BITSIGHT | EuroDefense Portugal

WHITE PAPER

The European Supply Chain Battlefield: Cybersecurity, National Defense, and the NIS2 Regulation

Contents

1. Introduction

Nowadays organizations rely on a vast network of suppliers, service providers, and third-party vendors. This complex web of interdependencies introduces significant challenges, as vulnerabilities within the supply chain can serve as gateways for cyber threats.

Supply chain attacks have become a big concern, with adversaries leveraging software dependencies, contractors, hardware and managed service providers (MSPs) to attack critical infrastructures.

The European Union's NIS2 Directive underscores the urgency of addressing supply chain security as part of a broader cybersecurity risk management strategy. Some articles of the directive establish stringent requirements for organizations to assess and mitigate cybersecurity risks within their supply chains, embedding cyber risk measures into contractual obligations and fostering EU-wide coordinated security risk assessments.These regulatory advancements reflect the growing recognition that a robust cybersecurity posture must extend beyond an organization's internal systems to encompass its entire ecosystem of partners and suppliers.

This topic is particularly challenging due to the diversity of supply chain attacks. Threat actors exploit a significant amount of techniques, from zero-day vulnerabilities and malicious software updates to social engineering and hardware compromises. Those attacks may produce cascading effects that could compromise not just a single organization, but an entire industry.

Moreover, supply chain cybersecurity is not only a corporate concern—it is increasingly a matter of national security. A single compromise can trigger widespread disruptions, affecting critical infrastructure, governmental institutions, and strategic sectors such as energy, telecommunications, and finance. Many of the documented attacks have directly impacted the defense sector, demonstrating how vulnerabilities in the supply chain can become a point of entry for nation-state actors engaging in cyber espionage, sabotage, and systemic destabilization.

In this article, we discuss how the NIS2 regulation improves the cybersecurity resilience of European organizations, with a special focus on supply chain security. By enforcing stricter security measures, risk management protocols, and coordinated oversight, the directive aims to reduce the likelihood of large-scale cyber incidents. As a result, it will play a crucial role in mitigating threats to national cybersecurity, safeguarding essential services, and ensuring the stability of digital ecosystems across Europe.

2. Supply Chain and National Security

Supply chain attacks are among the most critical security challenges faced by nations. Although there are no internationally binding rules specifically addressing supply chain cybersecurity, some countries have implemented legislation or policies to regulate supply chains. Efforts at the United Nations focus on establishing norms through diplomatic negotiations, but these norms are not binding rules or principles. One section of the Open-Ended Working Group (OEWG) 3rd Annual Progress Report[1] emphasizes the importance of voluntary, non-binding norms for reducing risks to international peace, security, and stability. These norms serve as standards of conduct for states in their use of Information and Communications Technologies (ICTs). Key aspects include:

- States should not allow their territory to be used for wrongful acts involving ICTs.
- Protection of critical infrastructure (CI) and critical information infrastructure (CII) is crucial.
- States need to strengthen measures to secure CI and CII, including international collaboration on best practices and recovery mechanisms.
- Norms should evolve over time, with existing rules being implemented alongside the development of new norms.
- **Supply chain security is a priority, requiring international cooperation and engagement with the private sector.**
- Security-by-design should be embedded in ICT product development, and public-private partnerships are vital for improving supply chain integrity.
- The Voluntary Checklist of Practical Actions was introduced as a living document for guiding implementation.

One norm[2] in the same report underscores the need for states to ensure supply chain integrity to foster trust in ICT products and prevent misuse. Recommended National-Level actions in this area include:

1. Establish comprehensive, transparent frameworks for supply chain risk management.
2. Promote good practices among ICT suppliers and vendors to enhance product security and quality.
3. Require ICT vendors to integrate safety and security throughout the product lifecycle.
4. Implement legislative safeguards for data protection and privacy.
5. Prohibit harmful hidden functions and vulnerabilities in ICT products.
6. Strengthen partnerships with the private sector to secure ICT supply chains.

Regarding international cooperation, the focus should be on fostering equal opportunities for all states to compete and innovate in ICT development with the goal to enhance global social and economic growth, maintain international peace and security, and protect national security and public interests.These measures aim to reduce vulnerabilities, foster collaboration, and promote best practices to enhance the global ICT ecosystem's security.

Let's now examine two compelling examples of how Europe has addressed supply chain risks from a national security perspective—specifically in the use of certain technologies within 5G infrastructure and cybersecurity products. The following sections provide further details on these cases, where concerns about the trustworthiness and reliability of technology suppliers were brought to the forefront.

[1] Report of the open-ended working group on security of and in the use of information and communications technologies 2021–2025

[2] Norm i, page 31, Report of the open-ended working group on security of and in the use of information and communications technologies 2021–2025

2.1 The EU's 5G infrastructure challenge

The importance of establishing mechanisms to address supply chain security for emerging technologies became clear in March 2019, when a resolution by the European Parliament highlighted security concerns related to the growing presence of Chinese technology in the EU's 5G infrastructure[3]. This threat prompted the European Commission[4] to urge Member States to carry out a coordinated national risk assessment of 5G network infrastructure. These assessments aimed to identify the main threats and actors affecting 5G networks, determine the sensitivity of 5G network components, functions, and examine various types of vulnerabilities, including technical vulnerabilities and those potentially arising from the 5G supply chain[5].

To address these security challenges, the NIS Cooperation Group created the EU Toolbox of Risk Mitigating Measures ("the Toolbox") on January 29, 2020[6]. The Toolbox outlines strategic, technical, and supporting actions to tackle risks associated with 5G networks, including their interdependencies with critical infrastructure across EU Member States, and highlights both technical and non-technical threats, including those originating from foreign countries. The supply-chain risks are mentioned many times across the Toolbox document.

The Toolbox was not legally binding but served as a coordinated framework of risk management best practices. Despite its non-binding nature, Member States had strong incentives to adopt its recommendations. The implementation of these measures remained at the discretion of each Member State.

In June 2023, ongoing challenges regarding the implementation of the EU's 5G security framework were highlighted[7]. Commissioner Thierry Breton emphasized that three years after the adoption of the 5G security toolbox, nearly all Member States have integrated its recommendations into their national laws, enabling them to restrict or exclude suppliers based on security risk assessments. However, only 10 Member States have utilized these provisions to limit or ban high-risk vendors, a pace deemed too slow by the Commissioner, who also mentioned that sluggishness posed a serious security risk, exposing the Union to major dependencies and vulnerabilities. On the same day, Member States unanimously approved the second report[8] on the implementation of the 5G security toolbox. Furthermore, the Commission issued a communication confirming that decisions by certain Member States to restrict or exclude Huawei and ZTE from their 5G networks are justified and consistent with the toolbox's guidelines. The original Toolbox didn't name any supplier but this new document names suppliers. In complement to this second report, on the same day, the commission announced the next steps on cybersecurity of 5G networks, where it was emphasized that, among other things, "Member States should achieve the implementation of the Toolbox without delay"[9].

According to the Danish consulting firm StrandConsult, as of this article's writing (December 2024), 10 EU countries have implemented the EU's 5G toolbox, 6 have partially implemented it, 5 are in the process of implementation, and 6 have not started implementation.

While the EU's 5G cybersecurity framework has taken some steps to mitigate supply chain risks, vulnerabilities within cellular networks remain a pressing concern. Recent research[10] has highlighted that LTE and 5G networks contain exploitable flaws that could allow attackers to disrupt entire cities' connectivity, raising severe implications for both national security and economic stability. These vulnerabilities, which span authentication mechanisms and network slicing implementations, underscore the necessity for continuous reassessment of the security measures protecting the EU's telecommunications infrastructure. Given the growing reliance on 5G for critical services—including emergency response, healthcare, and industrial automation—ensuring robust and adaptable security policies remains paramount.

[3] Security threats connected with the rising Chinese technological presence in the EU and possible action on the EU level to reduce them
[4] Commission Recommendation - Cybersecurity of 5G networks
[5] EU Member States complete national 5G risk assessments
[6] Cybersecurity of 5G networks - EU Toolbox of risk mitigating measures
[7] 5G Security: The EU Case for Banning High-Risk Suppliers | Statement by Commissioner Thierry Breton
[8] Second report on Member States' progress in implementing the EU Toolbox on 5G Cybersecurity
[9] Commission announces next steps on cybersecurity of 5G networks in complement to latest progress report by Member States
[10] Cellular Security - Florida Institute for Cybersecurity Research

2.2 The Kaspersky Ban

On June 20th, 2024, the Department of Commerce's Bureau of Industry and Security (BIS) announced[11] the prohibition of Kaspersky Lab, Inc., the U.S. subsidiary of a Russia-based anti-virus software and cybersecurity company, from directly or indirectly providing anti-virus software and cybersecurity products or services in the U.S. or to U.S. persons. The prohibition also applied to Kaspersky Lab, Inc.'s affiliates, subsidiaries, and parent companies.

That groundbreaking decision meant that Kaspersky was generally no longer able to, among other activities, sell its software within the U.S. or provide any updates to software already in use. Enterprises using Kaspersky in the U.S. were encouraged to find alternative solutions. Kaspersky was allowed to continue certain operational activities in the U.S. until September 29, 2024.

This action was the first of its kind and is the first Final Determination issued by BIS's Office of Information and Communications Technology and Services (OICTS), whose mission is to investigate whether certain information and communications technology or services transactions in the United States pose an undue or unacceptable national security risk.

BIS determined that Kaspersky poses an undue or unacceptable risk to U.S. national security. According to BIS, U.S. organizations are at risk from their use of Kaspersky because:

- Kaspersky is subject to the jurisdiction of the Russian Government and must comply with requests for information. This may allow the Russian government access to certain information that could imperil U.S. organizations.
- Kaspersky may be able to access sensitive U.S. customer information through administrative privileges, in the provision of cybersecurity and anti-virus software.
- Kaspersky possesses the capability or opportunity to install malicious software and withhold critical updates, leaving U.S. persons and critical infrastructure vulnerable to malware and exploitation.
- Kaspersky's integration with other products increases the likelihood that Kaspersky software could unwittingly be introduced into devices or networks containing highly sensitive U.S. personal data.

This is not the first time the U.S. government has issued a ban on Kaspersky. In 2017, the U.S. government took action against Kaspersky, when the Department of Homeland Security issued a binding operational directive[12] requiring U.S. federal agencies to remove and discontinue use of Kaspersky-branded products on U.S. federal information systems. The National Defense Authorization Act (NDAA) for Fiscal Year 2018 later prohibited the use of Kaspersky by the U.S. federal government.

[11] Commerce Department Prohibits Russian Kaspersky Software for U.S. Customers
[12] BOD 17-01: Removal of Kaspersky-branded Products

2.2.1. The Impact on Europe

Before the ban, and despite a previous warning[13] launched in 2022 by BSI (Federal Office for Information Security), observations[14] from Bitsight indicate 14 million unique IP addresses communicating with Karspersky update servers, with Germany, Italy, Spain, and France leading the pack.

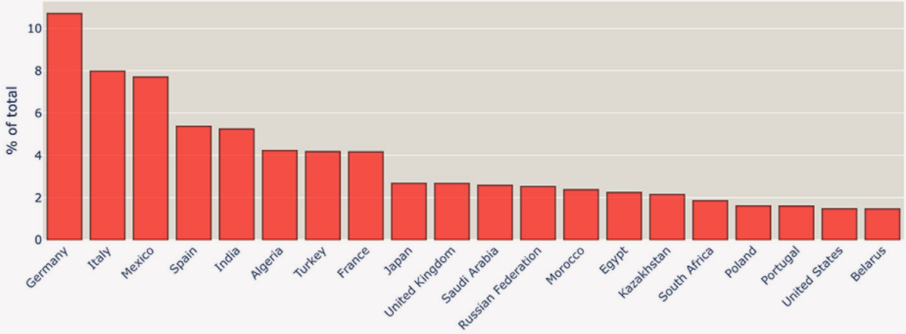

Figure 1 Percentage of unique IP addresses contacting Kaspersky servers

In many of the EU countries, as we can see in the figure below, this software was being used in critical sectors like manufacturing Technology (e.g. Service Providers), Healthcare, Government, and Public administration.

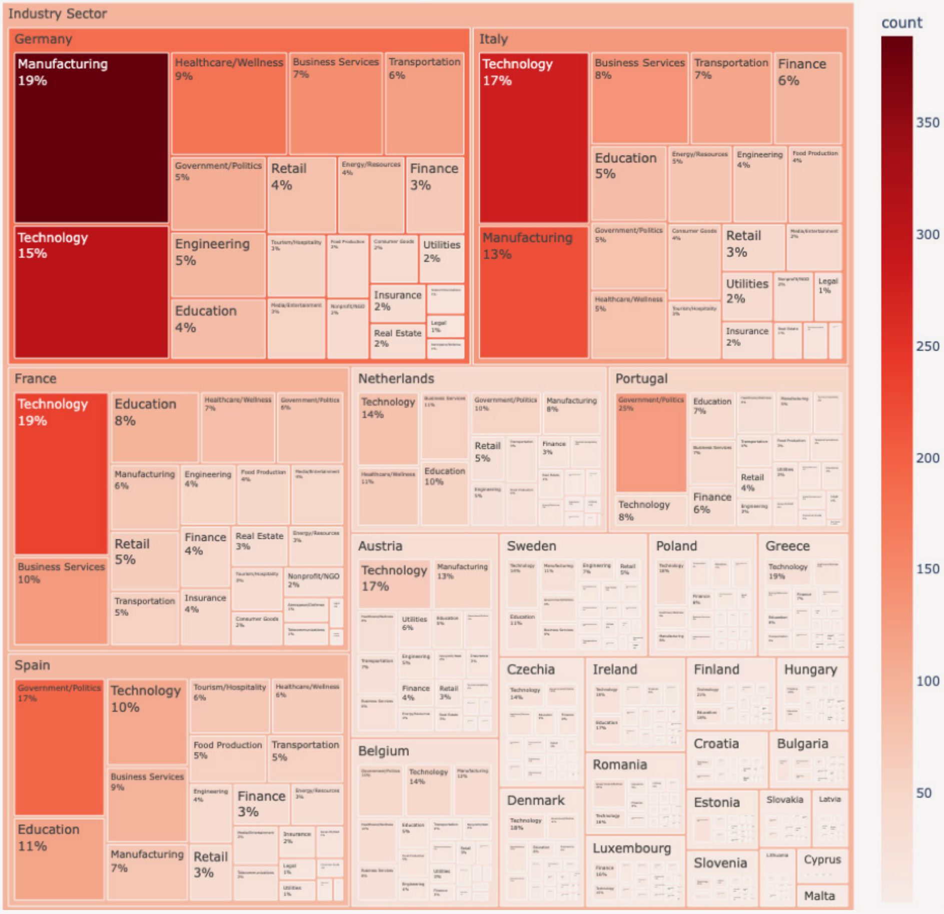

Figure 2 EU country/sector absolute count

[13] Warning about Kaspersky virus protection software according to §7 BSIG
[14] The Impact of the Kaspersky Ban

What impact has the US ban had on global and European usage of Kaspersky? Has it been effective? An analysis[15] from Bitsight shows that the ban has had a significant impact on global usage of Kaspersky, with dramatic decreases in usage also observed in organizations operating in countries that do not have formal bans on Kaspersky technology.

In April 2024, a pattern of nearly 22,000 global organizations and over 7 million unique IP addresses communicating monthly with Kaspersky update servers was observed. Around November 30, 2024, that number has fallen to around 8,000 global organizations and 2 million unique IP addresses.

Figure 3 highlights the rate at which organizations in various countries removed Kaspersky products between April and November 30, 2024. Interestingly, organizations in countries that did not impose outright bans on Kaspersky demonstrated a faster removal rate compared to those in the US. Notably, significant reductions in usage were observed in countries such as Germany, the UK, and Italy. These countries have either banned Kaspersky from government devices[16 17] or, in the case of Germany, issued a warning[18] in 2022 advising against its use in both public and private sectors. Despite the absence of an outright ban in Germany, the country experienced a 69% decline in Kaspersky usage during this period, surpassing the 58% decline observed in the US.

This raises questions about the effectiveness of different approaches: Is a ban inherently more impactful than a warning or recommendation? Perhaps previous warnings, which often targeted specific sectors like government and public administration, failed to capture the attention of other industries. Additionally, it invites reflection on the broader issue: under what circumstances can a technology deemed unsuitable for governmental or public administration use still be considered acceptable for critical infrastructure?

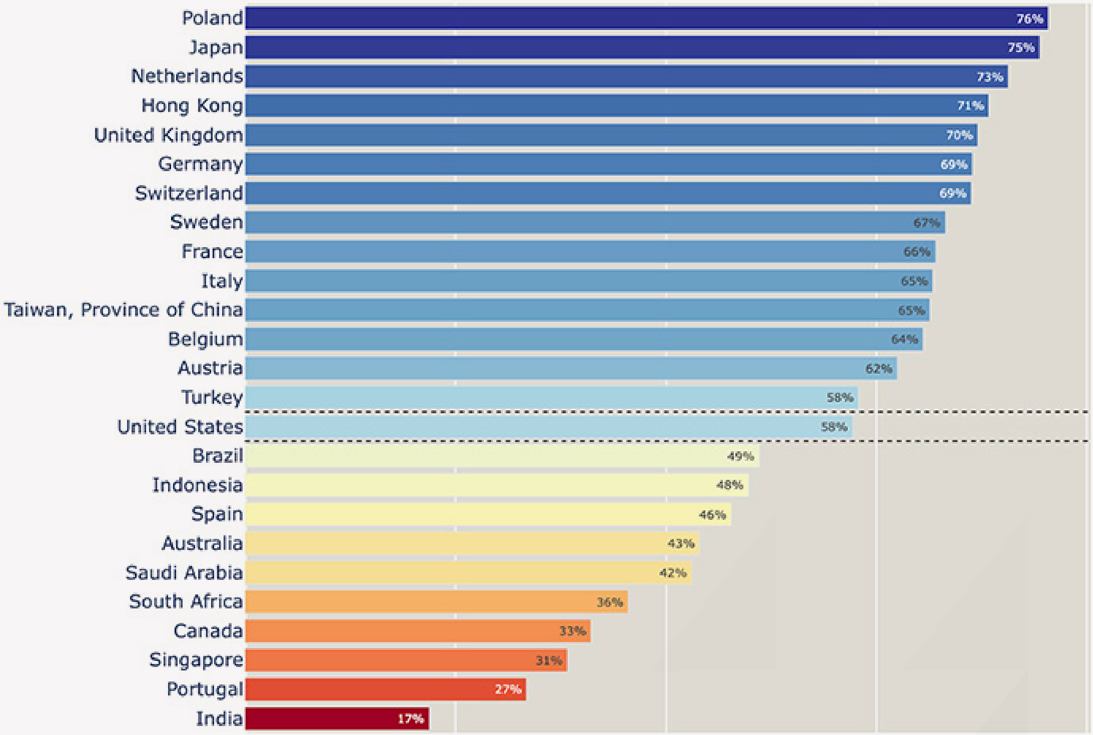

Figure 3 % Organizations drop per country

[15] The Aftermath of the Kaspersky Ban
[16] CIRCOLARE 21 aprile 2022, Agenzia per la Cybersicurezza Nazionale
[17] NCSC issues new warning on Russian software in UK tech supply chains
[18] Warning about Kaspersky virus protection software according to §7 BSIG

3. Supply Chain Attacks

A supply chain attack is a cyberattack targeting a business organization's supply chain to gain access to its systems or data. Instead of directly breaching the organization's defenses, attackers exploit vulnerabilities in third-party software or services connected to the company's network. These attacks can involve injecting malicious code, gaining unauthorized access, tampering with products, or stealing sensitive data. The impact often extends beyond the initial supplier, potentially compromising all businesses and stakeholders connected to the affected supply chain. ENISA's *Good Practices for Supply Chain Cybersecurity*[19] underscores the complexity and systemic risks posed by supply chain attacks, particularly those exploiting software dependencies and targeting identity providers or managed service providers. These attacks not only disrupt operations but also expose organizations to cascading vulnerabilities across sectors.

Below is an overview of some key sources that contribute to these vulnerabilities, each of which plays a crucial role in enabling the types of attacks detailed in this section:

Third-Party Software: the extensive use of third-party software, especially open-source components, creates opportunities for attackers to exploit vulnerable or outdated applications. These components often integrate deeply into organizational systems, and without rigorous auditing, they can act as unnoticed entry points for malicious actors.

Cloud Services: as organizations increasingly adopt cloud services for scalability and cost efficiency, these platforms become attractive targets for attackers. A compromise of cloud services can lead to unauthorized access to critical business data and disrupt essential operations.

Logistics and Hardware Suppliers: hardware and device suppliers are essential in modern supply chains. However, defective or intentionally compromised components can introduce risks such as embedded malware or hardware backdoors. These vulnerabilities are particularly concerning for critical sectors such as defense and infrastructure.

Consultants or Outsourced IT Teams: external service providers, including IT consultants, often have authorized access to sensitive systems. If compromised, these providers can become a vector for attackers to infiltrate their clients' networks, exposing sensitive data or enabling further exploitation.

From a national defense perspective, certain types of supply chain attacks are particularly critical because they directly impact a country's critical infrastructure, defense systems, and economic stability. National defense organizations are prime targets for nation-state actors aiming to exploit vulnerabilities in supply chains for espionage, sabotage, or large-scale disruption.

Supply chain attacks can take various forms, and their classification may differ depending on perspective or context. In this discussion, we will explore one way to categorize these attacks and provide examples of notable incidents for each group. Some of the most commonly recognized types include:

[19] Good Practices for Supply Chain Cybersecurity

3.1 Software Supply Chain Attacks

Software supply chain attacks represent one of the most strategic and insidious threats in cybersecurity today, posing serious risks to organizational resilience and national security. By exploiting trusted vendor relationships, attackers deliver malicious software, backdoors, or altered code through seemingly legitimate updates or packages, compromising systems critical to national defense, infrastructure, and economic stability.

The increasing reliance on open-source components and third-party software in application development has significantly expanded the attack surface, often outpacing risk mitigation efforts. As adversaries target these vulnerabilities, the cascading impact of such attacks extends beyond individual organizations, threatening entire sectors and undermining public safety, essential services, and defense operations.

A single breach can disrupt critical government functions, defense capabilities, and the broader economy. This underscores the need for a defense-oriented approach to cybersecurity, making supply chain security a cornerstone of national strategies to counter adversarial exploitation.

Supply chain attacks manifest in various forms, and their classification often depends on the context. This article will explore one framework for categorizing these attacks and provide examples of notable incidents for each category. Commonly recognized types include:

3.1.1 Zero-Day Vulnerabilities

Zero-day vulnerabilities are previously unknown security flaws in software or systems that adversaries exploit before developers can issue patches. These vulnerabilities are particularly dangerous in supply chains, as they can be weaponized to infiltrate trusted software, compromise critical infrastructure, or propagate malware through legitimate updates. Their versatility allows them to play a role in various types of supply chain attacks, from software compromises to targeting managed service providers. Two notable examples are Log4j and MOVEit.

The Log4Shell vulnerability, designated as CVE-2021-44228, is a stark example of the devastating potential of zero-day vulnerabilities. Discovered in December 2021, this flaw affected Log4j, a widely-used Java logging library embedded in countless enterprise and open-source software solutions. The vulnerability allowed attackers to achieve remote code execution (RCE) by simply crafting malicious log entries, turning this software library into a global cybersecurity emergency.

Due to Log4j's extensive adoption across industries - including the Defense sector, the scope of the attack was unprecedented, with systems ranging from critical infrastructure to cloud platforms left exposed. The simplicity of exploitation—a single malicious log message—intensified its impact, catching many organizations off guard. Attackers capitalized on the flaw to deploy ransomware, exfiltrate sensitive data, and disrupt services at scale.[20] [21]

Cybersecurity and Infrastructure Security Agency (CISA) Director Jen Easterly described it as the "most serious" vulnerability in her career. Despite rapid patching efforts, the deeply integrated nature of Log4j in supply chains made remediation challenging, leaving residual risks months after patches were released. [23] [24]

[20] Malicious Cyber Actors Continue to Exploit Log4Shell in VMware Horizon Systems
[21] Log4Shell Vulnerability in VMware Leads to Data Exfiltration and Ransomware
[22] CISA director says the LOG4J security flaw is the "most serious" she's seen in her career
[23] 30% of Log4j instances still remain vulnerable, with open source apps a major hurdle
[24] Log4j Vulnerability (Log4Shell): Ongoing Challenges in Remediation

This type of vulnerability was used by state-backed hackers[25] to create footholds in desirable networks for follow-on activity. According to VRT[26], some of the Belgium Ministry of Defense activities were paralyzed for several days as a consequence of this vulnerability. This is an example of how a zero-day can have an impact on National Security.

The Log4Shell incident underscores the criticality of proactive vulnerability management and threat intelligence. It demonstrated how vulnerabilities in seemingly innocuous components can have far-reaching impacts, emphasizing the importance of robust supply chain security measures and rapid response frameworks. For entities under the NIS2 directive, events like this one reinforces the need for continuous monitoring, coordinated risk assessments, and comprehensive third-party risk management.

The MOVEit Transfer vulnerability (CVE-2023-34362), identified in May 2023, exemplifies the devastating potential of zero-day exploits in trusted software. MOVEit, a widely-used Managed File Transfer (MFT) application, plays a critical role in secure data transmission for organizations worldwide. However, a SQL injection flaw in the application allowed threat actors to exploit the vulnerability and gain unauthorized access to databases, enabling the extraction of sensitive data.

This vulnerability's scope and impact were unprecedented, affecting nearly 2700[27] organizations across various sectors, including organizations related to the defense sector like the U.S. Department of Defense[28] (DoD) and Telos Corporation[29] (A defense contractor specializing in cybersecurity).The breach compromised the data of millions of individuals, illustrating the widespread ripple effects of such vulnerabilities in modern supply chains.

Attackers leveraged the flaw to execute arbitrary SQL commands, demonstrating the ease with which unsanitized inputs can be weaponized in web applications.

Despite rapid patching efforts[30], the pervasive integration of MOVEit in enterprise environments meant that residual vulnerabilities persisted long after initial remediation.

On December 2024 (when this article was written, around 38 aerospace/defense organizations were still vulnerable to MOVEit[31].

This incident serves as a crucial case study in zero-day vulnerability management, emphasizing the importance of continuous monitoring, threat intelligence sharing, and a robust incident response strategy.

[25] Log4j vulnerability now used by state-backed hackers, access brokers
[26] Defensie slachtoffer van zware cyberaanval, deel netwerk al dagen plat
[27] Unpacking the MOVEit Breach: Statistics and Analysis
[28] Hackers Accessed 632,000 Email Addresses at US Justice, Defense Departments
[29] Telos confirms data breach over MOVEit bug
[30] New research reveals rapid remediation of MOVEit Transfer vulnerabilities
[31] Progress Software Moveit Transfer Global Footprint

3.1.2 Compromised Open-Source Projects

Open-source projects can be susceptible to software supply chain attacks due to their collaborative and often decentralized nature. While open-source benefits from transparency and community scrutiny that helps identifying and fixing vulnerabilities, its widespread use and reliance on volunteer-driven maintenance can sometimes introduce risks. An attacker might gain control of a popular open-source project, either by purchasing or taking over its management. Once in control, they can exploit the trust of users by collecting sensitive data, embedding backdoors for future attacks, inserting malicious code, or weakening security features. The impact is magnified by the fact that many users fail to audit their dependencies regularly, leaving organizations reliant on open-source software exposed to significant risks.

Defense organizations and contractors often rely on open-source software for various systems and tools. Attackers compromising these projects can introduce vulnerabilities that infiltrate critical defense infrastructure.

In early February 2024, a significant supply chain attack unfolded after the company Funnull acquired the domain for the popular **Polyfill** CDN service (polyfill.io) and its associated GitHub account[32]. Polyfill, a widely-used JavaScript library, ensures compatibility of modern JavaScript features in older browsers, supporting functionality like screen resolution handling and media queries.

Shortly after the ownership transfer, the domain began distributing malicious JavaScript code, compromising over 110,000 websites. These websites, including phishing and malicious advertising platforms, redirected mobile users to various scam sites, leading to significant impacts on end-user security.

This vulnerability is considered highly critical due to its scope and method of exploitation. The malicious code injected into trusted websites redirects users to harmful sites or triggers downloads of malicious files. Such attacks can result in severe consequences, including data theft, malware distribution, and unauthorized access to sensitive information.

[32] Polyfill supply chain attack hits 100K+ sites and Polyfill Supply Chain Attack: Details and Fixes

3.1.3 Malicious Updates

Software used by organizations requires regular updates. If an update mechanism is compromised, malicious code can be distributed across secure networks.

Two of the most infamous malicious update cyberattacks highlight the devastating potential of compromised software update mechanisms. The **SolarWinds** Orion breach[33] in 2020 involved Russian state-sponsored actors, who infiltrated SolarWinds' build system and injected malware into legitimate updates of the Orion platform. These malicious updates were distributed to approximately 18,000 customers, including U.S. federal agencies, NATO, the U.K. government, and the European Parliament, enabling widespread espionage and unauthorized access to sensitive networks.

Similarly, the NotPetya attack in 2017 weaponized updates for MeDoc, a Ukrainian tax software widely used by businesses in the region. Attackers exploited the update mechanism to distribute malware disguised as legitimate updates. The malware, initially targeting Ukrainian entities, rapidly spread globally, disrupting critical systems and causing billions of dollars in damages. NotPetya encrypted systems and rendered them inoperable, underlining the global security implications of compromised update mechanisms. This incident demonstrated how cyberattacks could be weaponized as tools of geopolitical aggression. Unlike typical ransomware, which aims to extort money, NotPetya was designed to inflict widespread disruption and damage. Its origins linked to state-sponsored actors underline a broader strategy: using cyber tools to destabilize and harm national economies, critical infrastructure, and public trust. Such attacks bypass traditional military confrontation, allowing nations to execute covert, deniable operations with far-reaching consequences.

3.1.4 Embedded Backdoors

Embedded backdoors in software are among the most dangerous and enduring cybersecurity threats. These backdoors can be introduced at various stages, including during the software development process, after an initial attack (such as exploiting a vulnerability), or even via social engineering tactics targeting developers or contractors. Once embedded, these backdoors provide attackers with persistent access to systems, enabling further exploitation, espionage, or sabotage over time. Their impact is often magnified due to their transversal nature across supply chain types, where an initial compromise—such as a phishing attack or supply chain vulnerability—can lead to the insertion of a backdoor. This backdoor not only prolongs the damage but can also facilitate subsequent attacks, such as ransomware deployment, data exfiltration, or network disruption. A striking example of this was the SolarWinds Orion incident already mentioned in this document, where attackers used an embedded backdoor to infiltrate multiple organizations, allowing continued surveillance and exploitation long after the initial compromise. This highlights the necessity for comprehensive supply chain security measures, secure development practices, and continuous monitoring to mitigate the risks posed by embedded backdoors.

[33] 2020 United States federal government data breach

3.1.5 Build System Compromise (Attacks on the CI/CD)

CI/CD, which stands for Continuous Integration and Continuous Deployment, is a methodology used in software development to automate the building, testing, and delivery of applications. However, the CI/CD process can become a target for attackers. When malicious actors compromise the CI/CD pipeline by injecting malware into its environment—such as the operating system, build tools, or repositories—they can distribute tainted software updates to users. This type of attack exploits the trust placed in the CI/CD process, enabling widespread propagation of malicious code to downstream systems. They are challenging to detect because the malicious actions often mimic legitimate development processes, making it difficult to differentiate between normal operations and malicious activity.

A good example of an attack exploiting vulnerabilities in build systems is JetBrains TeamCity, which was targeted by North Korean and Russian[34] state-sponsored threat actors.

In October 2023, North Korean[35] nation-state actors Diamond Sleet (ZINC) and Onyx Sleet (PLUTONIUM) actively exploited a critical vulnerability (CVE-2023-42793) in JetBrains TeamCity, a widely-used CI/CD platform integral to software development and deployment. Known for their strategic focus on targeting defense sector organizations, these actors leveraged the vulnerability to achieve remote code execution, posing significant risks to organizations relying on TeamCity to manage their development pipelines. By infiltrating CI/CD environments, they were able to embed persistent malware, effectively bypassing traditional security measures. Microsoft's analysis revealed that these groups utilized advanced tools and techniques, enabling them to exploit vulnerabilities and maintain long-term, undetected access to compromised systems.

In September 2023, multiple national governmental agencies—including the U.S. Federal Bureau of Investigation (FBI), U.S. Cybersecurity & Infrastructure Security Agency (CISA), U.S. National Security Agency (NSA), Poland's Military Counterintelligence Service (SKW), CERT Polska (CERT.PL), and the UK's National Cyber Security Centre (NCSC)—issued a joint advisory. The advisory revealed that Russian Foreign Intelligence Service cyber actors had also exploited the critical JetBrains TeamCity vulnerability. These actors potentially gained access to source code, signing certificates, and the ability to compromise software compilation and deployment processes. Such access could enable them to facilitate supply chain operations, escalate privileges, move laterally within networks, deploy additional backdoors, and establish persistent, long-term access to compromised environments.

[34] Russian Foreign Intelligence Service (SVR) Exploiting JetBrains TeamCity CVE Globally
[35] Multiple North Korean Threat Actors Exploiting the TeamCity CVE-2023-42793 Vulnerability

3.2 Compromises through Social Engineering

According to the ENISA Threat Landscape 2024 report[36], supply chain compromises through social engineering is a key trend that is emerging. Here are some recent examples:

3.2.1 Maintainer Takeover

Maintainer takeover attacks are a sophisticated type of supply chain threat targeting open-source projects. These attacks exploit the decentralized and collaborative nature of open-source development by infiltrating a project's governance or maintainer team. Attackers often begin by gaining trust within the community, contributing legitimate code, engaging in discussions, or creating multiple personas to influence decision-making.

A good example of this type of attack is the **XZ Utils backdoor** incident, where a malicious actor gained maintainer status and introduced harmful code[37].In early 2024, a sophisticated supply chain attack targeted the XZ Utils project, a widely used data compression software integral to many Linux distributions. The attacker infiltrated the project over a three-year period, beginning in November 2021, by contributing seemingly benign code and engaging with the community to build trust.

Employing different tactics, the attacker applied pressure on the project's lead maintainer to delegate control. This persistent effort resulted in being granted co-maintainer status, providing the necessary access to embed a backdoor. This modification allowed unauthorized remote access to compromised systems. The backdoor was engineered to remain undetected, evading standard security measures. The backdoor had been incorporated into development versions of major Linux distributions.

This incident underscores the vulnerabilities inherent in open-source projects, particularly those maintained by small teams or individuals.

[36] ENISA THREAT LANDSCAPE 2024,' September 2024, pp.10

[37] The XZ-factor: social vulnerabilities in open source projects | By our experts | National Cyber Security Centre (ncsc.nl)

3.2.2 Phishing of Developers and Contractors

Phishing attacks targeting developers and contractors are another method for compromising supply chains. These attacks exploit human vulnerabilities by deceiving individuals into revealing credentials, granting unauthorized access, or downloading malicious software. Once an attacker gains access to developer accounts or contractor networks, they can manipulate source code, inject malicious updates, or poison software artifacts, creating a ripple effect across dependent organizations.

The two incidents below demonstrate how these attacks can introduce malware into widely used tools, ultimately threatening the integrity of critical systems.

GitHub repositories have been targeted using phishing campaigns that compromise developer credentials[38]. Attackers sent convincing emails with fake login links or GitHub notifications, tricking developers into entering credentials. That can lead to compromised repositories, malicious commits, and poisoned software artifacts in projects that rely on GitHub-hosted code.

Another example of targeting developers happened with the **North Korean Lazarus Group**. They target software developers by planting malicious packages in popular repositories like **PyPI** (Python Package Index) and npm[39]. They prepared the malware-containing malicious packages to target users' **typos** in installing Python packages, tricking developers into using or updating compromised packages. This gives attackers a way to propagate malware across dependent systems.

3.2.3 Vendor Impersonation

In this type of attack, adversaries impersonate legitimate suppliers or service providers to deceive defense organizations into granting access or information.

A notable example is described in an article from Palo Alto Networks, where threat actors associated with the Democratic People's Republic of Korea (DPRK), pose as recruiters to install malware on tech industry job seekers' devices[40]. This campaign may be financially motivated since the malware has the capability of stealing 13 different cryptocurrency wallets, but an important risk that this campaign poses is the potential infiltration of the companies that employ the targeted job seekers. A successful infection on a company-owned endpoint could result in the collection and exfiltration of sensitive information.

On another attack, the threat actors began by posing as fake IT workers to secure consistent income streams, but they then begun transitioning into more aggressive roles, including participating in insider threats and malware attacks[41].

"Operation North Star[42]" attacks used spear-phishing emails featuring legitimate job ads at defense contractors as a lure. According to McAff, the lures were job ads in engineering and project management positions across various US defense programs, including: F-22 fighter jets, Defense, Space and Security (DSS), photovoltaics for space solar cells and the Aeronautics Integrated Fighter Group. Later on other defense contractors based in other countries (Russia and India) were also identified as possible victims of these attacks[43].

[38] Security alert: new phishing campaign targets GitHub users
[39] New Malicious PyPI Packages used by Lazarus
[40] Contagious Interview: DPRK Threat Actors Lure Tech Industry Job Seekers to Install New Variants of BeaverTail and InvisibleFerret Malware
[41] Fake North Korean IT Worker Linked to BeaverTail Video Conference App Phishing Attack
[42] Operation North Star A Job Offer That's Too Good to be True?
[43] Operation North Star: Behind The Scenes

3.3 Suppliers with Access to Critical Data and Infrastructure

Suppliers and third-party vendors often have privileged access to defense-related systems, making them attractive targets. A notable example is the 2018 theft of classified information from the U.S. Navy[44]. In this case, a Chinese state-sponsored hacking group reportedly exploited vulnerabilities in the supply chain by targeting a subcontractor working on U.S. Navy projects. This breach compromised 614 gigabytes of data, including information about undersea warfare programs, plans for a supersonic anti-ship missile, and other classified details tied to national security. The incident exposed the vulnerabilities of relying on third-party contractors and demonstrated how insiders within the supply chain could unwittingly or maliciously aid adversaries in breaching critical defense infrastructure.

3.3.1 Compromised Managed Service Providers (MSPs)

Suppliers with privileged access to critical infrastructure are prime targets for zero-day exploits. For instance, vulnerabilities in VPN appliances or endpoint management tools used by Managed Service Providers (MSPs) can serve as entry points for adversaries to infiltrate sensitive networks undetected and gain access to their client's systems, including military contractors.

Operation Cloud Hopper[45], attributed to Chinese APT10, is a good example of compromising multiple MSPs.

3.3.2 Insider Threats

One notable example of an insider threat that affected national security in the defense sector is the Edward Snowden incident in 2013. Although not a traditional "supply chain" attack, Snowden, a former contractor for the National Security Agency (NSA), exploited his authorized access to sensitive systems to leak classified information about U.S. surveillance programs.

3.3.3 Hardware and Firmware Tampering

Hardware and firmware tampering has emerged as one of the most insidious and difficult-to-detect attack vectors. Unlike software-based exploits, which can often be patched or mitigated with updates, compromises at the hardware or firmware level pose long-term security risks, as they are deeply embedded within critical infrastructure. These attacks target the fundamental trust placed in the supply chain, allowing adversaries to implant backdoors, manipulate device behavior, or gain persistent access to sensitive systems.

As nations become increasingly reliant on globally interconnected supply chains for technology manufacturing, adversarial state actors and cybercriminal organizations have sought to exploit vulnerabilities at the production and distribution stages. From rogue microchips hidden in motherboards to firmware-level backdoors in telecommunications equipment, hardware and firmware tampering threatens not only corporate cybersecurity but also national defense operations. Two notable instances of hardware and firmware tampering, were the Stuxnet's firmware manipulation and the Supermicro spy chip controversy[46].

[44] China hacked a Navy contractor and secured a trove of highly sensitive data on submarine warfare
[45] Operation Cloud Hopper
[46] The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies

Stuxnet[47] is one of the most sophisticated and consequential cyberattacks in history, marking the first known instance of malware specifically designed to cause physical destruction through digital means. Discovered in 2010, Stuxnet was a highly complex worm believed to be developed jointly by the United States and Israel to sabotage Iran's nuclear program. The malware targeted Siemens programmable logic controllers (PLCs) used in uranium enrichment centrifuges at the Natanz facility. By exploiting multiple zero-day vulnerabilities, Stuxnet infiltrated industrial control systems, altering the operational speed of the centrifuges while displaying false readings to monitoring systems, thereby ensuring that the damage went undetected for an extended period. The attack reportedly led to the destruction of nearly 1,000 centrifuges, significantly delaying Iran's nuclear ambitions. Beyond its immediate impact, Stuxnet demonstrated the potential for cyber warfare to disrupt critical infrastructure, setting a precedent for future state-sponsored cyber operations and highlighting the vulnerabilities in industrial control systems worldwide.

In October 2018, Bloomberg Businessweek published an article[48] alleging that Chinese operatives had infiltrated the supply chain of Supermicro, a major hardware manufacturer, by implanting tiny microchips onto their server motherboards during production. These malicious chips were purportedly designed to create hardware backdoors, enabling unauthorized access to data on compromised servers. The report claimed that nearly 30 U.S. companies, including tech giants like Amazon and Apple, as well as various government agencies, were affected by this hardware tampering. However, the companies implicated, along with the U.S. Department of Homeland Security, strongly refuted these claims, asserting that there was no evidence to support the existence of such spy chips. Despite Bloomberg standing by its reporting and publishing a follow-up article in 2021[49] reiterating the allegations, no conclusive evidence has been publicly presented to substantiate the claims, leaving the controversy unresolved within the cybersecurity community but providing a good debate about the security of global supply chains and the challenges in detecting and preventing hardware-based cyber threats.

A more recent example is the BDBOX botnet[50]. It represents a cybersecurity threat, involving the distribution of off-brand Android devices—such as TV boxes, smartphones, and tablets—preloaded with malware. Upon activation, these compromised devices connect to command-and-control servers, allowing remote attackers to install malicious software, steal data, and conduct cybercriminal activities, including ad fraud and botnet-based attacks. With over 192,000 infected devices, including some from reputable brands like Yandex and Hisense, the sheer scale of this operation poses a risk to national cybersecurity. Malicious actors—potentially state-sponsored groups—could leverage this botnet for espionage, critical infrastructure disruption, or mass cyberattacks. If such devices are integrated into government agencies, defense networks, or essential services, they could serve as covert surveillance tools or attack vectors against national institutions. This case highlights the urgent need for supply chain security, stricter hardware vetting, and public awareness to prevent the infiltration of compromised consumer electronics into sensitive environments.

[47] An Unprecedented Look at Stuxnet, the World's First Digital Weapon
[48] The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies
[49] The Long Hack: How China Exploited a U.S. Tech Supplier
[50] BADBOX Botnet Is Back

4. The NIS2 directive

The NIS2 Directive[51] is a relevant initiative aimed at enhancing cybersecurity and resilience across the European Union. It is designed to ensure that the EU is well-equipped to handle cybersecurity threats and to establish a higher level of cybersecurity within organizations.

All EU member states were required to transpose NIS2 into their national legislation by October 17, 2024, meaning they must have integrated these regulations into their own legal systems. Countries are moving at different speeds. Four countries (Belgium, Croatia, Italy, and Lithuania) met the October 2024 deadline, while others are still in the early stages of the process.

It is estimated that this directive will directly impact approximately 160,000 organizations across the EU, highlighting the extensive reach and importance of these new regulations. This directive targets both organizations and member states.

Article 21 of the Directive outlines the ten measures that entities in scope must implement. They can be grouped into the following six key areas:

- Risk Assessment and management
- Data Integrity
- Incident Management and Reporting
- Business Continuity
- IT System Security
- Supply Chain Security

When analyzing these measures, organizations should perform a Risk assessment in order to identify potential risks, estimate their potential impact, and evaluate the likelihood of their occurrence.

According to the same article, the entities in scope must take appropriate and proportionate technical, operational, and organizational measures to manage the risks and, when doing that, entities should take into account the “state-of-the-art” and the cost of implementation of the measures, in order to ensure an appropriate level of security based on the risks posed.

A risk-based approach is suggested, but the directive is not highly prescriptive, which allows for different interpretations.

[51] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)

4.1. Supply Chain Security status in Europe

Supply chain cybersecurity is increasingly critical for European companies as reliance on third-party providers grows. The NIS Investments 2024 report[52], reveals that 65% of organizations reported increased investments in third-party risk management between 2021 and 2023, yet nearly 45% still experienced disruptions.

Despite this, significant gaps persist. ENISA surveys[53] show that while 86% of organizations have ICT/OT supply chain security policies, only 47% allocate budgets and 76% lack dedicated roles and responsibilities for supply chain risk. This challenge is particularly acute for SMEs, where supply chain risk management maturity remains lower compared to large enterprises[54]. SMEs often struggle with insufficient resources and expertise, making them more vulnerable to supply chain compromises.

To address these challenges, the NIS2 Directive introduces mandatory measures for supplier risk assessments, vulnerability handling, and secure development practices, driving improvements in supply chain resilience. However, the implementation remains complex, with 31% of organizations identifying supply chain risk management as one of the most difficult NIS2 requirements[55].

4.2. Supply Chain Security in NIS2

Interestingly, the supply chain was a key factor driving the update from the original NIS to NIS2. The European Parliament resolution[56] of 12 March 2019 on "security threats connected with the rising Chinese technological presence in the EU and possible action on the EU level to reduce them" urges the Commission to expand the scope of the original NIS Directive to include additional critical sectors and services not addressed by sector-specific legislation.

In June 2020, the Commission endorsed the Parliament's proposal, and by December 2020, it introduced a new proposal[57] for a strengthened legal framework to replace the original NIS Directive (2016/1148). This updated proposal for a revised Directive on Security of Network and Information Systems (NIS 2 Directive) explicitly emphasizes cybersecurity and the protection of supply chains for ICT services, systems, and products:

"Furthermore, the Commission proposes to address the security of supply chains and supplier relationships by requiring individual companies to address cybersecurity risks in supply chains and supplier relationships. At the European level, the proposal strengthens supply chain cybersecurity for key information and communication technologies. Member States in cooperation with the Commission and ENISA, will carry out coordinated risk assessments of critical supply chains, building on the successful approach taken in the context of the Commission Recommendation on Cybersecurity of 5G networks."

As we can see, the concerns covered in the section "2.1 The European Union Context" related to Chinese technology in the EU's 5G infrastructure were one of the main precursors of NIS2 and the inclusion of supply chain security in the new directive. The following sections will cover some details of that inclusion.

The concerns covered in section "2.1 The European Union Context," regarding the presence of Chinese technology in the EU's 5G infrastructure were key drivers behind the development of the NIS2 Directive and its focus on supply chain security.

European businesses must implement a robust, multi-faceted strategy for supply chain security, encompassing thorough third-party risk assessments, ongoing monitoring, and adherence to certification standards. Strengthening collaboration with suppliers, utilizing threat intelligence, and embedding resilience into procurement processes will be crucial to mitigating third-party risks and ensuring compliance with NIS2 regulations. Supply chain security must become a strategic priority to safeguard critical infrastructure and economic stability in the EU. The following sections will delve deeper into the specifics of how supply chain security has been incorporated into the new directive.

[52] NIS Investments 2024
[53] Good Practices for Supply Chain Cybersecurity
[54] NIS Investments 2024
[55] NIS Investments 2024
[56] European Parliament resolution of 12 March 2019 on security threats connected with the rising Chinese technological presence in the EU and possible action on the EU level to reduce them
[57] Proposal for directive on measures for high common level of cybersecurity across the Union

4.3. Supply Chain Security - articles 21(2)f and 21(3)

This article explicitly mentions that "*Supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers*," should be included in the Cybersecurity risk-management measures. The first part of the phrase clearly states supply chain security (which is detailed in other parts of the directive), and the second part is related to Implementing cyber risk measures into contractual obligations.

4.3.1 Implementing cyber risk measures into contractual obligations

Contracts are a line of defense. Well-drafted contracts can play a critical role in setting clear expectations, responsibilities, and security requirements for third-party vendors and suppliers. Consider including the following:

- **Defining cybersecurity requirements:** Stipulate the minimum cybersecurity requirements that vendors must meet. This can include adhering to standards or other relevant frameworks, technical controls, encryption standards, obligations to perform training and security certifications that vendors must maintain.
- **Incident response and reporting:** Contracts should require vendors to notify you of any cybersecurity incidents and vulnerabilities within a specified timeframe, along with their role in incident response. This ensures your organization is promptly informed of potential breaches or vulnerabilities within the supply chain and can take immediate action. Agree on how to manage an incident, periods and deadlines, form of notification, and get practical.
- **Perform regular risk assessments:** Right to audit your vendors' cybersecurity practices, including methods and time intervals, allowing you to verify that they are in compliance with the agreed-upon standards.
- **Supply chain risk management:** Contracts should require vendors to implement similar cybersecurity obligations with their own suppliers. This "cascading" effect helps protect the entire supply chain by ensuring that security is addressed at every level.
- **Consequences and termination clauses:** Contracts should include provisions on consequences in case of failure and allow you to terminate the agreement if a vendor fails to meet the required cybersecurity standards or has a significant security breach. This gives you the flexibility to move away from risky partners.

In the third paragraph of article 21 - article 21(3) - we can find additional context. When considering which measures should be adopted in the previous paragraph, organizations should take into account the following:

1. The vulnerabilities specific to each direct supplier
2. The overall quality of the products of their suppliers
3. The cybersecurity practices of their suppliers
4. The Secure development procedures of their suppliers.

Instead of adopting a one size fits all for all suppliers, depending on the impact each supplier can have on the organization, its services, its customers and the societal impact, different measures can be considered for those measures.

In the last part of article 21(3), it is mentioned that entities are required to take into account the results of the coordinated security risk assessments of critical supply chains when dealing with supply chain security, which is covered in the next section.

4.4. Coordinated security risk assessment and the Union/ National Security - article 22, recitals 90 and 91

A "coordinated security risk assessment" is a procedure initiated by the Cooperation Group (composed of representatives of Member States, the Commission, and ENISA) that is carried out at the EU level to assess and mitigate the level of risk of a specific supply chain. It is aimed at identifying, per sector, the critical ICT services, ICT systems, or ICT products, as well as their threats and vulnerabilities. It looks at measures, mitigation plans, and best practices to counter critical dependencies, potential single points of failure, threats, vulnerabilities and other risks associated with the supply chain.

In order to to complement the coordinated security risk assessments provided in Article 22(1), the European Council invited[58] the NIS Cooperation Group, in cooperation with the Commission and ENISA to develop a toolbox of measures for reducing critical ICT supply chain risks (**ICT Supply Chain Toolbox**). This new Toolbox is expected soon and will be built leveraging experiences from the 5G Toolbox and those gained at national level.

The "coordinated security risk assessment" in Article 22 of the NIS2 Directive is intricately connected to the national security and defense of EU Member States for several reasons, as it lays the groundwork for harmonized approaches to identifying and mitigating cybersecurity risks that transcend individual organizations or nations by:

1. Strengthening Critical Infrastructure Security -

- By focusing on critical ICT services, systems, and products (as emphasized in recital 90), it recognizes the interconnected nature of digital infrastructure across sectors like energy, healthcare, finance, and transportation, all of which are vital to national security. Any vulnerability in these sectors can lead to cascading effects that compromise a nation's stability.
- Recital 91 underscores the evaluation of emerging threats and dependencies on ICT supply chains, ensuring these assessments adapt to evolving technologies such as 5G, which are integral to both civilian and military operations.

2. Mitigating Geopolitical Risks

- The NIS2 Directive explicitly considers non-technical risk factors, such as the influence of third countries on ICT supply chains (Recital 90). This includes risks like concealed vulnerabilities, backdoors, and technological dependencies, which are often linked to geopolitical adversaries.
- This aligns with examples like the recent (June 2024) US prohibition of Kaspersky software, where a potential backdoor linked to a nation-state adversary was identified as a risk. Such actions demonstrate how supply chain security assessments extend to protecting against espionage, sabotage, and systemic disruptions that can impact national defense. The Bureau of Industry & Security (BIS) determined that a specific AV vendor poses an undue or unacceptable risk to national security for various reasons, including:
    - Jurisdiction, control, or direction of the Russian Government
    - Access to sensitive U.S. customer information through administrative privileges
    - Capability or opportunity to install malicious software and withhold critical updates
    - Third-party integration of products

[58] The Council of the European Union, 'Council Conclusions on ICT Supply Chain Security,' 17 October 2022, 13664/22

3. Unified Defense Against Cyber Threats

- A coordinated approach fosters cross-border collaboration and consistency in addressing risks. Multiple recitals and articles in the directive are related with the fact that risks identified in one Member State should be shared across the EU, promoting collective defense measures. This mirrors NATO's principle of shared security, where a cyberattack on one member affects the broader alliance.
- The involvement of entities like ENISA and the Cooperation Group ensures that the assessments are informed by expertise, shared intelligence, and best practices, strengthening national cybersecurity postures in a unified manner.

4. Countering Supply Chain Vulnerabilities

- Recital 90 highlights the goal of identifying single points of failure and critical dependencies in ICT supply chains. These vulnerabilities are often exploited in hybrid warfare strategies, where adversaries aim to destabilize a nation's economy or defense systems without direct confrontation.
- By addressing these risks, the NIS2 Directive ensures Member States are better equipped to prevent and mitigate disruptions that could weaken their resilience against both cyber and physical threats.

5. Encouraging Strategic Autonomy

- The focus on alternative ICT services, systems, and products (Recital 91) directly supports the EU's drive for technological sovereignty, by reducing reliance on external providers, particularly those from countries with different governance models or potentially adversarial intentions. This has clear implications for national defense, as it ensures critical technologies remain within secure and trustworthy ecosystems.

In conclusion, the "Union level coordinated security risk assessment" positions cybersecurity not only as a corporate or sectoral issue but as a fundamental element of national and supranational defense. By addressing both technical and geopolitical risks, the Directive empowers nations to protect their critical infrastructures, minimize dependencies on potentially compromised suppliers, and maintain a collective defense posture across the EU. This approach enhances resilience against threats, aligns with broader EU security objectives, and underscores the increasing convergence of cybersecurity with traditional concepts of national security and defense.

4.5. The Exponential Effect: NIS2's Supply Chain Requirements and Their Broad Scope

The NIS2 directive introduces transformative implications not only for organizations directly within its scope but also for countless others indirectly impacted by supply chain interdependencies. This cascading effect underscores how cybersecurity is no longer confined to an entity's internal operations but extends deeply into its relationships with suppliers, partners, and service providers, including those outside the EU.

This can happen if an organization delivers services or products to the EU in the NIS2-covered sectors, or if it has a presence in the EU, for example, a subsidiary.

It can also impact an organization, if it is a supplier of an in-scope entity. In that case, it may be indirectly impacted, for the following three reasons:

1. Imposed requirements (contracts)
2. Transfer of fines (contracts)
3. EU Coordinated Security Risk Assessment

The first scenario can happen when providing a service or product, to a company that is considered Essential or Important. As a supplier, a customer might contractually impose a minimal cybersecurity maturity, aligned with the NIS2 requirements. In this case, the organization will not be "supervised" by the national authorities, but it's your customer.

Another area we should be aware of, is related to the possibility of NIS2 fines being transferred to sub-service providers. A Sub-Service Provider is an entity to whom the Essential or Important entities intend to subcontract any part of the Services while remaining responsible to the Client, during the performance of the Contract. Fines under the directive, are imposed directly on companies falling within its scope. While there is generally no provision, for the direct transfer of fines to sub-service providers, Essential and Important Entities can incorporate specific clauses in contracts. These clauses may stipulate financial penalties for any breaches.

The last scenario, the Coordinated Security Risk Assessment has already been discussed in detail in the previous section. An entity covered by NIS2 may be considered non-compliant if there is an entity within its supply chain that is considered particularly risky under a coordinated risk assessment. As such, even if your company is not covered by the NIS2 directive, if it is part of the supply chain of a covered entity and uses one product or technology considered risky, it would be required by the customer to mitigate that risk.

In Summary, many organizations "not in scope" or "not from EU" will still be impacted by NIS2 through a customer/supplier relationship.

5. Conclusion

The NIS2 Directive represents a significant step towards improving supply chain cybersecurity, by creating awareness among EU member states and providing a structured legal framework to address cybersecurity risks at a European level.

From a national security perspective, one of its most valuable mechanisms is the Coordinated Security Risk Assessment, which establishes a legal basis for cross-border collaboration and ensuring that cybersecurity threats are jointly assessed and mitigated.

However, while NIS2 is a step in the right direction, implementation challenges do exist. The EU's previous attempt to use coordinated risk assessment mechanisms – through the EU 5G Toolbox – demonstrates the difficulty of translating policy into action. Despite the European Commission's strong recommendation that "Member States should achieve the implementation of the Toolbox without delay", by January 2025 (five years after its introduction) only 37% of EU members had implemented the recommendations. This slow reaction raises concerns about the EU's ability to implement its policies in this area effectively.

The 2024 ban on the use of Kaspersky solutions by the US government is another interesting example of the inconsistencies in how supply chain security risks are handled globally. Even though some EU member states have already issued national warnings about Kaspersky, many European organizations only reacted after the US government issued the formal ban. This raises some questions: Why did European organizations wait for a US decision instead of responding to their own national cybersecurity warnings? Under what circumstances can a technology considered unsuitable for use by public administration in some EU countries, be considered acceptable for use in the critical infrastructure of the same country? These inconsistencies suggest a different cybersecurity risk perspective by different EU members.

Whether it is the case of 5G security or the Kaspersky ban, the US has demonstrated a much lower risk tolerance compared to the EU. What the US finds unacceptable for its government agencies, businesses and citizens, the EU appears to accept, or at least tolerate, for a long time. However, when the US took decisive action, many European organizations followed, demonstrating a dependence on external leadership.

Ultimately, while the EU has created a solid regulatory foundation with NIS2, regulation alone is not enough. Political will and action are essential to ensure that cybersecurity is a true priority. The delay in the transposition of NIS2 by many Member States - at the beginning of 2025, only four of the 27 EU countries had completed the transposition of NIS2 - sends a mixed message about the EU's commitment to cybersecurity, raising concerns that national governments may not yet clearly recognize the strategic importance of this directive.

For NIS2 to reach its full potential, EU policymakers and national governments must demonstrate greater commitment, sense of urgency and better coordination. It is not enough to lay down regulations: Member States need to enforce them effectively and organizations must take decisive and timely action. Supply chain cybersecurity is not just a technical issue, it is also a matter of economic stability, national security and geopolitics. With NIS2, Member States appear to have the right tools, but now they need the determination to use them effectively.

Authors

Francisco Fonseca
SVP National Cybersecurity,
Bitsight

Paulo Moniz
Director, EuroDefense
Portugal

sales@bitsight.com

BOSTON (HQ)
RALEIGH
NEW YORK
LISBON
SINGAPORE

Bitsight is a cyber risk management leader transforming how companies manage exposure, performance, and risk for themselves and their third parties. Companies rely on Bitsight to prioritize their cybersecurity investments, build greater trust within their ecosystem, and reduce their chances of financial loss. Built on over a decade of technological innovation, its integrated solutions deliver value across enterprise security performance, digital supply chains, cyber insurance, and data analysis.