ISSN 2957-2169

DOI: https://doi.org/10.5281/zenodo.13626432

مجله مطالعات حقوق بین الملل ایران

Security Concerns of Microprocessors and the Sovereignty of Human Rights: A Critical Review of Privacy Issues

Amirali R. Davoudpour

Iranian Canon of Medicine and Law, Administrative Wing of Law and Healing Association, Iranian Watchdog of Medicine and Law, Tehran-Iran

Email of the corresponding author: davoudpour@canmedlaw.org

Accepted and published September, 2024

Abstract

The ubiquitous presence of smartphones and smart devices in modern life raises significant security concerns, particularly regarding privacy and civil rights. Recent incidents, such as the alleged use of intelligent techniques for terrorism in Tehran, have highlighted the risks associated with microprocessors, the core components in these devices. This article examines the security vulnerabilities inherent in microprocessors, focusing on the potential for privacy infringements and the impact of international regulations. It explores how hardware vulnerabilities, such as backdoors and hardware Trojans, pose serious threats to both individual privacy and global security. The discussion includes the geopolitical implications of microprocessor production, particularly the concentration of manufacturing in a few key regions, and the strategic importance of regulatory measures. Through a comprehensive analysis of design-level security, supply chain integrity, and policy frameworks, the article underscores the need for advanced detection methods and international collaboration to address these evolving threats.

Keywords: Microprocessors, Security Vulnerabilities, Privacy Infringements, Hardware Trojans, Espionage, International Regulations, Geopolitics, Supply Chain Security

Introduction

In the 21st century, smartphones and other smart devices have become integral to daily life. However, the widespread use of these devices has brought about significant security concerns, particularly regarding the protection of civil and human rights and raising privacy concern. Recent violence in the Middle East and the wide spread use of intelligent techniques to conduct terrors i.e. in case of Ismail Haniyeh[1] in Tehran-Iran has raised concerns about the intelligence means to promote violence in neutral and civil areas including the Iranian capital in Tehran. Such concerns have forced the Hezbollah Leader Sayyid Hasan Nasrallah to regard cell phones as “lethal spies”[2] the This article aims to explore the security vulnerabilities associated with the hardware especially microprocessors which is widely used to make cell phones, focusing on their potential for infringements of privacy rights, the impact of international regulations on microprocessor technology, and the broader implications for global security. We previously addressed that the psychological and intelligence conflicts has made serious damages to the Psycho-Social integrity of the Middle-Eastern countries including Iran (Davoudpour, A.R., 2024). Such physical threats left traces on the civil dignity, and social integrity as well as the sense of insecurity in the social affairs. Such a new front, including technological warfare is a matter of great concern both at political level and governance and in the realm of academia.

Microprocessors and Security Vulnerabilities

Microprocessors, often referred to as the "brains" of electronic devices, are crucial for the functioning of everything from smartphones to military equipment. The complexity of these

[1] World reacts to killing of Hamas political chief Ismail Haniyeh in Iran, Al-Jazeera news agency, August 1, 2024, https://www.aljazeera.com/news/2024/7/31/reactions-to-the-killing-of-hamass-ismail-haniyeh

[2] Why Nasrallah regards to cell phones as ‘lethal spies’, IRNA news agency, September 1, 2024, 8:31 AM. https://www.irna.ir/news/85584544/%D8%B4%DA%AF%D8%B1%D8%AF%D9%87%D8%A7%DB%8C-%D8%AC%D8%A7%D8%B3%D9%88%D8%B3%DB%8C-%D9%85%D9%88%D8%B3%D8%A7%D8%AF-%D8%AF%D8%B1-%D9%84%D8%A8%D9%86%D8%A7%D9%86-%DA%86%D8%B1%D8%A7-%D8%B3%DB%8C%D8%AF-%D8%AD%D8%B3%D9%86-%D9%86%D8%B5%D8%B1%D8%A7%D9%84%D9%84%D9%87-%D8%AA%D9%84%D9%81%D9%86-%D9%87%D9%85%D8%B1%D8%A7%D9%87 [In Persian]

microprocessors, especially in advanced smartphones, computers, and similar devices, opens the door for hidden layers of information that could be exploited for espionage. The ability to embed secretive functionalities within these chips poses a significant threat to both individual privacy and national security.

The structure of microprocessors allows for the possibility of incorporating hidden information layers, which can be used for unauthorized surveillance. This concern is exacerbated by the fact that most of the world's microprocessor manufacturing and design is concentrated in a few countries, making it difficult for others to have full transparency and control over these critical components. The lack of advanced reverse-engineering technologies to deconstruct and fully understand these chips further complicates the issue, leaving room for potential security breaches that may go undetected for years.

- **Backdoors in Microprocessor Design**

Backdoors in microprocessor design represent a significant security concern, particularly in the context of national security and critical infrastructure. A backdoor is an intentionally created vulnerability within a microprocessor that allows unauthorized access to the device, often bypassing standard authentication or security measures. These backdoors can be embedded during the design or manufacturing process and may be extremely difficult to detect, even with advanced reverse-engineering techniques.

The presence of backdoors in microprocessors can have catastrophic consequences. For example, they can be exploited by malicious actors to gain control over devices, steal sensitive information, or disrupt critical systems. In some cases, these vulnerabilities might be installed by state actors aiming to conduct espionage or sabotage. The Stuxnet worm, which targeted Iran's nuclear facilities, is one example where a sophisticated cyber weapon exploited vulnerabilities in industrial control systems (ICS), although it did not specifically target microprocessor backdoors (Langner, 2011). However, it underscores the potential impact that hardware-based vulnerabilities could have if similarly exploited.

The risk is further compounded by the globalization of the semiconductor supply chain. With much of the design and manufacturing concentrated in a few countries, including Taiwan and China, concerns have been raised about the potential for foreign governments to pressure or infiltrate companies to insert backdoors into microprocessors intended for global distribution (Clarke & Knake, 2010). This possibility has led to increased scrutiny and calls for more rigorous testing and verification of microprocessor integrity, particularly for devices used in sensitive areas such as military systems, government communications, and financial networks (Geer, 2014).

Given the difficulty of detecting backdoors, some experts have advocated for the development of new security frameworks and verification tools that can more effectively identify and neutralize these threats (Karri et al., 2010). Efforts are also underway to improve supply chain security, including initiatives to diversify semiconductor manufacturing and enhance cooperation between allied nations to reduce reliance on potentially compromised foreign suppliers.

In summary, backdoors in microprocessor design pose a serious and growing threat to global cybersecurity. As microprocessors continue to form the backbone of modern technology, ensuring their integrity is paramount to protecting national security, economic stability, and public safety.

- **Hardware Trojans**

Hardware Trojans are malicious modifications to integrated circuits (ICs) that are intentionally inserted during the design or manufacturing process to compromise the security, functionality, or performance of the affected device. Unlike software-based threats, hardware Trojans are embedded within the physical components of a device, making them particularly difficult to detect and mitigate. These malicious alterations can take various forms, from adding extra logic gates to modifying existing circuitry, and they can be activated under specific conditions or remain dormant until triggered by an external event.

The threat posed by hardware Trojans is significant, especially in critical systems where the integrity of hardware is paramount. For instance, in military applications, a hardware Trojan could be used to disable weapons systems, corrupt communication networks, or leak sensitive information to adversaries. The U.S. Department of Defense has recognized the potential dangers of hardware Trojans, leading to the establishment of stringent guidelines for the procurement and testing of ICs used in defense systems (Tehranipoor & Wang, 2011).

Detection of hardware Trojans presents a considerable challenge. Traditional testing and verification methods are often insufficient because hardware Trojans are designed to evade detection by consuming minimal power, occupying minimal space, or mimicking legitimate circuitry (Zhang, Tehranipoor, & Plusquellic, 2013). Advanced techniques such as side-channel analysis, which examines the power consumption, electromagnetic emissions, or timing behavior of ICs, have been developed to detect anomalies indicative of hardware Trojans (Agrawal et al., 2007). However, these methods require highly specialized equipment and expertise, making widespread implementation difficult.

The globalization of the semiconductor industry exacerbates the hardware Trojan threat. With various stages of chip design, fabrication, and assembly often distributed across multiple countries, the potential for malicious actors to introduce Trojans at some point in the supply chain increases. This risk has led to growing concerns about supply chain security and has spurred research into developing more secure and trustworthy hardware manufacturing processes (Tehranipoor et al., 2011).

In summary, hardware Trojans represent a critical and evolving threat to the security of integrated circuits, particularly in high-stakes environments such as defense, finance, and critical infrastructure. The development of more effective detection methods and secure manufacturing processes is essential to mitigating the risks associated with these insidious hardware-based attacks.

- **Malicious Code**

Malicious code refers to software or scripts that are intentionally designed to cause harm, disrupt operations, or gain unauthorized access to systems and data. Unlike benign software, malicious code operates with the intent to exploit vulnerabilities in systems, networks, or applications. This category includes a wide range of threats, such as viruses, worms, trojans, ransomware, spyware, and more. Malicious code can be introduced into a system through various means, including phishing emails, infected software downloads, or compromised websites.

Once executed, malicious code can perform a variety of harmful actions, such as stealing sensitive information, corrupting data, disrupting operations, or granting unauthorized access to attackers. For instance, ransomware encrypts the victim’s files and demands payment for the decryption key, effectively holding the data hostage (Richardson & North, 2017). Another common form of malicious code is the trojan horse, which disguises itself as legitimate software but executes harmful activities once installed, such as creating backdoors into the system (Choo, 2011).

Malicious Code in GUI Design

Malicious code can also be embedded within Graphical User Interface (GUI) design, presenting a unique and often overlooked threat. In this context, attackers exploit the visual elements of an interface to deceive users or compromise the underlying system. For example, a technique known as "clickjacking" involves layering a transparent or hidden malicious link over a legitimate GUI element. When the user interacts with the GUI, they inadvertently trigger the hidden action, such as downloading malware or granting administrative permissions to an attacker (Huang et al., 2012).

Another example is the use of deceptive GUI elements, such as fake login screens or dialogue boxes, designed to steal user credentials. These elements are crafted to mimic the appearance of legitimate applications or operating system prompts, tricking users into entering sensitive information. Once the information is entered, it is captured by the malicious code and transmitted to the attacker (Maurer, 2017).

Malicious code in GUI design is particularly dangerous because it preys on the user’s trust in the visual interface and can be difficult to detect. To mitigate these risks, developers must follow secure coding practices, conduct thorough testing of GUI elements, and educate users about potential threats associated with interacting with unfamiliar or suspicious interfaces (Bishop, 2003).

Global Regulatory Challenges

The global production and distribution of microprocessors are heavily influenced by international regulatory frameworks, particularly those emanating from the United States. These regulations, while intended to standardize and secure the use of electronic devices, often limit the ability of other nations to fully control the microprocessors used within their borders. For instance, major semiconductor companies are required to comply with U.S. regulations, which include restrictions on the use of certain radio bands and the encryption of internet data. However, these regulations do not necessarily guarantee the complete security of the chips themselves, as evidenced by the persistent security concerns raised by various nations.

The concentration of microprocessor production in regions like Taiwan, the Netherlands, and the United States adds another layer of complexity. Taiwan, for instance, produces over two-thirds of the world's microprocessors, including more than 90% of the most advanced chips. This concentration makes global supply chains vulnerable to geopolitical tensions, as any disruption in Taiwan could lead to a global shortage of microprocessors, with severe implications for industries ranging from consumer electronics to defense.

The Geopolitics of Microprocessor Production

The strategic importance of microprocessors has not gone unnoticed by global superpowers. The United States, in particular, has taken steps to limit China's access to advanced microprocessor technologies, recognizing the critical role these components play in both economic and military domains. In January 2023, the U.S. successfully persuaded the Netherlands and Japan to impose export controls on equipment used to produce advanced microprocessors, effectively restricting China's ability to develop its semiconductor industry.

Taiwan's role in the global microprocessor supply chain has been described as a "Silicon Shield," providing the island with a form of strategic deterrence against potential Chinese aggression. The United States has further strengthened its ties with Taiwan by encouraging Taiwanese semiconductor companies, such as TSMC, to invest in new manufacturing facilities on American soil. This move is part of a broader strategy to secure the supply of advanced microprocessors and reduce dependence on foreign production.

Potential for Espionage

The potential for espionage through microprocessors is a growing concern, especially in light of warnings from figures like Sayyed Hassan Nasrallah, Secretary-General of Hezbollah. Nasrallah has cautioned that smartphones can act as "killer spies," transmitting sensitive information to hostile entities. This assertion underscores the broader risks associated with the digital age, where the interconnectedness of devices provides unprecedented opportunities for surveillance and data collection.

Microprocessors, as the central processing units of these devices, are at the heart of this issue. The ability to embed surveillance capabilities within microprocessors means that even the most secure communication channels could be compromised if the underlying hardware is not trustworthy. This concern is particularly relevant in the context of military and intelligence operations, where the stakes are highest.

Different Approaches to Confront Hardware Threats and Espionage

As technology becomes increasingly embedded in every aspect of modern life, the security of hardware—particularly microprocessors and other critical components—has become a central concern for governments, industries, and individuals alike. Hardware threats, including malicious alterations, backdoors, and hardware Trojans, as well as the risk of espionage, pose significant challenges. This chapter explores various approaches to confronting these threats, highlighting the importance of a multi-faceted strategy that combines technical, policy, and operational measures.

1. Design-Level Security Measures

Design-level security is the first line of defense against hardware threats. This approach involves integrating security features directly into the hardware during the design phase, making it inherently more difficult for malicious actors to introduce vulnerabilities or exploit existing ones.

- *Secure Design Practices* : Implementing secure design practices, such as the use of trusted design libraries and tools, is crucial. Hardware designers must ensure that every component of the microprocessor is built with security in mind, using techniques like redundancy, error detection and correction, and secure boot processes to prevent unauthorized modifications (Tehranipoor & Wang, 2011).

- *Hardware Root of Trust (RoT)*: A hardware RoT is a set of security functions built into a chip that remains trusted because its integrity is verifiable. It forms the foundation for all other security mechanisms in a device, ensuring that even if other components are compromised, the core security functions remain intact (Chen & Shen, 2010).

2. Manufacturing and Supply Chain Security

The globalization of semiconductor manufacturing has made supply chain security a critical issue. Chips and other hardware components often pass through multiple stages of production, testing, and assembly in different countries, increasing the risk of tampering.

- **Trusted Foundries**: One approach to mitigating supply chain risks is the use of trusted foundries—manufacturing facilities that meet stringent security standards and are regularly audited to ensure the integrity of their production processes. Governments and critical industries often rely on trusted foundries for the production of sensitive components (Gorman, 2011).

- **Supply Chain Verification**: Implementing robust verification processes throughout the supply chain is essential. This includes the use of tamper-evident packaging, cryptographic signatures on chips, and continuous monitoring of components as they move through the supply chain. Advanced traceability mechanisms can help ensure that any unauthorized modifications are quickly detected (Koushanfar, 2010).

3. Reverse Engineering and Forensic Analysis

Reverse engineering plays a crucial role in identifying and mitigating hardware threats that have already been introduced into a system. By deconstructing and analyzing the physical components of a chip, experts can detect anomalies that may indicate the presence of hardware Trojans, backdoors, or other malicious elements.

- **Forensic Microanalysis**: This involves detailed examination of a chip's structure and operation using techniques such as Scanning Electron Microscopy (SEM) and X-ray imaging. These methods allow security experts to inspect the internal layout of a microprocessor at a microscopic level, revealing hidden circuits or unauthorized modifications (Waksman & Sethumadhavan, 2011).

- **Functional Testing and Side-Channel Analysis**: Functional testing involves running a chip through a series of predefined operations to observe its behavior, while side-channel analysis examines indirect outputs, such as power consumption and electromagnetic emissions, to detect deviations from expected behavior. These techniques are particularly effective in identifying hardware Trojans designed to remain dormant until triggered (Agrawal et al., 2007).

4. Policy and Regulatory Frameworks

Governments and international organizations play a vital role in establishing policies and regulations that promote hardware security and mitigate the risk of espionage.

- **Export Controls and Trade Restrictions**: To prevent adversarial nations from acquiring sensitive technologies, countries like the United States have implemented export controls on advanced semiconductor manufacturing equipment and design software. These controls are designed to limit the spread of cutting-edge technology that could be used for malicious purposes (Krebs, 2018).

- **Standards and Certifications**: Establishing global standards for hardware security can help ensure that devices meet minimum security requirements before they are deployed. Certifications such as Common Criteria (ISO/IEC 15408) provide a framework for evaluating the security of IT products, including microprocessors, against defined security requirements (Common Criteria, 2009).

5. Operational Security and Incident Response

Even with robust design, manufacturing, and policy measures in place, operational security and effective incident response are crucial for mitigating the impact of hardware threats.

- **Hardware Monitoring and Intrusion Detection**: Continuous monitoring of hardware components for signs of tampering or abnormal behavior is essential. Intrusion detection systems (IDS) that focus on hardware can alert administrators to potential threats, allowing for swift action to isolate and address the issue (Yue et al., 2014).

- **Incident Response and Recovery**: In the event of a security breach involving hardware, a well-prepared incident response plan is critical. This plan should include procedures for identifying compromised components, isolating affected systems, and restoring operations using backup hardware. Regular drills and updates to the incident response plan help ensure preparedness (West & Bhunia, 2015).

6. International Collaboration and Information Sharing

Addressing hardware threats and espionage requires international collaboration, particularly as the production and distribution of hardware components are globalized.

- **Multinational Security Initiatives**: Countries can work together to develop and enforce international standards for hardware security, share threat intelligence, and coordinate responses to global security incidents. Initiatives like the Wassenaar Arrangement, which controls the export of dual-use technologies, are examples of such collaboration (Wassenaar Arrangement, 2013).

- **Public-Private Partnerships**: Governments can also collaborate with private industry leaders to improve hardware security. These partnerships can facilitate the development of advanced security technologies, promote the adoption of best practices, and ensure that critical infrastructure is protected from hardware-based threats (Palmer, 2012).

Discussion

Microprocessors and Security Vulnerabilities

1. **Hidden Information Layers**: we mentioned the potential for microprocessors to contain "hidden layers of information" that could be used for espionage. The microprocessors could theoretically be designed with malicious features (like backdoors), the terminology "hidden layers of information" refers to "malicious code" or "hardware Trojans" embedded within microprocessors. These are well-known security threats that could be exploited for unauthorized surveillance.

2. **Complexity and Transparency**: The complexity of microprocessors and the concentration of manufacturing in a few countries pose security risks. Advanced reverse-engineering techniques do exist, though they are extremely challenging and resource-intensive. The difficulty lies in the fact that these techniques may not always detect subtle or well-concealed malicious modifications.

Global Regulatory Challenges

1. **U.S. Regulations and International Control**: We described how U.S. regulations affect global microprocessor production and distribution. It’s worth mentioning that these regulations not only restrict certain technologies but also seek to prevent the export of cutting-edge semiconductor manufacturing equipment to rival nations, particularly China. This is a key part of the broader strategic competition in technology.

2. **Concentration in Taiwan**: The article identifies Taiwan's significant role in global microprocessor production. This is often referred to as a "choke point" in the global supply chain, where geopolitical tensions, natural disasters, or other disruptions could have far-reaching consequences. We also reflect the strategic importance of Taiwan’s semiconductor industry, but it could elaborate on the global efforts to diversify semiconductor supply chains to mitigate these risks.

The Geopolitics of Microprocessor Production

1. **Export Controls on China**: The article points out the U.S.-led export controls aimed at restricting China’s access to advanced microprocessor technologies. These controls are part of a broader strategy to maintain technological superiority and limit China's ability to advance in critical areas like AI and military applications.

2. **Taiwan as a "Silicon Shield"**: The concept of Taiwan's semiconductor industry serving as a "Silicon Shield" is accurate and reflects a widely held view that Taiwan's economic importance, particularly in semiconductors, acts as a deterrent against potential aggression from China. The article correctly notes U.S. efforts to secure chip supplies by encouraging Taiwanese companies to invest in the U.S.

Potential for Espionage

1. **Espionage Risks**: We highlighted the risks of espionage through microprocessors. It references a statement from Sayyed Hassan Nasrallah, which, while relevant, might be better contextualized with broader examples of espionage concerns from other global leaders or experts. The concept that microprocessors could be compromised to facilitate surveillance is a legitimate and widely recognized threat in cybersecurity.

Conclusion

The security of microprocessors is a critical issue that extends far beyond individual privacy concerns. As the backbone of modern electronic devices, microprocessors play a pivotal role in global security, economic stability, and technological advancement. The potential for espionage, the impact of international regulations, and the strategic importance of microprocessor production all contribute to a complex landscape that requires careful consideration by policymakers, industry leaders, and security experts. Confronting hardware threats and espionage requires a comprehensive approach that spans design, manufacturing, policy, and operational security. By combining secure design practices, rigorous supply chain verification, advanced forensic analysis, and robust regulatory frameworks, it is possible to significantly reduce the risks posed by malicious hardware. Moreover, fostering international collaboration and maintaining vigilance in monitoring and incident response are key to protecting against evolving threats in an increasingly interconnected world.

Future research and policy efforts should focus on enhancing the transparency and security of microprocessor manufacturing, as well as developing advanced technologies for reverse-engineering and verifying the integrity of these critical components. Only through such measures can we hope to mitigate the risks associated with microprocessors and ensure that they continue to serve as reliable building blocks for the digital age. While in the context of global violence i.e. in the recent terror of Ismayil Haniyah in Tehran-Iran, the involving governments are a part of the conflicts, it is necessary to understands the threats that adhere to the many advantages of the technology including security threats and infringement in the privacy of regular users.

References

1- Agrawal, D., Baktir, S., Karakoyunlu, D., Rohatgi, P. & Sunar, B., 2007. 'Trojan Detection Using IC Fingerprinting.' *Proceedings of the 2007 IEEE Symposium on Security and Privacy*, pp.296-310.

2- ASML, 2023. 'Export Control Measures and their Impact on the Semiconductor Industry.' *ASML Corporate Report*.

3- Bishop, M., 2003. *Computer Security: Art and Science*. Addison-Wesley.

4- Chen, L. & Shen, X., 2010. *Trusted Computing Platforms: A Hardware-Based Approach*. Springer.

5- Clarke, R.A. & Knake, R.K., 2010. *Cyber War: The Next Threat to National Security and What to Do About It*. HarperCollins.

6- Common Criteria, 2009. *Common Criteria for Information Technology Security Evaluation*. ISO/IEC 15408.

7- Choo, K.K.R., 2011. 'The Cyber Threat Landscape: Challenges and Future Research Directions.' *Computers & Security*, 30(8), pp.719-731.

8- Davoudpour, A.R., 2024. 'Project "Mahan" or "Haman": An Analysis of its Pathological and Social Health Implications.' *Journal of Iranian International Legal Studies*, 1(1). Available at: https://doi.org/10.5281/zenodo.13188822 [Accessed 2 September 2024].

9- Geer, D., 2014. 'Cybersecurity as Realpolitik.' *Black Hat USA*.

10- Gorman, S., 2011. 'Pentagon's Cyber Strategy Calls for Trusted Foundries.' *The Wall Street Journal*.

11- Huang, L.-S., Moshchuk, A., Wang, H.J., Schechter, S. & Jackson, C., 2012. 'Clickjacking: Attacks and Defenses.' *USENIX Security Symposium 2012*, pp.413-428.

12- Karri, R., Rajendran, J., Rosenfeld, K. & Tehranipoor, M., 2010. 'Trustworthy Hardware: Identifying and Classifying Hardware Trojans.' *Computer*, 43(10), pp.39-46.

13- Koushanfar, F., 2010. 'Hardware Metering: A Survey.' *Proceedings of the 2010 Design Automation Conference (DAC)*, pp.676-681.

14- Krebs, B., 2018. 'US Imposes Export Restrictions on China's Semiconductor Sector.' *Krebs on Security*.

15- Langner, R., 2011. 'Stuxnet: Dissecting a Cyberwarfare Weapon.' *IEEE Security & Privacy*, 9(3), pp.49-51.

16- Maurer, J., 2017. *Social Engineering: A High-Tech Low-Tech Threat*. CRC Press.

17- Nasrallah, S.H., 2023. 'Mobile Phones as Tools for Espionage: A Strategic Overview.' *Al Rai Al Youm*.

18- Palmer, D., 2012. 'The Role of Public-Private Partnerships in Securing Critical Infrastructure.' *Journal of Homeland Security and Emergency Management*, 9(2), Article 18.

19- Richardson, R. & North, M.M., 2017. 'Ransomware: Evolution, Mitigation and Prevention.' *International Management Review*, 13(1), pp.10-21.

20- Ratti, C. & Claudel, M., 2021. 'The Geopolitics of Microprocessors and Global Supply Chains.' *Journal of International Affairs*, 74(2), pp.115-130.

21- Taiwan Semiconductor Manufacturing Company (TSMC), 2023. 'Investment Strategies and Global Semiconductor Supply Chains.' *TSMC Annual Report*.

22- Tehranipoor, M. & Koushanfar, F., 2010. 'A Survey of Hardware Trojan Taxonomy and Detection.' *IEEE Design & Test of Computers*, 27(1), pp.10-25.

23- Tehranipoor, M. & Wang, C., 2011. *Introduction to Hardware Security and Trust*. Springer.

24- Tehranipoor, M., Koushanfar, F. & Potkonjak, M., 2011. 'Recent Advances in Hardware Security and Trust.' *Design Automation Conference (DAC) 2011*, pp.289-294.

25- Waksman, A. & Sethumadhavan, S., 2011. ‘Silencing Hardware Backdoors.’ *IEEE Symposium on Security and Privacy*, pp.49-63.

26- Wassenaar Arrangement, 2013. *Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies*.

27- West, J. & Bhunia, S., 2015. ‘Gate-Level Information Flow Tracking for Security-Aware Circuit Design.’ *IEEE Design & Test*, 32(5), pp.66-75.

28- Xiao, K., 2016. ‘Security Implications of Hardware Reverse Engineering.’ *Proceedings of the ACM/IEEE International Symposium on Low Power Electronics and Design*, pp.329-334.

29- Yue, H., Liu, Y. & Shao, J., 2014. ‘Hardware Trojan Detection Based on Behavior Analysis.’ *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 33(11), pp.1648-1657.

30- Zhang, J., Tehranipoor, M. & Plusquellic, J., 2013. ‘Detecting Hardware Trojans in Untrusted ICs Using Delay-Based Side-Channel Analysis.’ *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, 18(7), pp.1063-1073.

31- United States Congress, 2022. *CHIPS Act of 2022*. Washington, D.C.: U.S. Government Publishing Office.

32- ASML, 2023. ‘Export Control Measures and their Impact on the Semiconductor Industry.’ *ASML Corporate Report*.

33- Taiwan Semiconductor Manufacturing Company (TSMC), 2023. ‘Investment Strategies and Global Semiconductor Supply Chains.’ *TSMC Annual Report*.

34- Ratti, C. & Claudel, M., 2021. ‘The Geopolitics of Microprocessors and Global Supply Chains.’ *Journal of International Affairs*, 74(2), pp.115-130.

35- Clarke, R.A. & Knake, R.K., 2010. *Cyber War: The Next Threat to National Security and What to Do About It*. HarperCollins.