Journal of Integrative International Relations,
Volume 11, No. 2 (2026) 159-174
ISSN 2477-3557 (Print); 2797-0345 (Online)
DOI: 10.15642/jiir.2026.11.1.159-174

Cyber Threats to the United States (U.S.) Defense Supply Chain in the Era of Globalization 2020–2025

Mia April Liana
Airlangga University, Surabaya, Indonesia
E-mail: mia.april.liana-2025@fisip.unair.ac.id

Risman Febrian
Universitas Muhammadiyah Yogyakarta, Yogyakarta, Indonesia
E-mail: risman.febrian.psc25@mail.umy.ac.id

Abstract

The development of globalization and digital transformation has increased the defense sector's dependence on information technology systems, while giving rise to increasingly complex cyber threats to defense supply chains. The United States, as a country with advanced military and technological capabilities, faces vulnerabilities in the network of defense contractors, subcontractors, and vendors that are targeted by state and non-state actors to carry out espionage, data theft, and sabotage. This study aims to analyze the form of cyber threats to the United States defense supply chain in the 2020–2025 period, identify their impact on national security, and examine the efforts of President Joe Biden's administration to minimize these threats. The research uses a qualitative method with a descriptive-analytical approach through literature studies sourced from government documents, cybersecurity agency reports, scientific journals, and official publications. The results show that threats are dominated by state-backed espionage and infiltration activities, especially Russia, China, and North Korea, through *supply chain attack methods*, *phishing*, *malware*, *ransomware*, and intrusion through third-party vendors. These threats have an impact on strategic information leaks, disruptions of critical infrastructure, and a decline in national defense resilience. In response, the Biden administration strengthened cybersecurity regulations, increased international cooperation, implemented security standards for defense contractors, and adopted *a zero-trust* approach to improve the resilience of defense supply chains.

Abstrak

Perkembangan globalisasi dan transformasi digital telah meningkatkan ketergantungan sektor pertahanan pada sistem teknologi informasi, sekaligus memunculkan ancaman siber yang semakin kompleks terhadap rantai pasokan pertahanan. Amerika Serikat, sebagai negara dengan kemampuan militer dan teknologi yang maju, menghadapi

Article History: Received 06 July 2026, Revised 06 August 2026,
Accepted 01 October 2026, Available online 16 November 2026
Copyright: © 2026. The authors.
This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International

kerentanan dalam jaringan kontraktor, subkontraktor, dan vendor pertahanan yang menjadi sasaran aktor negara dan nonnegara untuk melakukan spionase, pencurian data, dan sabotase. Studi ini bertujuan untuk menganalisis bentuk ancaman siber terhadap rantai pasokan pertahanan Amerika Serikat pada periode 2020–2025, mengidentifikasi dampaknya terhadap keamanan nasional, dan meneliti upaya pemerintahan Presiden Joe Biden untuk meminimalkan ancaman tersebut. Penelitian ini menggunakan metode kualitatif dengan pendekatan deskriptif-analitis melalui studi literatur yang bersumber dari dokumen pemerintah, laporan lembaga keamanan siber, jurnal ilmiah, dan publikasi resmi. Hasil penelitian menunjukkan bahwa ancaman didominasi oleh aktivitas spionase dan infiltrasi yang didukung negara, terutama Rusia, Tiongkok, dan Korea Utara, melalui metode serangan rantai pasokan, phishing, malware, ransomware, dan intrusi melalui vendor pihak ketiga. Ancaman-ancaman ini berdampak pada kebocoran informasi strategis, gangguan infrastruktur penting, dan penurunan ketahanan pertahanan nasional. Sebagai tanggapan, pemerintahan Biden memperkuat regulasi keamanan siber, meningkatkan kerja sama internasional, menerapkan standar keamanan untuk kontraktor pertahanan, dan mengadopsi pendekatan zero-trust untuk meningkatkan ketahanan rantai pasokan pertahanan.

Keywords: United States; Globalization; Cybersecurity; Defense Supply Chain; Cyber War.

Introduction

In the era of increasingly advanced globalization, there are many impacts that further increase technological developments. Where this era of globalization has given rise to a form of interdependent and interconnected relationship between nation-states and international actors that are globally integrated. The rapid development of information and communication technology allows the exchange of data, goods, and services to take place very quickly and efficiently. However, it can also pose complex new challenges, especially in terms of security and protection against cyber threats. Where in the era of globalization, threats are not only in physical form such as territorial protection, military, strategic infrastructure, and also the economy but also include cyber or cybersecurity.[1]

Cyber threats are criminal activities that target networks, computer systems, and interconnected technology supply chains. Cybersecurity is very important because the digital system is now the backbone of various state activities, including the defense sector. These technological advances can result in new vulnerabilities that can be exploited by malicious actors such as competing countries, cybercriminal groups, and other non-state actors. Usually, these crimes or cyber threats are in the form of stealing confidential data, sabotage of systems, monitoring activities, and infiltration of malware that damages critical software and hardware. It can be seen that cyberattacks are one of the threats that threaten national security. Therefore, cybersecurity is an integral part of the national strategy to maintain the country's sovereignty and stability in the midst of changing global dynamics.[2]

The World Economic Forum's latest Global Cybersecurity Outlook 2025 report states that the world's cybersecurity landscape is becoming increasingly complex. Where this development has implications for the world of industry and government. New technological developments can cause geopolitical uncertainty, the evolution of cybercrime, regulatory challenges, vulnerabilities in supply chain dependence, and a widening cyber skills gap. The complexity of cybersecurity can also exacerbate cyber injustices where there is a deepening of the gap between developed and developing economies, widening sectoral gaps and also gaps between large and small organizations.[3]

Then, there is the latest threat intelligence data that actually shows a sharp escalation. Where the number of cyber incidents with supply chain implications monitored in the realm of hacker conversations has doubled from the long-term average. The information technology and IT service provision sectors are the most exploited targets due to their unreachable downstream reach to thousands of customers at once, including institutions related to the defense sector.[4] A survey of hundreds of global cybersecurity leaders also showed that more than 70 percent of organizations experienced at least one material third-party cyber incident in the past year. In addition, there are also approximately half of organizations that are able to monitor more than half of the total ecosystem of their suppliers.[5]

Globalization actually brings great benefits to defense production and innovation, but alongside it there is also an expansion of attacks on it. One of the countries that is being hotly discussed in cyber threats is the United States. There are several targets of cyber threats felt by the United States, including the health industry, financial services, government agencies, energy and utilities, the education sector, retail and e-commerce, and defense supplies. One of the biggest vulnerabilities in the defense supply chain in the United States is a cyber threat in the defense supply chain of United States contractors.[6]

Many countries have made the United States the main target in hacking cybersecurity. This is because the United States is a superpower country that is the center of the world's economic, military, and technological power, so it has become a strategic and symbolic target for many state and non-state actors. As a superpower, the United States has a dominant position in the international world marked by the many contributions of the United States to various world policies. This usually has various reasons ranging from gaining technological advantages, stealing the secrets of the opponent's defense, accelerating military development in one's own country, to weakening the strategic advantage of the opposing country.

Several previous studies have examined the issue of U.S. cybersecurity and cyber threats to national security in general. First, Triwahyuni & Wulandari[7] research entitled "United States Cyber Security Strategy" used a qualitative method and found that the United States has placed cybersecurity as a top priority in its foreign policy, as stated in various official documents and national

security strategies. The study emphasizes that the United States needs a comprehensive strategy to protect its national interests in an increasingly globally connected world, but the study is still general and has not touched on specific sectors such as defense supply chains.

Second, Vimy et al[8] research entitled "Cyber Attack Threat to Indonesia's National Security" explains that cyberattacks are one of the significant non-traditional threats to a country's national security, including potential disruptions to technological infrastructure and defense systems. This study shows that the dynamics of cyber threats are cross-border and are not only relevant for developing countries such as Indonesia, but also for developed countries as the main targets. However, the study focuses on the Indonesian national security context so it does not specifically explain how cyber threat patterns work in the defense supply chains of superpowers such as the United States or how policy responses are taken in a certain period of time.

Based on previous research studies, research gaps were found where studies on the United States' cybersecurity strategy tend to discuss policies in general without focusing on the defense supply chain sector, while studies on cyber threats to national security take more context from developing countries such as Indonesia[9] and have not specifically targeted superpowers in the contemporary period. In addition, these studies have generally not directly linked cyber threats to the complexity of defense supply chains involving contractors, subcontractors, and third-party technology vendors across countries. Therefore, the novelty of this study lies in the focus of a study that specifically maps the form of cyber threats to the United States defense supply chain in the 2020-2025 time frame, by linking actual cases such as SolarWinds, Colonial Pipeline, Salt Typhoon, and the infiltration of North Korean IT workers to the concrete policy response of President Joe Biden's administration, something that has not been widely discussed in an integrated international relations or previous cybersecurity studies[10]

This study aims to explain the forms and patterns of cyber threats targeting the United States defense supply chain in the 2020-2025 period, analyze the impact of these threats on the national, economic, and social security of the United States, and examine the policy steps taken by President Joe Biden's administration in minimizing cyber threats to the defense supply chain. Academically, this research contributes to enriching the literature on international relations regarding non-traditional security, especially in linking the concept of cyber warfare with the issue of defense supply chains which has not been studied in detail. Practically, this research is expected to be a consideration for stakeholders, both the government and the defense industry sector, in formulating cyber risk mitigation policies and strategies that are more adaptive to global geopolitical dynamics.

Theoretical Framework

Cyber threats in the era of globalization can be understood through non-traditional security theories in international relations. Where the concept of security is not only physical defense but also digital and informational forms. According to Verma & Shri,[11] cybersecurity is a real thing and comes as the global community becomes increasingly dependent on digital technology. Kaldor also said that cyber threats are included in the framework of a "new war" in which control over information and communication technology is an important element in contemporary conflicts that are on par with physical violence. The theory explains that cybersecurity is a global security architecture that requires policy, strategic, and broad cooperation adaptation. Therefore, in the midst of the progress of globalization and technological developments, cyber security is not only a national defense strategy but also an important pillar in maintaining the sovereignty, stability, and legitimacy of the country in the digital era.

In addition to non-traditional security frameworks, the study also uses a global supply chain socio-political perspective to explain why cyber vulnerabilities in the defense sector tend to persist. The modern defense supply chain is a multi-layered network involving hundreds of thousands of companies across levels and each additional layer creates new failure points that are difficult for key contractors to monitor.[12] Where the economic incentive structure in the supply chain tends to prioritize cost efficiency over security resilience, investment in supply chain risk management is often seen as an additional cost burden that reduces profit margins. rather than as a strategic whole. This view shows that cyber threats to defense supply chains are not only defensive technical problems but also structural problems rooted in market logic and the division of responsibilities between major contractors, subcontractors and regulators.

Research Methods

This study uses a qualitative research method with a descriptive-analytical approach. This approach was chosen to deeply understand the dynamics of cyber threats to the United States defense supply chain and analyze the policy responses implemented during the 2020–2025 period. The research was carried out through literature studies (*library research*) by utilizing various relevant secondary data sources. The research data was obtained from official documents of the United States government. In addition, the research also uses scientific journals, books, reports of international institutions, publications of cybersecurity companies, and scientific articles that discuss cybersecurity, defense supply chains, and national security policy of the United States.

Results and Discussion

Forms of Cyber Threats to the United States Defense Supply Chain

In this context, cyber threats cannot be separated from the dynamics of globalization that trigger an increasing power competition between countries in

the digital space. Many countries have competed to excel and expand their influence through information technology and digital infrastructure as part of their geopolitical strategy. Competition arises not only in the development of technology but also through cyberattacks to weaken or disrupt the stability of other countries without having to conduct open conflicts or military wars which are traditional conflicts. Therefore, cybersecurity is not just a technical issue but has turned into an arena for global power struggle that affects the political structure and resilience of a country in the era of globalization.

The United States is a superpower country that is the center of the world's economic, military, and technological power, so it has become a strategic and symbolic target for many state and non-state actors. In addition to the factors of the dominant position of the United States in the international world, there is also a geopolitical dimension that strengthens the reasons why this country is the main target of cyberattacks. The rivalry of great powers such as between the United States, China, and Russia is now taking place not only in the conventional economic and military spheres, but also in the digital space. Cyber warfare is a new form of global geopolitical competition in which the power of information and strategic data mastery are highly effective weapons. In this context, cyberattacks against the United States often have political motives to undermine legitimacy, create disinformation, and undermine public trust in the government. This phenomenon is in line with the concept of hybrid warfare, where modern conflict strategies combine conventional and non-conventional elements, including cyber, psychological, and economic operations to achieve national interests without having to engage in open war.

Globalization and the integration of technology in defense production have made the U.S. network of contractors not only produce physical parts such as aircraft components and combat vehicles but also rely on software, firmware, electronic design, and technology consulting services. The defense supply chain includes many fragments starting from designing, manufacturing microelectronic parts, device development, to logistics suppliers, so that there are many weak points that can be exploited by malicious parties. Hardware components could be compromised with malicious chips, while software could contain hidden loopholes that are not yet known. The perpetrators who carry out cyberattacks can be developed countries or strategic competitors with espionage or technological spying capabilities such as Russia, China, North Korea, Iran, cybercriminal groups, or non-state entities that rent *"hacker-for-hire" services.*[13]

In the case of the United States in 2020 to 2025, there are security reports from domestic and international cyber intelligence such as CISA *(Cybersecurity and Infrastructure Security Agency*), *FBI (the Federal Bureau of Investigation),* NSA *(National Security Agency)* as well as through military contract regulations that require security audits, incident reporting and vendor monitoring. Where they revealed that there were cyber infiltration attempts against the United

States defense sector from 2020 to 2025. China and Russia are countries that are often accused by the United States, that they often espionage and even *hack* information systems, both government infrastructure and private companies.[14]

The report revealed that from January 2020 to February 2022, Russian state-sponsored cyber actors actively targeted U.S. defense contractors who had obtained security clearances or *Cleared Defense Contractors* (CDCs).[15] The target of this activity is not only to large companies, but also to small subcontractors whose security systems are usually weaker. This action is carried out by *spear-phishing methods, brute force/password spraying, and exploitation of software* vulnerabilities that have not been updated. Once the perpetrators have successfully gained access to the network, they then collect credentials and access important technical data such as weapon specifications, military communication systems, aircraft designs, and technology development plans. From the theft of the data, it provides an advantage to the opposing country (Russia) because it can accelerate the development of their own military system and can even at the same time compensate for or exceed the defense capabilities of the United States.

In 2020, there was a SolarWinds attack targeting several government agencies and companies in the United States. The attack is believed to have been carried out by Russians who managed to infiltrate the systems of technology company SolarWinds that provides a network management software service called Orion. The hackers put malicious code into the Orion software update where every user makes an update and then unknowingly installs a backdoor into the hackers' system. As a result, many government organizations and private companies are vulnerable to the attack. The United States concluded that this attack was carried out by hackers supported by the Russian government, specifically APT29 which has ties to the Russian foreign intelligence service (SVR). The SolarWinds attack shows how fragile the global software supply chain is because by hacking into just one service provider, hackers can gain access to critical institutions in the United States.[16]

In the spring of 2021, hackers launched a ransomware attack on Colonial Pipeline, the largest refined oil products pipeline in the United States. This cyberattack caused a critical disruption of the United States' fuel supply that extended along the east coast and had a significant impact. This cyberattack was carried out by a group of people better known as *the Dark Side* who originated from Russia.[17] They managed to penetrate the internal networks of United States companies through VPN accounts without double authentication. The losses suffered from these attacks are quite a lot because they not only hack large operators but also target small business owners. It is mentioned that DarkSide stole about 100 Gibytes of data in two hours and also infected the company's network with this type of malicious software. In the end, *Colonial*

Pipeline shut down thousands of miles of its pipeline to stop the spread of ransomware and prevent hackers from doing more vulnerable things.

The report states that China is also one of the main actors in the cyber espionage campaign against the United States. On March 5, 2025, the United States Department of Justice reported that 12 Chinese nationals, including several law enforcement officials, were charged with conducting a global computer intrusion campaign. These attacks spread to a wide range of important institutions including defense companies, academic institutions, and United States government agencies. These perpetrators also carry out almost the same techniques as Russia, namely with phishing, malware, and infiltration techniques through third-party vendors. The perpetrators also use *hacker-for-hire networks* to carry out their actions with the main target of stealing trade secrets, strategic information and accessing sensitive technology-related data.[18]

In addition, in 2023-2024 there is information about hackers from the Chinese government who have broken into several US internet service providers in recent months to obtain sensitive information. This cyberattack was carried out by the Salt Typhoon group supported by the Chinese government by targeting telecommunications networks in the United States. These attacks aim to gather intelligence, monitor communications, and also embed long-term access to strategic systems. This threat is not only a technological threat but also a threat to national security. Fundamentally, the national security of the United States is now shifting from traditional military defense to digital and information defense that has become the mastery of geopolitical communication networks in the era of digital globalization.[19]

Then, there is a critical urgency of this issue is that the Salt Typhoon operation does not stop in 2024, but continues and even increases its depth until early 2026. On January 9, 2026, it was known that Salt Typhoon successfully targeted the emails of the staff of the United States House of Representatives Committee, especially personnel who handle national security issues related to foreign policy towards China.[20] The FBI leader even emphasized that the operation was still actively ongoing while a US senator revealed that two major telecommunications companies had withheld the publication of security assessment reports related to the Salt Typhoon. From this, it is questioned about the transparency and supervision of the telecommunications sector regulations. It is also evident from the combination of continued access to telecommunications infrastructure and direct penetration of congressional emails that Salt Typhoon may have gained visibility into U.S. policy deliberations toward China. This shows that there is a failure of counterintelligence. With implications that go far beyond the incident of technical data theft alone.

In another development, there is also North Korea that is recorded to take a more subtle but dangerous approach. In July 2024, it was stated that there was a North Korean cyber group that used infiltration techniques through fake IT workers applying for remote jobs at United States companies. The

perpetrators carried out a systematic global espionage campaign to support the regime's military and nuclear programs in Pyongyang. Their main targets are organizations in the defense, aerospace, nuclear, and engineering sectors. They do so with the aim of stealing sensitive or confidential technical and intellectual property information such as specifications of drones, missile systems, satellites, and radar surveillance technology. The perpetrators carried out various methods in doing so, such as exploiting vulnerabilities in web servers, deploying web shells, and using special tools and malware for remote access, lateral movement, and slow data extraction from within the company's network.[21]

United States Efforts to Reduce Cyber Threats

From some of these cases, the United States has suffered considerable losses ranging from theft of technical data, defense secrecy, weapon specifications, to the strategic advantage of the United States military. Another impact of these cyber threats is that competing countries are aware of the weaknesses and tactics designed by the United States. In addition, the impact of cyberattacks in the United States also endangers the country's national, social, geopolitical and economic security as well as other sectors Economically, in 2023 it is explained that there will be losses due to cybercrime which are estimated to exceed 8 trillion dollars. Cyberattacks also target large companies and small and medium businesses and even paralyze them, harming finances and reputations. In the social aspect, defense attacks can penetrate energy networks, military hospitals, and defense educational institutions, which can cause a national privacy security crisis.[22]

During Joe Biden's tenure as president of the United States from 2020 to January 2025, he took action to minimize existing cybersecurity threats. Where Biden focuses on defending digital infrastructure, securing critical services and capabilities in the digital realm, and building capacity to counter significant threats, including China This policy was taken by Biden with the goal of increasing the accountability of software and cloud service providers, strengthening federal communications security and identity management systems and encouraging the advancement and adoption of new technologies for cybersecurity across American departments Union. To improve the cybersecurity of the federal system, President Biden emphasized an executive order that requires the implementation of security practices that have been established by industry. In addition, President Biden is also prioritizing investments in innovative technology and identification processes in the future as well as phishing-resistant authentication options that will be used by FCEB institutions. The federal government must maintain the ability to quickly and effectively identify threats across federal enterprises.[23]

In 2022 in October, the United States Department of State advanced the National Cybersecurity (NCS) strategy. NCS is an effort to advance the United

States' vision of leadership in cyberspace, digital economy, and emerging digital technologies of a "free, open, secure, and prosperous world" NCS also aims to establish international partnerships to build a more open, resilient, and sustainable digital ecosystem while respecting human rights. This is done by rebalancing cyber defense responsibilities to governments and private sector organizations that are able and in the best position to mitigate risk, realign incentives to support long-term investments in cybersecurity through diplomacy, partnerships and information exchange. This strategy will be complemented by the United States Agency for International Development (USAID) Digital Policy.[24]

At the international level, the United States also encourages the formation of global norms and rules related to state behavior in cyberspace through forums such as *the United Nations Group of Governmental Experts* (UNGGE) and *the Open-Ended Working Group* (OEWG). The goal is to create international cyber governance that is transparent, accountable, and legally accountable. In addition, the United States also establishes bilateral cooperation with allies such as Japan, Australia, the United Kingdom, and Canada through the Five Eyes Alliance to strengthen cyber intelligence exchanges. This step is a form of collective cyber defense that reflects the awareness that cybersecurity is collective and cannot be achieved unilaterally. By expanding diplomatic cooperation and digital defense, the United States seeks to build a global cyber order that is stable, open, and free from the domination of authoritarian states.

To deal with increasingly complex cyber threats in defense supply chains, the United States also needs to strengthen cybersecurity regulations and policies, particularly regulating defense contractors and subcontractors. Improvement and implementation of a more stringent cybersecurity certification system for all defense partners, such as increasing standards in the Cybersecurity Maturity Model Certification (CMMC). Then, conducting routine audits of third-party vendors' information technology systems and strict monitoring of unnatural activities in the defense network so that they can minimize large cyber attacks. Furthermore, strengthening collaboration between the government, the private sector, and also international institutions. Strengthen and improve inter-agency coordination with technology and defense companies through real-time cyber intelligence coordination centers. The establishment of a special cyber task force tasked with monitoring and investigating potential cyber infiltration from competing countries so that it can be stronger in dealing with long-term espionage threats. No less important is the implementation of zero trust architecture, which is an application in cybersecurity that assumes that no user or device can be trusted just like that. Therefore, every user, device, and system must be constantly verified and monitored to prevent free movement and in the event of an intrusion, the damage does not spread widely because access is strictly restricted.[25]

The transition of power to President Donald Trump's administration in January 2025 does not necessarily stop this policy direction, despite a shift in emphasis. In March 2026, the Trump administration released a policy document titled President Trump's Cyber Strategy for America, accompanied by an executive order on countering cybercrime, fraud, and predatory schemes against U.S. citizens. This strategy gives greater leeway to private sector offensive cyber operations, encourages a more aggressive deterrence posture, explicitly placing ransomware groups, criminals allied with the state, and state actors as a primary concern, as well as promoting closer public-private coordination as a core defense pillar, by continuing the June 2025 executive order focused on the critical protection of nation-state cyber operations. This policy shift signals that the federal government recognizes the United States is in an era of active cyber conflict, not just an increased risk.[26]

Criticism of the United States' efforts to mitigate Cyber Threats

Cyber threats that occur often continue to recur even though regulations continue to be tightened, so that there is a tendency to see existing structural patterns. The defense industrial base of the United States is estimated to involve between one hundred thousand and three hundred thousand companies, and about ninety-two percent of these are small businesses. The majority of these companies struggle to meet even the most basic cybersecurity practices, such as email security and routine information technology hygiene, making phishing loopholes and missed software updates a favorite entry point for attackers.[27]

Independent survey data shows a striking gap between the perception of compliance and the reality of readiness. A study from Merrill Research found that only about four percent of defense contractors are actually ready to meet the Defense Department's minimum cybersecurity requirements set forth in the Cybersecurity Maturity Model Certification (CMMC), while three-quarters of contractors believe they are compliant. Only about twenty-one percent of contractors implement multi-factor authentication, a basic security control commonly used even for personal social media accounts, and only about fifteen percent implement software patch management adequately. This gap between belief and reality is at the heart of the problem: formal compliance with regulatory frameworks does not necessarily result in real operational resilience..[28]

A follow-up survey in 2026 of more than eight hundred and fifty federal contractors, subcontractors, assessors, and suppliers reinforces this picture. More than a quarter of defense organizations surveyed said they had experienced a software supply chain compromise in the past year, but only about thirteen percent routinely generated a Software Bill of Materials to identify exposures when new vulnerabilities emerge. Threat intelligence sharing is still uneven, with about sixty percent of respondents relying only on standard information feeds from the government, while only twenty-nine percent

participate in industry-specific threat sharing groups. Former senior U.S. cybersecurity official Rob Joyce asserted in the report that attackers are not concerned with the size of the organization, but rather about which path is easiest to sensitive information. And the line now often leads to small suppliers with part-time information technology support. This statement confirms that compliance certification should be understood as the minimum starting point, not the end goal of security risk management[29]

This problem is exacerbated by the disproportionate burden of compliance costs. The defense industry base is expected to spend about sixty-three billion US dollars over the next two decades to meet CMMC requirements, while these costs are often seen as a ceiling of achievement rather than a minimum floor towards truly effective defence. Most mid-level organizations estimated the cost of assessment preparation to be between fifty thousand and one hundred and fifty thousand United States dollars, and more than half of the participants stated assessors often interpreted the requirements inconsistently, adding to the uncertainty of the process. Ironically, on the other side of the attack ecosystem, the cost for an attacker to compromise a defense contractor's device that has reached a certain level of maturity through credential-stealing malware is estimated to be only around ten US dollars.[30]

The institutional capacity to verify compliance is also limited. Until early 2026, the CMMC certification body ecosystem has fewer than one hundred certified third-party appraisal organizations and fewer than eight hundred certified assessors to serve tens of thousands of companies that are required to meet various levels of certification. These capacity gaps create long queues and time pressures that in turn encourage a number of contractors to meet requirements documentably without completely changing their cybersecurity operational practices. This phenomenon is in line with the findings that the main cause of defense supply chain vulnerabilities is not a mere lack of regulation, but rather an economic incentive structure that prioritizes costs over security, over-reliance on overseas suppliers, and planning that is still peacetime-oriented rather than anticipating sustained conflict. These three causal factors explain why supply chain risk management investments are often viewed as a cost accounting burden with no clear return on investment, so contractors tend to delay allocating resources for safety until an incident actually occurs.[31]

Concluding Remarks

It can be concluded that cyber threats to the defense supply chain of the United States show that the global security dimension has fundamentally evolved in the era of digital globalization, especially in 2020-2025 during the presidency of Joe Biden. Security is no longer a military monopoly, but a complex ecosystem involving technology, diplomacy, law, and economics. Cases of infiltration by Russia, China, and North Korea confirm that digital supremacy is becoming a new arena for global power struggles. Therefore, cybersecurity

should be viewed as a strategic instrument of equal importance to conventional military power. The United States, as a global leader, faces the challenge of maintaining its technological superiority while building a collaborative, ethical, and equitable cyber defense system in an increasingly connected international order.

The cases that occurred in the United States also prove that globalization and technological advances can also pose a threat. Cyber threats to the security of defense supply chains are a critical point in modern national security strategies. In the current era of globalization, the supply chain is no longer just a logistical affair but has become the main target in global cyber warfare, so defending cyber threats requires a cross-sectoral, cross-country and cross-technology strategy. Therefore, to deal with this, a strategy is needed that includes strict regulations, international cooperation, improving security standards, and the application of technology such as zero trust to build an adaptive, collaborative cyber defense system and minimize evolving attacks.

References

Anderson, L. (2026). *Gaining the Cyber Supply Chain Advantage | RealClearDefense*. https://www.realcleardefense.com/articles/2026/06/03/gaining_the_cyber_supply_chain_advantage_1186476.html

Aqua. (2023). SolarWinds Attack: Play by Play and Lessons Learned. *AquaSecuritySoftware*.

Blinken, A. J. (2025). United States International Cyberspace & Digital Policy Strategy. *Statego*.

CISA. (2022). *Russian State-Sponsored Cyber Actors Target Cleared Defense Contractor Networks to Obtain Sensitive U.S. Defense Information and Technology | CISA*. Russian State-Sponsored Cyber Actors Target Cleared Defense Contractor Networks to Obtain Sensitive U.S. Defense Information and Technology | CISA. (n.d.). Retrieved September 22, 2025, from https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-047a

CISA. (2024). *North Korea Cyber Group Conducts Global Espionage Campaign to Advance Regime's Military and Nuclear Programs | CISA*. https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-207a

Clay, J. (2026). *U.S. Public Sector Under Siege: Threat Intelligence for Q1 2026*. Trendmicro.

Cyble. (2025). *Supply Chain Attacks Surge In 2025: Double The Usual Rate*. https://cyble.com/blog/supply-chain-attacks-double-in-2025/

Insurica. (2024). Cyber Case Study: Colonial Pipeline Ransomware Attack. *INSURICA*.

Kaldor, M. (2021). War and Transition. *Research Policy*, *50*(10). https://doi.org/10.1016/j.respol.2021.104344

Levene, Col. D. (2025). Causes of Vulnerabilities and Key Threats to Defense Supply Chains. *Airuniversity.Af.Edu*.

Mediana, C. (2025). Tantangan Keamanan Siber Global Tahun 2025 Makin Kompleks. *Kompas.Id*.

nextgov/FCW. (2024). *America's defense contractors are failing basic cybersecurity and China is exploiting it - Nextgov/FCW*. https://www.nextgov.com/ideas/2024/10/americas-defense-contractors-are-failing-basic-cybersecurity-and-china-exploiting-it/400596/

Office of Public Affairs. (2025). *Justice Department Charges 12 Chinese Contract Hackers and Law Enforcement Officers in Global Computer Intrusion Campaigns | United States Department of Justice*. Office of Public Affairs | Justice Department Charges 12 Chinese Contract Hackers and Law Enforcement Officers in Global Computer Intrusion Campaigns | United States Department of Justice. (n.d.). Retrieved September 22, 2025, from https://www.justice.gov/opa/pr/justice-department-charges-12-chinese-contract-hackers-and-law-enforcement-officers-global?

One, S. (2025). Top 7 Cyber Attacks in the United States. *SentinelOne*.

Ribeiro, A. (2025). Biden issues executive order to further strengthen national cybersecurity, targets digital defense and accountability. *IndustialCyber*.

SecurityBrief. (2026a). *Federal cybersecurity report flags supply chain gaps*. https://securitybrief.news/story/federal-cybersecurity-report-flags-supply-chain-gaps

SecurityBrief. (2026b). *US defence suppliers lag on cybersecurity readiness*. https://securitybrief.news/story/us-defence-suppliers-lag-on-cybersecurity-readiness

SecurityScorecard. (2025). *2025 Supply Chain Cybersecurity Trends*. SecurityScorecard.

Thornebrooke, A. (2024). China-Backed Salt Typhoon Hacking Group Remains Embedded in US Telecommunications. *Theepochtimes*.

Triwahyuni, D., & Wulandari, T. A. (2016). STRATEGI KEAMANAN CYBER AMERIKA SERIKAT. In *Jurnal Ilmu Politik dan Komunikasi: VI* (Number 1). http://www.census.gov/population/www/popc

Verma, A., & Shri, C. (2025). Cyber Security: A Review of Cyber Crimes, Security Challenges and Measures to Control. *Vision*, *29*(4), 478–492. https://doi.org/10.1177/09722629221074760

Villasenor, J. (2013). *Compromised By Design? Securing the Defense Electronics Supply Chain Executive Summary*.

Vimy, T., Wiranto, S., Widodo, P., Suwarno, P., Studi Keamanan Maritim, P., Keamanan Nasional, F., & Pertahanan Republik Indonesia, U. (2022). ANCAMAN SERANGAN SIBER PADA KEAMANAN NASIONAL INDONESIA. *Jurnal Kewarganegaraan*, *6*(1).

Yanuar, A. P. (2021). Cyber War : Ancaman Baru Keamanan Nasional dan Internasional (Cyber War: New National and International Security Threat). In *Jurnal Keamanan Nasional: VII* (Number 1). https://www.kompasiana.com/deky91/5528eab76ea8346b-

Endnotes

[1] Yanuar, A. P. (2021). Cyber War : Ancaman Baru Keamanan Nasional dan Internasional (Cyber War: New National and International Security Threat). In *Jurnal Keamanan Nasional: VII* (Number 1). https://www.kompasiana.com/deky91/5528eab76ea8346b-

[2] Vimy, T., Wiranto, S., Widodo, P., Suwarno, P., Studi Keamanan Maritim, P., Keamanan Nasional, F., & Pertahanan Republik Indonesia, U. (2022). ANCAMAN SERANGAN SIBER PADA KEAMANAN NASIONAL INDONESIA. *Jurnal Kewarganegaraan*, *6*(1).

[3] Mediana, C. (2025). Tantangan Keamanan Siber Global Tahun 2025 Makin Kompleks. *Kompas.Id*.

[4] Cyble. (2025). *Supply Chain Attacks Surge In 2025: Double The Usual Rate*. https://cyble.com/blog/supply-chain-attacks-double-in-2025/

[5] SecurityScorecard. (2025). *2025 Supply Chain Cybersecurity Trends*. SecurityScorecard.

[6] One, S. (2025). Top 7 Cyber Attacks in the United States. *SentinelOne*.

[7] Triwahyuni, D., & Wulandari, T. A. (2016). STRATEGI KEAMANAN CYBER AMERIKA SERIKAT. In *Jurnal Ilmu Politik dan Komunikasi: VI* (Number 1). http://www.census.gov/population/www/popc

[8] Vimy et al., 2022.

[9] Vimy et al., 2022.

[10] Triwahyuni & Wulandari, 2016.

[11] Verma, A., & Shri, C. (2025). Cyber Security: A Review of Cyber Crimes, Security Challenges and Measures to Control. *Vision*, *29*(4), 478–492. https://doi.org/10.1177/09722629221074760

[12] Levene, Col. D. (2025). Causes of Vulnerabilities and Key Threats to Defense Supply Chains. *Airuniversity.Af.Edu*.

[13] Villasenor, J. (2013). *Compromised By Design? Securing the Defense Electronics Supply Chain Executive Summary*.

[14] Triwahyuni & Wulandari, 2016.

[15] CISA. (2022). *Russian State-Sponsored Cyber Actors Target Cleared Defense Contractor Networks to Obtain Sensitive U.S. Defense Information and Technology | CISA*. Russian State-Sponsored Cyber Actors Target Cleared Defense Contractor Networks to Obtain Sensitive U.S. Defense Information and Technology | CISA. (n.d.). Retrieved September 22, 2025, from https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-047a

[16] Aqua. (2023). SolarWinds Attack: Play by Play and Lessons Learned. *AquaSecuritySoftware*.

[17] Insurica. (2024). Cyber Case Study: Colonial Pipeline Ransomware Attack. *INSURICA*.

[18] Office of Public Affairs. (2025). *Justice Department Charges 12 Chinese Contract Hackers and Law Enforcement Officers in Global Computer Intrusion Campaigns | United States Department of Justice*. Office of Public Affairs | Justice Department Charges 12 Chinese Contract Hackers and Law Enforcement Officers in Global Computer Intrusion Campaigns | United States Department of Justice. (n.d.). Retrieved September 22, 2025, from https://www.justice.gov/opa/pr/justice-department-charges-12-chinese-contract-hackers-and-law-enforcement-officers-global?

[19] Thornebrooke, A. (2024). China-Backed Salt Typhoon Hacking Group Remains Embedded in US Telecommunications. *Theepochtimes*.

[20] Clay, J. (2026). *U.S. Public Sector Under Siege: Threat Intelligence for Q1 2026*. Trendmicro.

[21] CISA. (2024). *North Korea Cyber Group Conducts Global Espionage Campaign to Advance Regime's Military and Nuclear Programs | CISA*. https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-207a

[22] One, 2025.

[23] Ribeiro, A. (2025). Biden issues executive order to further strengthen national cybersecurity, targets digital defense and accountability. *IndustialCyber*.

[24] Blinken, A. J. (2025). United States International Cyberspace & Digital Policy Strategy. *Statego*.

[25] One, 2025.

[26] Clay, 2026.

[27] Anderson, L. (2026). *Gaining the Cyber Supply Chain Advantage | RealClearDefense*. https://www.realcleardefense.com/articles/2026/06/03/gaining_the_cyber_supply_chain_advantage_1186476.html

[28] nextgov/FCW. (2024). *America's defense contractors are failing basic cybersecurity and China is exploiting it - Nextgov/FCW*. https://www.nextgov.com/ideas/2024/10/americas-defense-contractors-are-failing-basic-cybersecurity-and-china-exploiting-it/400596/

[29] SecurityBrief. (2026a). *Federal cybersecurity report flags supply chain gaps*. https://securitybrief.news/story/federal-cybersecurity-report-flags-supply-chain-gaps

[30] Anderson, 2026.

[31] Levene, 2025.