_CHAPTERS
i-scoop	Industrial Internet of Things (IIoT) – cybersecurity risks, solutions and evolutions	https://www.i-scoop.eu/internet-of-things-iot/industrial-internet-things-iiot-saving-costs-innovation/cybersecurity-industrial-internet-things/
FORBES	cybersecurity In The Industry 4.0 Era	https://www.forbes.com/sites/forbestechcouncil/2022/02/03/cybersecurity-in-the-industry-40-era/
NATO	Cybersecurity and reliability challenges from adoption of Industry 4.0 in IACS environments	https://industrialcyber.co/industry-4-0/cybersecurity-and-reliability-challenges-from-adoption-of-industry-4-0-in-iacs-environments/

2.1.4 DATA ANALYSIS

Introduction and contextualisation

General situation

With Industry 4.0, there is a change in manufacturing systems, provided by the development of communication and information technologies, adding intelligence components in manufacturing factories, through connectivity and interaction, throughout the supply chain (intelligent manufacturing systems and cyber-physical systems), with still Human in the centre of activities. However, this revolution of Industry 4.0 is growing on an extremely sensitive and critical question of the data and systems security.[1]

Industry 4.0 and optimization of production in Advanced Manufacturing to obtain greater productivity and to generate more profits has led towards smart manufacturing, with the Internet of Things, a global network of interrelated physical devices, such as sensors, actuators, intelligent applications, computers, mechanical machines and objects, and even people, through the Internet.

These devices are data sources that provide abundant information on manufacturing processes in an industrial environment. These challenges raise concerns about security, more specifically cybersecurity, which makes it possible to avoid damages to production lines and to information and data.[2]

Particularly in combination with the Internet and other disruptive technologies such as cloud computing, so many opportunities and new business models are emerging.

However, there are also many risks associated with this transformation, particularly with regard to cyber security. Against the backdrop of increasing dependence on networked information

[1] Armando Araújo de Souza Junior et al., « The State of Cybersecurity in Smart Manufacturing Systems: A Systematic Review », *European Journal of Business and Management Research* 6, nº 6 (16 décembre 2021): 188-94, https://doi.org/10.24018/ejbmr.2021.6.6.1173.

[2] Roman Rudenko et al., « A Brief Review on Internet of Things, Industry 4.0 and Cybersecurity », *Electronics* 11, nº 11 (janvier 2022): 1742, https://doi.org/10.3390/electronics11111742.

technology, the attack of companies is increasing. To this end, it is necessary to assess the negative impact on business caused by cyber security attacks in Industry 4.0.[3]

New situation: Home work

More people than ever have joined the digital economy, and an Owl Labs survey found that 80% of people expect to work at least three days a week from home. A report by Upwork predicts that "by 2025, 36.2 million Americans will be working remotely, an 87% percent increase from pre-pandemic levels."[4]

Rise in attacks

Manufacturers worldwide are being targeted by cybercriminals at an astonishing − and increasing − rate.

Last year, the number of cyberattacks on manufacturers spiked by more than +300%, accounting for 22% of all attacks across all sectors, up from +7% the previous year.

Most US industrials sector executives (Deloitte survey 2021) expect cyber threats to increase, with 66% saying they believe there will be increased threats from cyber criminals, hacktivists (62%) and nation states (60%).

- Increasing complexity is creating critical vulnerabilities. Most of these executives agree that complexity across their organization poses cyber and privacy risks at “concerning levels.” Complex cloud environments pose risks for 81% of respondents, as do complex governance of data (79%).
- Cyber lies at the core of business, attested to by 82% of respondents agreeing that they’ve seen an increased alignment of cyber strategy with business strategy over the last two years. Another 82% say recent key mergers and acquisitions have involved cybersecurity considerations.

[3] Antonio João Gonçalves de Azambuja, Alexander Kern, et Reiner Anderl, « Analysis of Cyber Security Features in Industry 4.0 Maturity Models », in *Computer Security. ESORICS 2021 International Workshops: CyberICPS, SECPRE, ADIoT, SPOSE, CPS4CIP, and CDT&SECOMANE, Darmstadt, Germany, October 4–8, 2021, Revised Selected Papers* (Berlin, Heidelberg: Springer-Verlag, 2021), 91-106, https://doi.org/10.1007/978-3-030-95484-0_6.

[4] Yevgeny Dibrov, « Council Post: How Can Your Company Stay Safe Amid Skyrocketing Cyber Attacks? », Forbes, s. d., https://www.forbes.com/sites/forbestechcouncil/2021/10/11/how-can-your-company-stay-safe-amid-skyrocketing-cyber-attacks/.

- Supply chain risks are the next big thing. 63% of sector leaders expect that third party threats will increase, with 58% anticipating an increase in reportable incidents occurring at the supply chain software level.[5] [6] [7]

Based on a survey on 500 companies, one thing that has improved very little in the past year is organizations' security outcomes. A staggering 93% of organizations experienced an intrusion in the past 12 months, and 78% experienced more than three. Impacts included downtime, financial or data loss, brand degradation, and even reduced physical safety. Clearly, most organizations have work to do. Fortunately, a small percentage of respondents managed to avoid intrusions for the past year, and this report identifies several of the best practices they are more likely to employ.[8]

Ransomware was the top attack type, accounting for 23% of attacks on manufacturing organizations and underscoring the heavy focus ransomware actors placed on manufacturing.

Server access attacks came in second place at 12%, representing probably some failed attacker operations.

BEC and data theft tied for third place, at 10% each. BEC attackers are probably seeking to capitalize on the many supplier and wholesale shipping relationships manufacturing organizations develop, and attempt to redirect payments between partners to accounts under the BEC attackers' control.

About Geography, Manufacturing faced the most attacks in Asia (32%), North America (27%), and Europe (26%).

Manufacturing Threat intelligence

Based on their survey, Fortinet declares that organizations repost modest moves forward in the overall maturity of their OT security posture. But looking at specific best practices brings nuance

---

[5] « Industry 4.0 and Cybersecurity | Deloitte Australia | Cyber Risk », Deloitte Australia, 2022, https://www2.deloitte.com/au/en/pages/risk/articles/industry-4-cyber-security.html.

[6] « Global Threat Intelligence Report 2022 », NTT, 2022, https://www.security.ntt/global-threat-intelligence-report-2022.

[7] PricewaterhouseCoopers, « Manufacturer Cybersecurity and Supply Chain », PwC, 24 février 2022, https://www.pwc.com/us/en/industries/industrial-products/library/cyber-supply-chain.html.

[8] « Fortinet | Arcview Research Analysis », Fortinet, 2022, https://global.fortinet.com/lp-en-ap-arcview?utm_source=Paid-Search&utm_medium=Google&utm_campaign=OT-EMEA-FR&utm_content=AR-ARC-OTNeedsITSec-G&utm_term=ot%20security&lsci=7012H0000021ommQAA&UID=ftnt-9346-41823&s_kwcid=AL!11440!3!650979883409!p!!g!!ot%20security&gclid=Cj0KCQjwuLShBhC_ARIsAFod4fLvBfniohK0hYwPpQxLlgSaZsz-R9V4n4iTmqciq6gZRyCQfwl3dNgaAhivEALw_wcB.

to the issue. Only 13% of respondents have achieved centralized visibility of all OT activities, and only 52% are able to track all OT activities from the security operations centre (SOC). Only around half of respondents claim to track and report various basic security metrics, and fewer than half of respondents are using any of a dozen specific security technologies and practices. The latter indicates a diversity in how organizations address OT security and reflects a market that is still evolving.[9]

The next for industrials: Third-parties and supply-chain risks

Looking ahead, manufacturers are continuing to up their cybersecurity systems. Top goals for the next three years include achieving more successful outcomes for their organization's transformation, preventing attacks and gaining more confidence of leaders in their ability to manage current and future attacks. But, the next big subject for industrials will be Third-parties and supply-chain risks.[10]

Public strategies

An OECD report analyses the latest generation of "national cybersecurity strategies" in ten countries and identifies commonalities and differences.

This comparative analysis reveals that cybersecurity policy making is at a turning point. In many countries, it has become a national policy priority supported by stronger leadership. A single definition of cybersecurity cannot be derived from these strategies. Nevertheless, all new strategies are becoming integrated and comprehensive. They approach cybersecurity in a holistic manner, encompassing economic, social, educational, legal, law-enforcement, technical, diplomatic, military and intelligence-related aspects. "Sovereignty considerations" have become increasingly important.

The new generation of national cybersecurity strategies aims to drive economic and social prosperity and protect cyberspace-reliant societies against cyber-threats. A key challenge of cybersecurity policy making today is to pursue these two objectives while preserving the openness of the Internet as a platform for innovation and new sources of growth.[11]

---

[9] « Fortinet | Arcview Research Analysis ».
[10] PricewaterhouseCoopers, « Manufacturer Cybersecurity and Supply Chain ».
[11] « Comparative analysis of national cybersecurity strategies », OECD, s. d., https://www.oecd.org/digital/ieconomy/comparativeanalysisofnationalcybersecuritystrategies.htm.

Objectives / research question / problem statement:

The objective of the report is to detect major challenges and trends for cybersecurity in ADMA: Advanced Manufacturing.

- What are major challenges of cybersecurity in ADMA?
- What are the challenges of IoT cybersecurity?
- What types of cybersecurity are used in IoT?
- With Industrial Cybersecurity, how can we secure these new use cases and support business projects?

2.2 FINDINGS

Facing increasing data flow, and numerous and subtler threats, 4 major trends are noticed these last years in Cybersecurity for ADMA & I4.0:

- **Efforts on national / public support to Cybersecurity**
- **Developments in standardisation**
- **New training courses in cybersecurity and self-control analysis**
- **New ways to work.**

Efforts on national / public support to Cybersecurity

The implementation of a programme for digitising European industry (Industry 4.0) is an ambitious endeavour, which is linked to a number of new challenges that go beyond the large-scale cybersecurity framework tackled until now by the European strategies and legislation.

- Key European strategies and legislation on cybersecurity, including R&D investments are currently focused on:
  - Protection of personal data
  - Security of operation of large scale and publicly accessible information networks
  - Protection of operation of key infrastructures (of public importance)
- The importance of cybersecurity in industrial settings is only marginally recognised in relevant EU policies
- Development of appropriate legislative and support activities particularly adapted to computerized manufacturing has to become a more vigorous feature of the Digital Single Market

- Cybersecurity in the context of digitised industry requires a more holistic approach"12

Strengthening European efforts in Cyber Capacity Building

Enhancing cybersecurity capacity building is quickly becoming a priority for governments, international organisations and the private sector. While the demand for skilled cybersecurity professionals continues to accelerate, organizations are struggling to find the right talent to fill jobs.

Making global supply chains cyberthreat-proof[13] [14]

Global supply chains have to become more secure and resilient against cyberattacks.

Efforts in standardisation

Cybersecurity: ISO 27001 is a standard that has become unavoidable: ISO 27001 deals with the security of information systems and concerns both digital and paper data.

A trajectory in line with global developments, since the number of certificates worldwide will jump from 36,000 to 58,000 between 2019 and 2021. Nearly 100,000 sites worldwide, including nearly 1,600 in France. In terms of countries, the top three are China, Japan and the United Kingdom, all of which have more than 5,000. The main reason for this growth is the central role played by data protection issues.[15]

Development of Training courses and self-control analysis

A report about Cybersecurity experts in Europe found that in the last years, there has been a significant increase in the number of programmes offered by the higher education system in Europe, most of them being master's degrees. Overall, these programmes match the skills

---

[12] Miklos Gyorffi, « Digitising Industry (Industry 4.0) and Cybersecurity », *PE 607.361*, s. d., 12.
[13] « Making Global Supply Chains Cyberthreat-Proof | News | CORDIS | European Commission », Cordis, s. d., https://cordis.europa.eu/article/id/442568-making-global-supply-chains-cyberthreat-proof.
[14] « Strengthening European Efforts in Cyber Capacity Building | News | CORDIS | European Commission », Cordis, s. d., https://cordis.europa.eu/article/id/411432-strengthening-european-efforts-in-cyber-capacity-building.
[15] CHRISTELLE MAMBUENI, « Cybersécurité : ISO 27001, une norme devenue incontournable », *Groupe AFNOR* (blog), 23 novembre 2022, https://www.afnor.org/actualites/cybersecurite-iso-27001-norme-incontournable/.

required, but there is still room for improvement. Indeed, some skills such as Law, Compliance or Privacy are underrepresented, which requires more diversity in the offered programmes.

The number of enrolled students is increasing. This is closely related to the number of graduate students in cybersecurity, which is estimated to double in the next two to three years. However, although all these findings are important, there is an issue that still needs to be emphasised: gender balance. Looking at the percentage of new students enrolled, there is a big difference between female (20%) and male (80%).[16] [17]

"Economic Security" labels

For instance, MINALOGIC[18] project aims to Provide in France, a simple and effective response to help cluster members (and more broadly companies in the Auvergne-Rhône-Alpes French region) to assess their risk exposure and provide them with support in setting up a phased remediation plan and pragmatic.

Based on proven cooperation models between Fraunhofer and universities of applied sciences, a model is being implemented for the further training of IT security specialists which involves the universities of applied sciences as partners in cooperative research, in the development of further training concepts and teaching modules and finally in the teaching of the course content.

By setting up the Cyber Security Training Laboratory[19] and networking the continuing education offers of various partner consortia, users and decision-makers are addressed. The modules are tailored to the needs of industry and public administration in terms of sectors, topics and functions.

Because Companies in all sectors are well into their digital transition, they concentrate a lot of their know-how, their strategic information and their operational capacities in their digital uses.

---

[16] « EC Webinar: 'How to Train More Cybersecurity Experts in Europe' - European Forum for Vocational Education & Training », 21 mars 2022, https://efvet.org/ec-webinar-how-to-train-more-cybersecurity-experts-in-europe/.

[17] « DTAM: A New EU Project to Facilitate the Digital Transformation in Advanced Manufacturing - European Forum for Vocational Education & Training », 18 janvier 2021, https://efvet.org/dtam-a-new-eu-project-to-facilitate-the-digital-transformation-in-advanced-manufacturing/.

[18] « Minalogic lance son label pour augmenter la cyber-résilience de ses adhérents », Minalogic, 21 février 2023, https://www.minalogic.com/cybersecurite-comment-proteger-votre-entreprise/.

[19] « Cybersecurity Training Lab - Fraunhofer IOSB », Fraunhofer Institute of Optronics, System Technologies and Image Exploitation IOSB, s. d., https://www.iosb.fraunhofer.de/en/projects-and-products/cybersecurity-learning-lab.html.

This opens the door to thefts, interruptions or malfunctions that can severely impact their prosperity.

Therefore, it becomes necessary to control the business risk linked to the use of new digital technologies. This objective is made difficult by the technical and varied nature of cybersecurity issues. But it is achievable, if we do it right."

"You want to evaluate your company's cybersecurity maturity and your ability to resist the main threats? Take stock in 15 minutes, measure the level of cybersecurity of your company and your ability to protect yourself. Why perform the self-diagnosis? 35 questions to evaluate yourself on the physical, organizational, human resources or information system security axis. The self-diagnosis is done in 3 steps.

The result is a personalized diagnosis that establishes your company's maturity in terms of cybersecurity and recommendations for services and training based on your answers in each of the areas covered. The results obtained are exportable and resources are suggested according to your results, some of which are available online. The main Objective of the self-diagnosis is to measure the level of cybersecurity of your company and your ability to protect yourself.[20] [21]

The “Cybersecurity Best Practices For SMEs Assessment” is a simple and quick online self-assessment questionnaire launched by 4 Cybersecurity research projects funded by the European Commission. In less than 15 minutes SMEs can easily understand where they stand in terms of cybersecurity practices implementation and learn basic security guidelines to be applied in their day-to-day routine.[22]

Regarding the Question: What are major challenges of cybersecurity in ADMA ? **The trends that will impact your applications next years are:**

One of the challenges highlighted in the recent NATO Energy Security Center of Excellence (NATO ENSEC COE) guide is the adoption of Industry 4.0 or industrial Internet of Things (IIoT) that has led to the integration of manufacturing with business functions, with sensors added to collect data on all the machine-to-machine activity for data analysis, and then risks about cybersecurity.[23]

---

[20] « Formation en ligne Cursus Cybersécurité - Bpifrance Université », *BPI France Universite* (blog), s. d, https://www.bpifrance-universite.fr/formation/e-parcours-cybersecurite/.
[21] « Formation en ligne Autodiag Cybersécurité - Bpifrance Université », *BPI France Universite* (blog), s. d., https://www.bpifrance-universite.fr/formation/autodiag-cybersecurite/.
[22] « Making Global Supply Chains Cyberthreat-Proof | News | CORDIS | European Commission ».
[23] Anna Ribeiro et al., « Cybersecurity and Reliability Challenges from Adoption of Industry 4.0 in IACS Environments », *Industrial Cyber* (blog), 30 janvier 2022, https://industrialcyber.co/industry-4-0/cybersecurity-and-reliability-challenges-from-adoption-of-industry-4-0-in-iacs-environments/.

Taking the time to evaluate software security within an organization is paramount and could be among the best resolutions. Many technologies have emerged in recent years with cybersecurity challenges. Here are a few that should be part of our daily lives in the years to come.

Ubiquitous connectivity: We are moving towards a world where everything is connected: devices, software, objects... As data flows between enterprise applications, cloud- and SaaS-connected software, and IoT devices, the risk of cyberattack increases exponentially for businesses. A shared responsibility model between cloud providers and companies will address this, alongside a zero-trust approach.

Abstraction and componentization: Software and technology continue to be at the core of business development. As a result, companies are constantly looking for ways to innovate and create software faster. To get faster, many development teams are turning not only to the cloud but also to microservices. Microservices break down entire applications into the smallest reusable blocks possible, so they can be assembled into processes or workflows.

Hyper-automation of software delivery: The hyper-competitiveness of the market leads to a need to go faster and faster and to eliminate all process inefficiencies through hyper automation. This also concerns software development, and all processes that interact with software delivery. This will put code at the centre: security as code, compliance as code, and infrastructure as code. In addition, IT security teams will be more involved in defining security policies.

Evolution of open-source libraries: Open-source libraries provide teams with common features that can be easily incorporated into code and thus make them more efficient. Unfortunately, most developers admit that they never update third-party libraries after incorporating them into the code base. As open-source libraries continue to evolve, not updating their vulnerabilities is a major cause for concern. In fact, nearly one-third of applications now have more security flaws in their third-party code than in their source code.[24]

[24] « Cybersécurité : les tendances qui auront un impact sur vos applications en 2022 », JDN, 7 janvier 2022, https://www.journaldunet.com/solutions/dsi/1507951-cybersecurite-les-principales-tendances-qui-auront-un-impact-sur-vos-applications-en-2022/.

3. CONCLUSION

New Generation of National Cybersecurity Strategies[25] [26]

OECD RECOMMENDS that Members and non-Members adhering to this Recommendation to adopt a digital security risk management approach to build trust and take advantage of the open digital environment for economic and social prosperity, applicable at all levels of government and in public organisations; based on the following principles, which are complementary, should be taken as a whole, and are meant to be consistent with risk management processes, best practices, methodologies, and technical standards; and CALLS on private organisations to promote and implement the following principles.

Cybersecurity in Industry for Advanced and Intelligent Manufacturing Environments[27]

Companies can adopt a number of different tactics to create an effective cybersecurity strategy: 'Enterprises should conduct audits on a regular basis, use two-factor authentication, identify the major threats, and enforce a strong sign-off policy. Investments into platforms that have a track record of robustness and security strength must be a priority in this information era,' Similarly, Garrett Austin, Business Development Lead at Rockwell Automation, describes a three-pronged approach to help manufacturers stay safe, which involves determining OT Maturity by increasing visibility and monitoring; establishing an IT/OT Strategy and creating governance around it; and building bridges between engineering, operations and IT"

Regarding Question of what to do: **Best Practices of Top-Tier Organizations are:**

1. One way might be to propose appropriate security measures, "4.0" measures (for the industrial environment in any case) that have already proved their worth in other environments:

[25] « OECD Legal Instruments », OECD Legal Instruments, s. d., https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0479.
[26] « Science and Technology - OECD », OECD, s. d., https://www.oecd.org/science/.
[27] Carla Larkin, « Cybersecurity for Advanced and Intelligent Manufacturing Environments », *ATMS*, s. d., 1.

- To prevent a threat from spreading, one shall strengthen detection resources, especially the flows from and to industrial IS. This is the time to take advantage of this opportunity to dock with the Group SOC if it has not already done so.
- To ensure the integrity and traceability of transmitted/received data, encryption and authentication can be implemented. Do you already have a Group PKI? Why not think about extending it to industrial perimeters.
- It is also the right time to strengthen its OCM / SCM process. Is the solution connected with the outside? No more excuses for not installing an antivirus, updating it, installing security patches for your favourite OS, etc. This point should be anticipated prior to purchasing the solution, rather than once the product has already been installed!
- Finally, the solution is critical for the business? A cyber-resilience component must be anticipated so that the solution can be quickly rebuilt and restarted in the event of an attack.

As we have just seen, there is no shortage of solutions, but they require adapted support from the cybersecurity teams and going beyond theoretical models.[28]

2. Top-tier organizations are 177% more likely to have security vulnerability response time as one of their top three success metrics.

As the old adage goes, “What gets measured gets improved,” and responding quickly to OT security vulnerabilities is key to protecting these systems. The organizations with the best outcomes are nearly three times as likely to have this measurement as a prominent part of their performance review.

3. Top-tier organizations are 37% more likely to have network access control technology in place.

Ensuring that only authorized parties can access specific systems is critical for securing any technology asset. When it comes to OT, people who need access to such systems have a relatively narrow range of job titles. Organizations that avoided intrusions last year are much more likely to have such controls in place.

4. Top-tier organizations are 48% more likely to report security compromises to senior/executive leadership. Items that are included in regular reports to executive leadership tend to remain at front of mind throughout the year. Organizations that keep

[28] Julien Verrier, « La cybersécurité industrielle à l’ère de l’Industrie 4.0 », RiskInsight, 2021, https://www.riskinsight-wavestone.com/en/author/julien-verrier/.

top leaders apprised of security compromises tend to have fewer of them. Top-tier organizations tend to be more transparent with executive management.

5. Top-tier organizations are 32% more likely to have their SOC monitor and track OT security.

Security operations centres (SOCs) have existed for decades and have developed granular best practices for managing IT security. OT leaders who have avoided intrusions are more likely to have entrusted OT security to the same group.

6. Top-tier organizations are 44% more likely to track and report intrusions detected and remediated.

Understanding past attacks sharpens an organization's skills at thwarting future ones, and this starts with keeping records. Organizations that avoided intrusions are more likely to routinely report them when they do occur.

7. Top-tier organizations are infinitely more likely to use just one vendor for their IP-enabled OT devices. Avoiding complexity in networking and systems is a good way to reduce the attack surface and improve the security posture. None of the organizations that experienced 10 or more intrusions were using just one vendor for their IP-enabled OT devices, while nearly one-third of top-tier organizations had achieved this.[29]

Regarding Question: **"What are the challenges of IoT cybersecurity?",** the biggest challenge is the rapid detection of attacks and their identification to act more effectively, thus reducing severe consequences, as we are talking about an IoT environment that consists of several connected sensors. Usually, low processing capacity makes it difficult to protect them. Researchers seek to create innovative tools that can overcome these obstacles while keeping IoT sensors protected to solve this problem. A significant challenge is linked to the evolution of increasingly innovative and sophisticated attacks, leading industries to seek innovative solutions to combat current and future attacks. As security evolves, cyberattacks evolve too.

Regarding Question: **"What types of cybersecurity are used in IoT?",**

Several forms of protection against cyberattacks lay in different industries. The cybersecurity of intelligent manufacturing has to be developed in a personalized way. There is no common

[29] « Fortinet | Arcview Research Analysis ».

method of use, although the concept presents variations with similarities. However, the most promising are based on machine learning and blockchain.[30]

To strengthen standardization.[31] [32] [33] [34]

We have noticed four major trends in the past years in cybersecurity for Advanced Manufacturing & I4.0:

- **Cybersecurity is becoming a national and public concern.**

  Europe, national governments, and national bodies are concerned with cyber threats in industry, which have increased significantly in the past years. that have increased a lot in the last few years. The rules and good practices to apply across industry to counter threats are across Europe. Educational courses within Advanced Manufacturing should consider cybersecurity.

- **Standardisation is becoming a general trend in Industry, Industry 4.0 and Advanced manufacturing.**

  National and European organisations are working on standardisation within cybersecurity. Educational courses for future industry professionals should take this into account.

---

[30] Rudenko et al., « A Brief Review on Internet of Things, Industry 4.0 and Cybersecurity ».

[31] « Gartner® Predicts 2023: Cybersecurity Industry Focuses on the Human Deal | Bitsight », Bitsight, 2023, https://www.bitsight.com/resources/gartner-predicts-2023-cybersecurity-industry-focuses-human-deal-ppc?utm_adgroup=emea_cybersecurity&utm_ad=648358504977&utm_matchtype=p&utm_placement=&utm_device=c&utm_network=g&utm_targetid=kwd-271609081&utm_campaignid=12258443672&utm_adgroupid=116807633745&utm_extensionid=&utm_source=adwords&utm_medium=ppc&utm_campaign=emea_cybersecurity&utm_term=cybersecurity&utm_content=gartner_urgency_report&hsa_acc=9761199014&hsa_cam=12258443672&hsa_grp=116807633745&hsa_ad=648358504977&hsa_src=g&hsa_tgt=kwd-271609081&hsa_kw=cybersecurity&hsa_mt=p&hsa_net=adwords&hsa_ver=3&gad=1&gclid=Cj0KCQjwpPKiBhDvARIsACn-gzDunAu_cRp15JloMVudJ7iNKcmAPOTaFLMYYhrKoNKgkoUcaAmMH7saAppnEALw_wcB.

[32] Renate Verheijen, « Cybersecurity Standardisation Conference 2022 », Event, ENISA, 2022, https://www.enisa.europa.eu/events/cybersecurity_standardisation_2022.

[33] Olga MEYER, « Olga MEYER | Group Leader | Fraunhofer Institute for Manufacturing Engineering and Automation IPA, Stuttgart | IPA | Competence Center DigITools for Manufacturing | Research Profile », ResearchGate, s. d., https://www.researchgate.net/profile/Olga-Meyer.

[34] « Standards for Digital Manufacturing Webinar: Recordings and Presentations Are Now Available! », EFFRA, 21 octobre 2020, https://www.effra.eu/news/standards-digital-manufacturing-webinar-recordings-and-presentations-are-now-available.

- **New training courses must involve cybersecurity in each step, and self-control analysis by professional users must become more common.**

  Educational courses need to include cybersecurity at each step. Professionals within the industry need to apply self-control analysis at each step of their work.

- **Cybersecurity must be introduced in Industry 4.0 and Advanced manufacturing, for within- and between company communication.**

  Industry 4.0 should threat cybersecurity within and between companies seriously, considering the increase of cyber threats in the past years. Educational courses for future industry professionals should take this into account.

4. REFERENCES

Azambuja, Antonio João Gonçalves de, Alexander Kern, et Reiner Anderl. « Analysis of Cyber Security Features in Industry 4.0 Maturity Models ». In *Computer Security. ESORICS 2021 International Workshops: CyberICPS, SECPRE, ADIoT, SPOSE, CPS4CIP, and CDT&SECOMANE, Darmstadt, Germany, October 4–8, 2021, Revised Selected Papers*, 91-106. Berlin, Heidelberg: Springer-Verlag, 2021. https://doi.org/10.1007/978-3-030-95484-0_6.

Bitsight. « Gartner® Predicts 2023: Cybersecurity Industry Focuses on the Human Deal | Bitsight », 2023. https://www.bitsight.com/resources/gartner-predicts-2023-cybersecurity-industry-focuses-human-deal-ppc?utm_adgroup=emea_cybersecurity&utm_ad=648358504977&utm_matchtype=p&utm_placement=&utm_device=c&utm_network=g&utm_targetid=kwd-271609081&utm_campaignid=12258443672&utm_adgroupid=116807633745&utm_extensionid=&utm_source=adwords&utm_medium=ppc&utm_campaign=emea_cybersecurity&utm_term=cybersecurity&utm_content=gartner_urgency_report&hsa_acc=9761199014&hsa_cam=12258443672&hsa_grp=116807633745&hsa_ad=648358504977&hsa_src=g&hsa_tgt=kwd-271609081&hsa_kw=cybersecurity&hsa_mt=p&hsa_net=adwords&hsa_ver=3&gad=1&gclid=Cj0KCQjwpPKiBhDvARIsACn-gzDunAu_cRp15JloMVudJ7iNKcmAPOTaFLMYYhrKoNKgkoUcaAmMH7saAppnEALw_wcB.

BPI France Universite. « Formation en ligne Autodiag Cybersécurité - Bpifrance Université », s. d. https://www.bpifrance-universite.fr/formation/autodiag-cybersecurite/.

BPI France Universite. « Formation en ligne Cursus Cybersécurité - Bpifrance Université », s. d. https://www.bpifrance-universite.fr/formation/e-parcours-cybersecurite/.

BPI France Universite. « Formation en ligne Cursus Industrie du Futur - Bpifrance Université », s. d. https://www.bpifrance-universite.fr/formation/e-parcours-industrie-du-futur/.

C4IIOT. « Www.C4iiot.Eu – Cyber Security 4.0: Protecting the Industrial Internet of Things », s. d. https://www.c4iiot.eu/.

Cetim. « Cybersécurité des systèmes industriels - Formations - Cetim », s. d. https://www.cetim.fr/formation/formation/industrie-du-futur/Transformation-numerique/IIOT/Collecte-et-stockage-des-donnees/cybersecurite-des-systemes-industriels-sie01.

Cetim Engineering. « Cetim Engineering », s. d. https://www.cetim-engineering.com/.

COLLABS. « Home - COLLABS », s. d. https://www.collabs-project.eu/, https://www.collabs-project.eu/.

Connected factories. « Search Cybersecurity », s. d. https://www.connectedfactories.eu/search/node/cybersecurity.

Cordis. « Cybersecurity Risk Management: How to Strengthen Resilience and Adapt in 2021 | News | CORDIS | European Commission », s. d. https://cordis.europa.eu/article/id/429338-cybersecurity-risk-management-how-to-strengthen-resilience-and-adapt-in-2021.

Cordis. « Dynamic Cybersecurity Management for Organisations and Local/Regional Networks Based on Awareness and Collaboration | CS-AWARE-NEXT Project | Fact Sheet | HORIZON | CORDIS | European Commission », s. d. https://cordis.europa.eu/project/id/101069543.

Cordis. « Effective Protection of Critical Infrastructures against Cyber Threats | News | CORDIS | European Commission », s. d. https://cordis.europa.eu/article/id/429128-effective-protection-of-critical-infrastructures-against-cyber-threats.

Cordis. « Making Global Supply Chains Cyberthreat-Proof | News | CORDIS | European Commission », s. d. https://cordis.europa.eu/article/id/442568-making-global-supply-chains-cyberthreat-proof.

Cordis. « Protect Your Company with a New Cybersecurity Self-Assessment », s. d. https://cordis.europa.eu/article/id/418093-protect-your-company-with-a-new-cybersecurity-self-assessment.

Cordis. « Strengthening European Efforts in Cyber Capacity Building | News | CORDIS | European Commission », s. d. https://cordis.europa.eu/article/id/411432-strengthening-european-efforts-in-cyber-capacity-building.

Deloitte Australia. « Industry 4.0 and Cybersecurity | Deloitte Australia | Cyber Risk », 2022. https://www2.deloitte.com/au/en/pages/risk/articles/industry-4-cyber-security.html.

Dibrov, Yevgeny. « Council Post: Cybersecurity In The Industry 4.0 Era ». Forbes, s. d. https://www.forbes.com/sites/forbestechcouncil/2022/02/03/cybersecurity-in-the-industry-40-era/.

———. « Council Post: How Can Your Company Stay Safe Amid Skyrocketing Cyber Attacks? » Forbes, s. d. https://www.forbes.com/sites/forbestechcouncil/2021/10/11/how-can-your-company-stay-safe-amid-skyrocketing-cyber-attacks/.

« DTAM: A New EU Project to Facilitate the Digital Transformation in Advanced Manufacturing - European Forum for Vocational Education & Training », 18 janvier 2021. https://efvet.org/dtam-a-new-eu-project-to-facilitate-the-digital-transformation-in-advanced-manufacturing/.

« EC Webinar: 'How to Train More Cybersecurity Experts in Europe' - European Forum for Vocational Education & Training », 21 mars 2022. https://efvet.org/ec-webinar-how-to-train-more-cybersecurity-experts-in-europe/.

EFFRA. « ConnectedFactories CyberSecurity for Digital Manufacturing Pathway Webinar », 1 avril 2022. https://www.effra.eu/events/connectedfactories-cybersecurity-digital-manufacturing-pathway-webinar.

EFFRA. « ConnectedFactories Final Event - Presentations and Recordings Available », 23 novembre 2022. https://www.effra.eu/news/connectedfactories-final-event-presentations-and-recordings-available.

EFFRA. « Cybersecurity Workshop_Presentations and Recordings », 20 janvier 2021. https://www.effra.eu/events/cybersecurity-workshoppresentations-and-recordings.

EFFRA. « Standards for Digital Manufacturing Webinar: Recordings and Presentations Are Now Available! », 21 octobre 2020. https://www.effra.eu/news/standards-digital-manufacturing-webinar-recordings-and-presentations-are-now-available.

efvet. « REWIRE Cybersecurity Blueprint: The Future of Cybersecurity Education in Europe Online Event - European Forum for Vocational Education & Training », 1 février 2023. https://efvet.org/rewire-cybersecurity-blueprint-the-future-of-cybersecurity-education-in-europe-online-event/.

ENISA. « Cybersecurity Is a Key Enabler for Industry 4.0 Adoption ». Press Release, s. d. https://www.enisa.europa.eu/news/enisa-news/cybersecurity-is-a-key-enabler-for-industry-4-0-adoption.

« Formation en ligne La cybersécurité de ma PME : par où commencer ? - Bpifrance Université », s. d. https://www.bpifrance-universite.fr/formation/la-cybersecurite-de-ma-pme-par-ou-commencer/.

Fortinet. « Fortinet | Arcview Research Analysis », 2022. https://global.fortinet.com/lp-en-ap-arcview?utm_source=Paid-Search&utm_medium=Google&utm_campaign=OT-EMEA-FR&utm_content=AR-ARC-OTNeedsITSec-G&utm_term=ot%20security&lsci=7012H0000021ommQAA&UID=ftnt-9346-41823&s_kwcid=AL!11440!3!650979883409!p!!g!!ot%20security&gclid=Cj0KCQjwuLShBhC_ARIsAFod4fLvBfniohK0hYwPpQxLlgSaZsz-R9V4n4iTmqciq6gZRyCQfwl3dNgaAhivEALw_wcB.

France compétences. « RNCP34975 - Opérateur en cybersécurité », s. d. http://https%253A%252F%252Fwww.francecompetences.fr%252Frecherche%252F.

Fraunhofer Institute of Optronics, System Technologies and Image Exploitation IOSB. « Cybersecurity Training Lab - Fraunhofer IOSB », s. d. https://www.iosb.fraunhofer.de/en/projects-and-products/cybersecurity-learning-lab.html.

Groupe AFNOR. « AFNOR solutions – Les services du groupe en France et à l'international », s. d. https://www.afnor.org/.

Gyorffi, Miklos. « Digitising Industry (Industry 4.0) and Cybersecurity ». *PE 607.361*, s. d., 12.

Herman, Arthur. *Freedom's Forge: How American Business Produced Victory in World War II*. 1st ed. NDIA. New York: Random House, 2012. https://content.ndia.org/-/media/sites/ndia/divisions/cybersecurity/ndia-cyber-div-cfam-ortiz-20170627-v5.pdf?download=1.

« Industry 4.0 and Cybersecurity ». Deloitte, s. d. https://www2.deloitte.com/content/dam/insights/us/articles/3749_Industry4-0_cybersecurity/DUP_Industry4-0_cybersecurity.pdf.

Infrastress. « Critical Infrastructure », s. d. https://www.infrastress.eu.

i-SCOOP. « Industrial Internet of Things (IIoT) - Cybersecurity Risks, Solutions and Evolutions », s. d. https://www.i-scoop.eu/internet-of-things-iot/industrial-internet-things-iiot-saving-costs-innovation/cybersecurity-industrial-internet-things/.

JDN. « Cybersécurité : les tendances qui auront un impact sur vos applications en 2022 », 7 janvier 2022. https://www.journaldunet.com/solutions/dsi/1507951-cybersecurite-les-principales-tendances-qui-auront-un-impact-sur-vos-applications-en-2022/.

JDN. « Cybersécurité : mieux vaut prévenir que guérir », s. d. https://www.journaldunet.com/cybersecurite/.

Junior, Armando Araújo de Souza, José Luiz de Souza Pio, Jó Cunha Fonseca, Marcelo Albuquerque de Oliveira, Otávio Cesar de Paiva Valadares, et Pedro Henrique Souza da Silva. « The State of Cybersecurity in Smart Manufacturing Systems: A Systematic Review ». *European Journal of Business and Management Research* 6, nº 6 (16 décembre 2021): 188-94. https://doi.org/10.24018/ejbmr.2021.6.6.1173.

Kukreja, Puneet, Hugh Callaghan, et Carol Murphy. « Cybersecurity Solutions | EY Ireland ». EY, s. d. https://www.ey.com/en_ie/consulting/cybersecurity.

Kunnath, Vikram, Vivek Kasture, et Denis O'Dwyer. « Digital Manufacturing Technology | EY Ireland ». EY, s. d. https://www.ey.com/en_ie/consulting/digital-manufacturing-technology.

Larkin, Carla. « Cybersecurity for Advanced and Intelligent Manufacturing Environments ». *ATMS*, s. d., 1.

L'Usine Nouvelle. « L'Usine Nouvelle : l'actualité économique, les infos sur les entreprises et tous les secteurs de l'industrie », s. d. https://www.usinenouvelle.com/.

MAMBUENI, CHRISTELLE. « Cybersécurité : ISO 27001, une norme devenue incontournable ». *Groupe AFNOR* (blog), 23 novembre 2022. https://www.afnor.org/actualites/cybersecurite-iso-27001-norme-incontournable/.

MEYER, Olga. « Olga MEYER | Group Leader | Fraunhofer Institute for Manufacturing Engineering and Automation IPA, Stuttgart | IPA | Competence Center DigITools for Manufacturing | Research Profile ». ResearchGate, s. d. https://www.researchgate.net/profile/Olga-Meyer.

Minalogic. « Minalogic lance son label pour augmenter la cyber-résilience de ses adhérents », 21 février 2023. https://www.minalogic.com/cybersecurite-comment-proteger-votre-entreprise/.

« Mission & Vision - European Forum for Vocational Education & Training », 28 novembre 2022. https://efvet.org/who-we-are/.

NTT. « Global Threat Intelligence Report 2022 », 2022. https://www.security.ntt/global-threat-intelligence-report-2022.

OECD. « Comparative analysis of national cybersecurity strategies », s. d. https://www.oecd.org/digital/ieconomy/comparativeanalysisofnationalcybersecuritystrategies.htm.

OECD. « Science and Technology - OECD », s. d. https://www.oecd.org/science/.

OECD Legal Instruments. « OECD Legal Instruments », s. d. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0479.

PricewaterhouseCoopers. « Manufacturer Cybersecurity and Supply Chain ». PwC, 24 février 2022. https://www.pwc.com/us/en/industries/industrial-products/library/cyber-supply-chain.html.

PwC. « manufacturing-supply-chain-cybersecurity-feb.pdf », 2021. https://www.pwc.com/us/en/industries/industrial-products/library/assets/manufacturing-supply-chain-cybersecurity-feb.pdf.

« report-2022-ot-cybersecurity.pdf », s. d. https://www.fortinet.com/content/dam/fortinet/assets/analyst-reports/report-2022-ot-cybersecurity.pdf.

Ribeiro, Anna, Sarah Fluchs, Elad Ben-Meir, Tom Smertneck, et Anna Ribeiro Smertneck Sarah Fluchs, Elad Ben-Meir and Tom. « Cybersecurity and Reliability Challenges from Adoption of Industry 4.0 in IACS Environments ». *Industrial Cyber* (blog), 30 janvier 2022. https://industrialcyber.co/industry-4-0/cybersecurity-and-reliability-challenges-from-adoption-of-industry-4-0-in-iacs-environments/.

Rudenko, Roman, Ivan Miguel Pires, Paula Oliveira, João Barroso, et Arsénio Reis. « A Brief Review on Internet of Things, Industry 4.0 and Cybersecurity ». *Electronics* 11, nº 11 (janvier 2022): 1742. https://doi.org/10.3390/electronics11111742.

SeCoIIA. « SeCoIIA | Secure Collaborative Intelligent Industrial Assets », 26 juillet 2022. https://secoiia.eu/.

Techniques de l'Ingénieur. « "L'industrie et les défis de la cybersécurité " - Livre blanc », s. d. https://www.techniques-ingenieur.fr/actualite/livre-blanc/lindustrie-et-les-defis-de-la-cybersecurite-118035.

Thames, Lane, et Dirk Schaefer. « Cybersecurity for Industry 4.0: Analysis for Design and Manufacturing CALL FOR CHAPTERS », 21 janvier 2016. https://www.researchgate.net/publication/291337650_Cybersecurity_for_Industry_40_Analysis_for_Design_and_Manufacturing_CALL_FOR_CHAPTERS.

Verheijen, Renate. « Cybersecurity Standardisation Conference 2022 ». Event. ENISA, 2022. https://www.enisa.europa.eu/events/cybersecurity_standardisation_2022.

Verrier, Julien. « La cybersécurité industrielle à l'ère de l'Industrie 4.0 ». RiskInsight, 2021. https://www.riskinsight-wavestone.com/en/author/julien-verrier/.

5. INDEX OF TABLES

Table 1 : Presentation and brief description of main sources 8
Table 2 : Presentation and brief description of DATA 11

LCAMP

Learner Centric Advanced Manufacturing Platform

Co-funded by
the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.