Securing Critical Infrastructure across Cyber and Physical Dimensions
Editors: Gabriela Ciocarlie, Jianying Zhou, sp4-23@computer.org

Current Perspectives on Securing Critical Infrastructures' Supply Chains

Rodrigo Roman
University of Malaga, Spain

Cristina Alcaraz
University of Malaga, Spain

Javier Lopez
University of Malaga, Spain

Kouichi Sakurai
University of Kyushu, Japan

***Abstract*—The advances brought by digitalization and paradigms like the Industry 4.0 and beyond are transforming the landscape of Critical Infrastructures and their supply chains. Thanks to the integration of numerous emerging technologies, it is possible to deploy new services that enhance transparency and trust in the management of supply chains, amongst other benefits. However, as a side effect of these transformations, supply chains are becoming even more intertwined and complex – which in turn also increases the number of threats that can target them. In order to better understand what are the approaches that can be used to protect this ecosystem, alongside with the issues that are associated with the integration of such protection strategies, this paper provides an overview of the potential solutions (both in terms of existing and prospective technologies) given the existing threats and challenges.**

■ **SUPPLY CHAINS** are one of the cornerstones of any society. Since ancient times, it has been essential to procure citizens with the goods they need to work their jobs and live their lives. Therefore, it has been always crucial to establish networks of entities, resources and activities with the aim of connecting producers, distributors and consumers. Such networks have evolved greatly: from local supply chains and trade routes like the Silk Road, to the more global and complex actual supply chains. In fact, many of the technological advances of modern history have been applied to improve the efficiency and effectiveness of supply chains: from transportation (e.g, railways, trucks, cargo vessels) to long distance communications (e.g., telegraphy, telephones), logistics (e.g., pallets, containerization), and computerization. As a result, we now live in a completely interconnected world in which many goods are available worldwide, and where any disturbance in these supply chains would in turn disrupt the economy and the overall functioning of society.

The nature of such disturbances has also evolved over time. With the advent of digitalization and paradigms like the Industry 4.0 and beyond, which have brought an increased interconnection and information transparency thanks to various emerging technologies (e.g., Internet of Things), malicious actors have now more opportunities to manipulate any element of a supply chain remotely, causing harm to operations, assets, individuals, and even society as a whole. In fact, the number of attacks targeting supply chains has increased during last years, where one single incident (e.g. Kaseya, Solarwinds Orion) has been able to affect different industries and sectors without much additional effort. As a result, the resilience and security of supply chains has been declared a national priority by countries and supranational entities such as the United Stated of America and the European Union, requiring the integration of protection mechanisms at all levels.

Achieving such resiliency and security is even more important in the context of critical infrastructures (CIs) – essential systems and assets, such as financial services, public administration, and energy sectors, that are so vital to a nation that their incapacitation would have a debilitating impact on society. All CI sectors require various goods and services, including specialized equipment (e.g., nuclear equipment in the nuclear sector) in order to operate properly, and hence they require of specific supply chain networks that are able to produce and distribute such goods. Therefore, in this context of digitalization and hyperconnectivity, it is important to understand what are the main threats and challenges that affect these supply chains, as well as what are the potential solutions that may be applied to limit their impact.

However, when discussing the security aspects of supply chains in the specific context of CIs, it is important to not lose sight of the security aspects of CIs themselves. The reason is simple: both supply chains and CIs are closely intertwined. For example, many of the resources and activities that are crucial to have a functional supply chain network are, in fact, CIs themselves, such as manufacturing, transportation, communications, and information technology. In addition, many CIs are part of the supply chain network of other CIs, since the goods produced by one of them are needed by others (e.g., the water produced by the water sector and consumed by the healthcare sector and the agriculture sector). Moreover, the supply chain sector itself is considered by some experts as a CI, given the underlying technologies used and the impact on society due to potential disruptions.

CURRENT CONTEXT

Supply chains are inherently complex. They are comprised of multiple tiers of stakeholders (from suppliers and providers to other supporting entities like certification bodies) interacting with each other through various physical and digital services (e.g., production, transportation, certification, and usage), in order to exchange various types of goods, including physical ones such as medical supplies, digital such as software libraries, and hybrid such as hardware components with embedded firmware. These services are made possible by various assets that conform the supply chain ecosystem, including fixed infrastructures (e.g., buildings), mobile infrastructures (e.g., transport vehicles), logistic units (e.g., labels, pallets), a specialized workforce, information technologies (IT) infrastructures, and operational technologies (OT) systems and networks.

Precisely, one of the main developments in both critical infrastructures and their supply chains is their digitalization [1]. Although supply chain ecosystems are highly heterogeneous, with dissimilar requirements depending on their relevance (e.g., bicycle supply chains vs. airplane supply chains), all of them without exception are increasingly dependant on IT technologies. For example, various industrial sectors that make up supply chains – including those belonging to CIs – have become “digitally transformed industrial settings”, where closed systems have evolved into highly interconnected systems – not only for human administrators and operators, but also for the industrial devices themselves. This way, due to better measurement capabilities and remote control, it is possible to improve various services such as the ability to react against unexpected scenarios. As for the impact of this transformation in supply chains, it has improved the availability of information to all partners, which brings numerous benefits such as monitoring the state and location of parts on demand and in real-time, and predicting potential availability problems that may affect the production, integration, and distribution of goods.

This digitalization is not limited to the integration of traditional IT technologies: novel and emerging technologies such as the (industrial) Internet of Things ((I)IoT), Cloud Computing, Edge Computing, Artificial Intelligence (AI), Machine-Learning (ML), Augmented Reality (AR), Virtual Reality (VR), eXtended Reality (XR), and Digital Twins (DT) are being integrated as well [2]. The reason is simple: they complement and/or improve existing services, helping in various cases to maintain or lower operational costs. For example, not only the amount of information about the state of all the elements of an ecosystem can increase exponentially, but also the ability to intelligently analyze such information in a scalable manner and present it to relevant parties – both in the factory floor and at a business level – increases as well. This can facilitate the introduction of better transparency, trust, and traceability. Moreover, these technologies can also be used to improve supply chain cybersecurity, providing on-demand, continuous intelligent monitoring.

A side effect of this digitalization is the increased dependencies among all entities, at all levels. From a broad perspective, CIs are now more dependent on multiple physical and digital resources – from the high-level, cross-domain interactions between specific verticals (e.g., maritime transport services and telecommunication systems) to the low-level, internal interactions between technologies (e.g., IIoT and control processes). This hyper-connected scenario not only increases the complexity of managing, operating, and protecting a CI, but also increases the complexity of their supply chains. On the one hand, supply chain actors are more dependent on each other due to their own digitalization. On the other hand, CIs need to manage even more supply chains in order to integrate the necessary resources to implement not only end-user services (e.g., on-demand manufacturing) but also operational services (e.g., traceability of materials and goods).

It is necessary to also understand that there are other not so common factors that can influence existing supply chains, as we have been able to realise recently. One of those examples has been the COVID-19 pandemic, that has shown several underlying problems related to the implementation of the just-in-time principles. Additionally, it has demonstrated that social services, online shopping, and even recreational spaces can be considered critical infrastructures, due to their importance in current society [3]. A second example is global climate change, that is adding further pressure to implement operational services related to more sustainable operations. In this sense, there is an increased complexity in a number of services in order to consider environmental factors like, for instance, the monitoring of carbon footprint in traceability services, and the integration of environmental and social practices in certification processes.

Finally, it is crucial to consider how the heterogeneity of actors in the supply chain ecosystem influence over the various factors described above. In particular, one major issue is the technical and human resources required to integrate and maintain all services linked to the digitalization of the ecosystem and the interactions among the actors. Not all companies have those resources available due to budgetary or size constraints: for example, in Europe, above 99% of the companies are small and medium-sized enterprises (SMEs). Nevertheless, in terms of speaking of human resources, we also need to consider the need to develop a skilled workforce considering various challenges such as an aging population in many zones of the world.

EXISTING THREATS

As we have mentioned, the digitalization process has greatly increased the complexity of CIs and their supply chains. As a direct consequence, the attack surface and the amount of potential vulnerabilities and weaknesses has increased as well – which in turn has multiplied the amount of threats that can target these ecosystems. However, it is important to note that there are several weaknesses in supply chains that are demanding a solution since before the advent of Industry 4.0. Such threats not only encompass the digital dimension but also the physical one: from general threats against the whole system (e.g., sabotage, service disruption) to others against goods (e.g., manipulation, counterfeits, theft), information (e.g., intellectual property theft), and other services (e.g., piracy, smuggling).

There are several works that have aimed to provide a **taxonomy** of potential threats that can affect supply chain ecosystems from different perspectives. For example, *NIST Special Publications 800-30r1 and 800-161r1* [4] analyze such threats from the point of view of risk analysis. As such, it relies on the identification of the most critical actors, services and assets, paired with a study on the likelihood and impact caused by the successful execution of a threat. Such threats are classified according to the cyber kill chain of Advanced Persistent Threats (APT) campaigns: reconnaissance, weaponization, delivery, exploitation, action & objectives execution, and command & control. Most of these threats focuses on potential attacks against the IT infrastructures, although other aspects (such as structural, environmental, and accidental failures) are also considered.

Another example is the *threat landscape for supply chain attacks* by the European Union Agency for Cybersecurity (ENISA) [5]. This taxonomy focuses on complex attacks launched by sophisticated cyber crime groups that target more than one actor (suppliers and customers) of the supply chain ecosystem. In particular, the taxonomy organizes every attack into four parts: i) attacks against the supplier (IT, physical, social and counterfeiting attacks), ii) supplier assets targeted (software, information, processes, people, and hardware), iii) attacks against the customer (IT, physical, social, counterfeiting and trusted relationship attacks), and iv) customer assets targeted (software, information, processes, people, bandwidth, and financial).

Both taxonomies focus mostly on **threats** against IT infrastructures. The reason is simple: the digitalization of supply chains and their intertwined nature causes a wider attack surface, but also facilitates the existence of multiple attack paths. This way, a malicious adversary can use any vulnerable IT infrastructure as an entry point to take control of any part of the supply chain infrastructure – being it services (e.g. information exchange), assets (e.g. OT networks), or even the goods themselves (e.g. software libraries or firmware). It should be noted, though, that threats of other nature, such as physical vulnerabilities (e.g. improper tamper-proof packaging), can also be used as entry points to launch IT-based attacks (e.g., firmware manipulation).

Due to its increasing importance, one particular attack chain described in both taxonomies needs to be highlighted, that is, the abuse of software elements. This abuse is not only limited to exploiting vulnerabilities in specific software components (e.g., Log4J library exploits) to gain access to the infrastructures. In many cases, adversaries are hijacking the software supply chain to inject malicious functionality, which can be later exploited once they are deployed at a target infrastructure. Such functionality ranges from malicious back doors, such as in the SolarWinds Orion attack, to destructive ransomware, such as in the Kaseya attack. Moreover, adversaries are also targeting build automation processes, open source code repositories, and even developers.

Although these taxonomies provide a comprehensive overview of the threats that affect existing supply chains, it is necessary to highlight additional issues that exist in this particular context, which need to be carefully considered. One of such aspects is the *specific threats against emerging technologies* (e.g., IoT, cloud/edge, AI, DTs) that are being integrated into critical infrastructure ecosystems and their supply chains. For example, it is essential to carefully consider the challenges related to the limited capabilities, Internet accessibility, and software maintenance issues of IIoT devices, which are well known. In fact, various sophisticated cyber crime groups such as the Conti group have explicitly mentioned how they use IoT devices as entry point to organizations' infrastructures. As for cloud and edge technologies, the use of shared virtualization infrastructures is a double-edged sword. On-demand resources can be deployed by any supply chain actor, but that includes malicious insiders. Advanced metrics can be used to refine and optimize the behaviour of the services, yet limited forensic information will be available after an attack. Moreover, internal services are outsourced to external cloud companies with a pay-per-use

Table 1: Summary and examples of existing threats

Threat Sources	**Adversarial** (from individual to organizations and nation-states), **Accidental**, **Structural** (IT/OT, hardware, software), **Environmental** (natural, man-made, infrastructure failure)
Assets Targeted	**Software**, **Hardware**, **Data** (Configurations, IP), **Information flow**, **Processes and Services**, **Emerging and Prospective technologies**, **People**, **Stakeholders**, **Financial**
Attack Techniques	**Reconnaissance** (OSINT, sniffing), **Social Engineering** (phishing, manipulation), **Abuse of Vulnerabilities** (malware, configurations), **Abuse of Trust** (counterfeiting, trojan, shared environments), **Sabotage** (jamming, destruction, degradation), **Corruption**, **Theft** (goods, IP), **Smuggling**, **Piracy**

model that ensure a certain quality of service, except when compliance violations occur due to first or third party issues and availability is severely reduced.

The threats associated to AI are related not only to the cybersecurity challenges of its extended ecosystem of processes, tools, artefacts, models, stakeholders, and data, but also to other subtler issues. For instance, it is not possible to understand the decisions made by most AI algorithms due to poor explainability. As a result, AI-supported processes might provided suboptimal or even plain wrong advice due to various factors – including malicious manipulation. Moreover, AI can also be used as a weapon against our infrastructures, that is, not only adversaries can make use of AI to improve their OSINT capabilities, but also take advantage on advances in areas such as image generation and language models to launch various kinds of social attacks – from phishing to hostile social manipulation. Finally, the main challenge of DTs is related to their nature as virtual representations of physical systems. Their potential as a monitoring and predictive system is only achievable if there is a bidirectional connection with such physical systems. This situation opens new avenues to malicious attackers, which can manipulate one dimension (e.g., physical) to influence the other (e.g., digital).

Beyond the need to consider the integration and maintenance of specific emerging technologies, it is also essential to plan against *threats targeting their very own supply chains*. Two clear examples of this are IoT and AI technologies, whose relevance has caused entities like ENISA to explicitly consider them in their guidelines. These guidelines describe various threats that are relevant to these contexts, as well as several security considerations that should be adopted across their whole supply chain – including security awareness, security by design, and integrity metrics. It should be noted that a small subset of these threats are specific to the supply chain of a particular technology. One example is the information related to the creation of an AI model: an adversary can access this information to develop specific adversarial attacks tailored to that particular model, and even can stealthy manipulate such information in order to create flawed models that will behave as Trojan horses – carrying the will of the adversary.

CHALLENGES OF THE ECOSYSTEM

The complexity of the aforementioned threats, whose summary is presented in **Table 1**, and the intertwined nature of the ecosystem requires a holistic defense approach that can provide comprehensive protection against such threats. However, there are several **challenges** in these supply chain ecosystems that complicate the task of developing and deploying security and privacy solutions – both proactive and reactive – that can be integrated by all participants.

One of such challenges is the *lack of transparency and cooperation*. The central idea behind this challenge is that, even with the current improvements on information availability, it is difficult to securely obtain accurate information about another participant of the supply chain – even more when this participant is located at a distant tier. The nature of this information is very broad, as it concerns not only information related to the operations of each participant, but also information related to their cybersecurity. One example of this is threat intelligence, which would allow all participants to be aware of current threats and their tactics, techniques and procedures. Beyond the accuracy of the information, another crucial aspect is its privacy: even between trusted partners, it is necessary to ensure that no sensitive information is shared.

Another challenge, related to the previous one, is the need to *ensure trust* in the behaviour and assets of partners. As aforementioned, not only the goods but also the services provided by partners can become an avenue for cyberattacks. Therefore, it is essential to certify that all interactions between partners are exempt from security concerns. Precisely, there are various security certifications, either focused on supply chains (e.g., ISO 28000, ISO/IEC 20243) or specific to certain technologies (e.g., IoT and ETSI EN 303 645) that can help to achieve this goal. However, compliance with such certifications improve but do not guarantee security assurance, mostly because compliance is checked at a point in time; and even if security procedures are in place, a determined and hostile actor can take control of assets at any time.

Lastly, one challenge is linked to the concept of *cascading failures* or cascade effects, an area that has been extensively studied in both CIs and supply chains. This area studies how faults propagate unpredictably in intertwined ecosystems, mostly due to hidden interdependencies. In the context of cybersecurity, cascade effects must be considered from two points of view: from the integration of security and privacy services, and from their availability. In terms of integration, all protection services need to consider the existence of cascade effects, and incorporate this knowledge into their functionality (e.g., risk assessment and redundancy policies, identification of weak links). In terms of availability, it is crucial to consider how a malicious attack might hinder access to such services, either directly (e.g., service hijacking) or indirectly (e.g., power outages).

POTENTIAL SOLUTIONS

To address the threats that thrive in such hyperconnected and heterogeneous contexts, and to implement a holistic defense approach, it is wise to consider a defense in depth that integrates existing security solutions for CIs and supply chains. As with any defense in depth, it involves mainly two planes: i) regulatory frameworks to establish common security and privacy controls at different scales and dimensions (at the CI level, between CIs and in the entire supply chain); and, ii) technical security approaches focused on providing protection strategies based on robust design principles.

In the **regulatory plane**, there are already various *directives, standards and recommendations* in place to create interoperable ecosystems where regulated operations can be executed – both locally and between organizations (cf. **Table 2**). The General Data Protection Regulation (GDPR) on supply chain risks, or the Network and Information Security (NIS)-2 Directive are two clear examples of these progresses, and there are also other standards, guidelines and good practices defined by international organizations, such as ISO/IEC 27000 series, NIST SP 800-161r1, SP 800-53r5, NISTIR 8276, among others – as also stated in [1]. All these regulations serve as tractor elements to transparently manage operational processes and build trustworthiness on a strongly globalized market, where it is necessary to identify actors and actions, limit access, and establish and maintenance provenance of goods, processes and data. Although much remains to be defined in this field of application and, in particular, in the standardization of specific SW/HW supply chain security solutions, significant efforts are being made in this direction. The "*Cybersecurity Supply Chain Risk Management*" (C-SCRM) approach, recently published by NIST in SP 800-161r1 [6], precisely provides the guidelines for identifying and assessing cybersecurity risks from governance, as well as the tools to enable preparedness and resilience against unexpected threat scenarios [7].

For this preparedness and resilience, *dynamic risk management* is also relevant, especially when it comes to protecting inherently complex networks susceptible to APTs. Using traditional and recent (C-)SCRM approaches and methodologies (e.g. SP 800-161r1, NIST 800-53r5, ISO 31000:2018), it is possible to find services appropriate to the application context. These services mainly focus on (i) identifying and categorizing (process, supply, information, external, natural [7]) risks, and (ii) monitoring and assessing such risks using metrics, which are generally linked to assets, states and (inter-)dependencies. In order to automate the risk management process, automated monitoring solutions capable of mapping IT and OT assets and their relationships are needed to subsequently identify (zero-day) vulnerabilities and attack paths, and calculate costs and impact. For this estimation, traditional

Table 2: Directives, Standards and Recommendations

Acronym	Title	Year
CSA STAR	Cloud Security Alliance - Security, Trust, Assurance and Risk	2021
ENISA 10.2824/168593	Threat Landscape for Supply Chain Attacks	2021
ENISA 10.2824/314452	Guidelines for Securing the Internet of Things: Secure Supply Chain for IoT	2020
ENISA 10.2824/874249	Securing Machine Learning Algorithms	2021
ETSI EN 303 645	Cyber Security for Consumer Internet of Things: Baseline Requirements	2020
GDPR	General Data Protection Regulation	2016
ISA/IEC 62443 series	Industrial communication networks - Network and system security	2009-20
ISO/IEC 15408 series	Information security, cybersecurity and privacy protection - Evaluation criteria for IT security	2022
ISO/IEC 20243 series	Information technology - Open Trusted Technology ProviderTM Standard (O-TTPS)	2018
ISO/IEC 27000 series	Information technology - Security techniques	2016-22
ISO/IEC 27036 series	Cybersecurity - Supplier relationships	2013-22
ISO 28000:2022	Security and resilience - Security management systems – Requirements	2022
ISO 31000:2018	Risk management - Guidelines	2018
NIS-2	Network and Information Security Directive	2022
NIST SP 800-30r1	Guide for Conducting Risk Assessments	2012
NIST SP 800-53r5	Security and Privacy Controls for Information Systems and Organizations	2020
NIST SP 800-161r1	Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations	2022
NISTIR 8276	Key Practices in Cyber Supply Chain Risk Management: Observations from Industry	2021

analysis and modelling methodologies can be applied, such as (i) attack trees/graphs combined with learning models for interpretability [9], (ii) STRIDE-DREAD [8] to quantify and prioritise risks; (iii) graph theory to compute/predict interdependencies; or (iv) uncertainty theories to explore severity degree and tentative ripple effects together with disruptions in the supply chain, as the case of the global pandemic of 2020-2021 (analyzed in detail in [7]).

As part of governance, it is also crucial to consider *compliance with certifications* for assurance [10], especially applied to evaluate the cybersecurity and safety of CIs and their supply chains. To this end, it is widely recommended to establish conformity assessment schemes following: (i) existing standards and recommendations (e.g. ISO/IEC 27000, ISA/IEC 62443, ISO/IEC 15408 or ISO/IEC 27036 series), as well as (ii) the official security certification framework established within the EU Cybersecurity Act [11], managed by ENISA. But despite these advances, there is still no full guarantee of ensuring sustainability in the auditing process due to the dynamic nature of the application context. This issue has raised the current need to move towards *continuous certifications* supported by automated verification processes. These processes must incorporate monitoring services capable of mapping the requirements extracted from the standards and verifying that these requirements are still valid. Currently, there are already significant advances in terms of official programs (such as the Security Trust Assurance and Risk (STAR) for cloud services), and the establishment of cyclic methodologies, based on the posture of Plan-Do-Check-Act [10], with support in automatic monitoring services and the extraction of HW/SW usage descriptors to be evaluated according to metrics and initial conditions.

As for the **technical plane**, interoperable and secure IT and OT networks must be subject to strict *hardening measures*, both in terms of perimeter and (legacy) devices. Many of these are already considered by experts [12], who have extracted the first cybersecurity requirements to protect critical applications of the supply chain. Experts stress the relevance of protecting the entire value chain, in terms of confidentiality, integrity, authentication (using federated schemes and decentralized and self-sovereign frameworks), and access control, but also in terms of distributed detection and response to anomalies or intrusion. Yet, for a comprehensive defense and business continuity, these latter measures must be based on proactive approaches, perhaps supported by disruptive technologies [13], [14], [15]. Among the technologies most widely applied today, we can highlight the following: (i) AI/ML models and federated learning to predict anomalous states and conditions; (ii) Big Data to deal with large volumes of data and rapid decision-making; (iii) cloud/edge to coherently distribute security services in CIs and throughout the entire supply chain; (iv) DTs to simulate states equivalent to the physical counterpart, identify risks, make decisions and react accordingly; and (v) 5G to streamline the wireless interconnection of operational processes [15]. All of these technological capabilities can even enhance *situational awareness and attractive ways to react in a timely manner* with support of specialized platforms, such as Security Information and Event Management (SIEM) and Security Operations Centers (SOC), to create cyber intelligence for a more coordinated response. Moreover, many of the anomalies reported throughout these trustworthy platforms are normally related to vulnerabilities associated to the SW supply chain itself, and come from open source components. For this reason, best practice for *secure development* together with the use of Software Bill of Materials (SBOMs) strategies to detail information about SW components and dependencies, are recommended. Also, traditional *testing* methods and the use of modelling and simulation technologies, e.g. DTs, are good approaches to verify the integrity of components, as well as their functions and behaviour.

Integrity must also be part of the secure exchange of data in critical supply chain ecosystems to promote *transparency and trust*. To this end, it is possible to apply various technologies such as (i) standardized Electronic Data Interchange (EDI) formats (e.g., GS1 integrated as part of IoT consumer devices and RFID tags), (ii) Physical Unclonable Function (PUF) to prevent counterfeiting of goods and devices, and (iii) blockchain-enabled solutions based on smart contracts. Precisely, blockchain is a leading technology in the field of supply chain [14], as it enables *immutable traceability and accountability in workflows and tracking* [12]. In turn, it can be combined with other relevant technologies, such as: (i) AI models and EDI formats to streamline logistics and management processes; (ii) regulated access policies and authentication mechanisms for privacy and trust; and (iii) automatic monitoring and traceability services to predict inconsistencies, promoting accurate detection and response.

After assessing the efforts to secure supply chains, it is legitimate to think that there is sufficient progress in the protection of this area. However, there are various aspects that need to be further developed – especially when many of the CIs' goods and services are considered essential by governments, such as water or electricity. As such, the following section stresses next protection steps to be addressed in the future, so as to create trustworthy ecosystems with less cybersecurity risks.

NEXT PROTECTION STEPS

In the context of supply chains there are numerous disruptive technologies (some of which still unexplored) that can be used to implement hyper-connected processes based on complex solutions for verification, tracking, traceability and transparency – and even to implement protection mechanisms themselves (e.g., DTs for prevention and detection, XR for improving human response). However, this integration will also bring numerous novel challenges that can disrupt the security and resilience of the supply chain itself. This impact is mostly related to the inherent features of these disruptive technologies, whose security is still at a low state of maturity due to their novelty. One clear example are blockchain technologies, which still presents, for instance, limitations in terms of scalability, storage and transaction cost, policy management for regulated access, and efficient and fast traceability of blocks and privacy [14].

Another aspect to consider is the evolution of existing industrial paradigms, such as the vision of the Industry 5.0. Here, it is expected to integrate solutions that not only address (i) innovation and digital transformation focused on human-centric applications, but also solutions that ensure (ii) good use of existing resources without impacting energy consumption and climate change, as well as (iii) resilience to potential threats [14], [13]. This sets the pace not only for what types of technologies will be integrated into future supply chain ecosystems and how, but also for the features that might be expected in protection mechanisms. Examples of such features are *lightweight security solutions* to comply with the energy requirements, and also criteria related to *modularity* to meet constant operability in the field.

Continuing with the evolution of existing technologies, there are various prospective technologies (corresponding to Industry 5.0 and beyond) that are expected to form part of the supply chain. Among the technologies mentioned in [13], we stress cobots (collaborative robots), quantum computing and 6G technology, whose launch could accelerate interconnection processes

Table 3: Current advances, next steps and enabling technologies

Current protection advances	Potential technologies	Next protection steps	Potential technologies
Directives, standards and recommendations	AI	Continuous defense in depth (*)	AI
Dynamic risk management	ML	Continuous regulation	ML
(Continuous) certification	Federated learning	Continuous certification (*)	Federated learning
Confidentiality and integrity	Blockchain	Privacy-preservation	Blockchain
Authentication and authorization	Cloud/edge	Continuous validation and testing (*)	Cloud/edge
Detection and situational awareness	DTs	Security by design principles	DTs
(Coordinated) response	PUF	Zero-trust principles	PUF
Secure SW/HW development	5G	Strategic plans and new roadmaps	Cobots
Validation and testing		Cybersecurity awareness and training	XR/AR/VR
Auditing, traceability and accountability		Automatic response (*), trust	Quantum comp. / Quantum-safe
		Recovery and reconfiguration	6G/Beyond

*: research still needed to find improved designs with respect to the current ones, in terms of simplicity and modularity.

and the management of goods. However, this technological advance may also change the priorities of the current CIs' supply chain security roadmaps (e.g., [2]) so as to contemplate, for example, future *quantum-safe approaches* and foster resistance against potential quantum attacks [13]. At the same time, it is important to consider how these technologies can also be applied to improve security and privacy, such as 6G for high connectivity of protection services, and cobots for physical infrastructure security.

During this evolution, international cooperation for *continuous regulation and certification* may become mandatory, especially when, as previously discussed, the current trend is to integrate emerging technologies from practically their infancy to boost innovation, enhance the production chain and foster industrial globalization. In addition, this trend may require the establishment of *specific privacy-preservation techniques*, *rigorous and automated validation processes* and the application of *zero-trust and security by design principles*. Proven security designs and controls must be integrated into these new technology streams to maintain trust in an ecosystem that may consolidate in the coming years.

The attempt to regulate digital sovereignty and its management among organizations and countries may also lead to the need to establish *future strategic plans and new roadmaps* beyond the existing ones. Government institutions and international organizations can initiate coordinated actions to impose limits on access to private data, establish guidelines to enforce integrity and transparency in/between organizations, and protect end-users' privacy. Such plans may also consider *cybersecurity awareness and practical training programs*. All stakeholders should be aware of their rights and obligations within the supply chain ecosystem, and commit to apply good practices and security. Similarly, experts in the field of education will have to update training models to adapt them to each new context of application in line with new trends. For preparedness, simulation technologies supported by cyber-range models and DTs can be good approaches for this purpose, as they do not interfere with real environments. In addition, the use of these technologies can provide feedback to other protection services (related to prevention, situational awareness and risk management) by dynamically updating their processes according to the learning outcomes about weaknesses (e.g., human errors) or vulnerabilities exploited.

Last but not least, the development of self-healing solutions for CIs' supply chains is essential to ensure *continuous resilience*. Recovery and reconfiguration of states, processes and parameters in optimal times must predominate within protection schemes to ensure the provision of essential services, as well as business continuity. Also, coordinated actions guided by distributed intelligent solutions, such as interconnected DT networks, can be a good approach. Yet, while these virtual networks can help create a common repository of cyber intelligence and promote proactive actions, two questions arise at this point: (i) what types of automated decisions can be delegated to be made in extremely critical environments without affecting the confidence of one or more organizations, and (ii) how to implement such decisions to achieve such *trust*.

CONCLUSION

The digitalization of supply chains – not only in the context of CIs but also as a whole – has brought various novel threats to this area, which are mostly related to the protection of their underlying technological paradigms and their innovative services in a hyperconnected environment. Even so, the objectives that must be achieved in order to protect these ecosystems are known, and there are multiple efforts to bring security and privacy mechanisms to these ecosystems from both the regulatory and technical perspectives. These advances are summarized in **Table 3**, which also includes the needs that may become a priority in the near future. From the table we conclude that, although important advances have already been made in the security and privacy of supply chains, there are still a number of outstanding issues that need to be addressed through research, continuous regulation, and technical procedures, especially when the digital transformation depends mainly on existing and prospective technologies.

ACKNOWLEDGMENT

This work has been supported by the EU H2020-SU-ICT-03-2018 Project No. 830929 CyberSec4Europe (cybersec4europe.eu) project.

REFERENCES

1. A. Morot and S. Hón, “Cybersecurity of the supply chain”, SCOR, The Art & Science of Risk, 2022.
2. E. Markatos et. al., “Research and Development Roadmap 3”, Deliverable D4.5 of CS4E: Cybersecurity for Europe, funded by the European Union’s Horizon 2020 Research and Innovation Programme (No. 830929), 2022.
3. C. Scholz, S. Schauer, and M. Latzenhofer. “The emergence of new critical infrastructures. Is the COVID-19 pandemic shifting our perspective on what critical infrastructures are?”, *International Journal of Disaster Risk Reduction*, no. 83, 2022.
4. J. Boyens, A. Smith, N. Bartol, K. Winkler, A. Holbrook, and M. Fallon. “Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations”, NIST Special Publication (SP) 800-161 Rev. 1, 2022.
5. I. Lella, M. Theocharidou, E. Tsekmezoglou, A. Malatras, S. Garcia, and V. Valeros (eds.). “Threat Landscape for Supply Chain Attacks”, ENISA Report, 2021.
6. J. Boyens, A. Smith, N. Bartol, K. Winkler, A. Holbrook, and M. Fallon, “Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations”, NIST SP 800-161r1, 2022.
7. D. Ivanov, “Supply Chain Risks, Disruptions, and Ripple Effect”, *Introduction to Supply Chain Resilience*, Classroom Companion: Business, Springer, Cham, pp. 1-28, 2021.
8. G. Kavallieratos, C. Grigoriadis, A. Katsika, G. Spathoulas, P. Kotzanikolaou, S. Katsikas, “Risk assessment and control selection for cyber-physical systems: a case study on supply chain tracking systems”, *J. Surveill. Secur. Saf.*, 3(4), pp. 128-49, 2022.
9. A. Nadeem, S. Verwer, S. Moskal and S. J. Yang, “Alert-Driven Attack Graph Generation Using S-PDFA”, *IEEE Transactions on Dependable and Secure Computing*, vol. 19, no. 2, pp. 731-746, 1, 2022.
10. A. d. S. Oliveira and H. Santos, “Continuous Industrial Sector Cybersecurity Assessment Paradigm: Proposed Model of Cybersecurity Certification”, 18th International Conference on the Design of Reliable Communication Networks (DRCN), pp. 1-6, 2022.
11. European Commision, “Information and Communication Technology cybersecurity certification (”Cybersecurity Act”)”, 526/2013, COM(2017) 477 final, 2017.
12. S. Fischer-Hubner, C. Alcaraz, A. Ferreira, C. Fernandez-Gago, J. Lopez, E. Markatos, L. Islami, M. Akil, “Stakeholder Perspectives and Requirements on Cybersecurity in Europe”, *Journal of Information Security and Applications*, vol. 61, 2021.
13. P. K. R. Maddikunta, Q. Pham, Prabadevi B, N Deepa, K. Dev, T. R. Gadekallu, R. Ruby, M. Liyanage, “Industry 5.0: A survey on enabling technologies and potential applications”, *Journal of Industrial Information Integration*, vol. 26, pp. 100257, 2022.
14. P. Bhattacharya, N. Madhani, C. Trivedi, B. Bhushan, S. Tanwar, G. Sharma, P. N. Bokoro, R. Sharma, “Blockchain for Industry 5.0: Vision, Opportunities, Key Enablers, and Future Directions”, *IEEE Access*, vol. 10, pp. 69160-69199, 2022.
15. A. Rejeb, J.G. Keogh, “5G Networks in the Value Chain”, *Wireless Pers. Commun.*, vol. 117, pp. 1577–1599, 2021.

Rodrigo Roman is an associate professor at the University of Malaga, Spain. Contact him at rroman@uma.es.

Cristina Alcaraz is an associate professor at the University of Malaga, Spain. Contact her at alcaraz@uma.es.

Javier Lopez is a full professor at the University of Malaga, Spain. Contact him at javierlopez@uma.es.

Kouichi Sakurai is a full professor at the University of Kyushu, Japan. Contact him at sakurai@inf.kyushu-u.ac.jp.