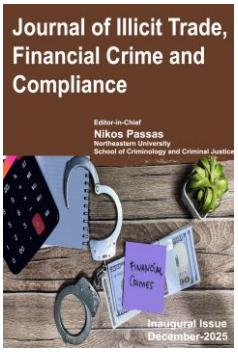
Journal of Illicit Trade, Financial Crime, and Compliance

ISSN (online): 3070-6122



Forward to the Past: Sanctions and Strategic Trade Control in the Age of Algorithms, Semiconductors and Artificial Intelligence

Enrico Carisch [1,*], Saurabh D. Chowdhury[2], Durra Sahtout[3]; Sune Danielsson[4]

[1]*Chief Executive Officer and Compliance Specialist of Compliance and Capacity Skills International (CCSI) New York, NY 10025 – USA*
[2]*Honorary Visiting Fellow of CCSI, San Francisco, CA 94121 – USA*
[3]*Digital Transformation- Artificial Intelligence Specialist and CEO of CCSI X, Paris, 75015 – France*
[4]*Strategic Trade Control Specialist, Zagreb, - Croatia*

ARTICLE INFO

Article Type: Research Article

Keywords:
Sanctions
Strategic Trade
Semiconductors
Artificial Intelligence
End-user Certification
Strategic Trade Control
Nonproliferation Regimes
GaN, Performance Elasticity

Timeline:
Received: February 05, 2026
Accepted: March 05, 2026
Published: March 16, 2026

Citation: Carisch E, Chowdhury SD, Sahtout D, Danielsson S. Forward to the past: Sanctions and strategic trade control in the age of algorithms, semiconductors and artificial intelligence. J Illicit Trade Financ Crime Compli. 2026; 2: 1-19.

DOI: https://doi.org/10.65879/3070-6122.2026.2.01

*Corresponding Author
Email: ec@ccsi.global.com

ABSTRACT

This paper analyzes how software and artificial intelligence enhancements, applied throughout the lifecycle of advanced and off-the-shelf semiconductors, enable performance elasticity—allowing standard hardware to achieve enhanced or restricted capabilities, including the development of weaponized variants. We examine how the potential for weaponizing hardware-software synergies is challenging traditional strategic trade controls and arms embargoes. In the Wassenaar Arrangement, the leading nonproliferation regime for conventional arms and dual use technologies, Russia's obstruction has frustrated the work on necessary controls. We are also discussing how these disruptions and technological advances are exploited by adversarial actors for the illegal transfer of semiconductors to the embargoed Iran, North Korea and Russia.

Our research indicates that these illegal transfers are not stopped with the recent shift by the US and EU towards "Know-Your-Product" (KYP) lifecycle governance. Their technical definitions still overlook and underregulate the versatility of the software/AI's performance elasticity and consequently, their compliance guidance is not proactive.

The Emerging Threat

Two categories of computing present the most intractable threats to peace and security:

1. Cutting-edge semiconductor designs that enable equally advanced software architectures and artificial intelligence (AI) applications will soon be further amplified by quantum technology. Commonly, they are considered dual use technologies, and their transfers are restricted under international sanctions and strategic trade controls. The reason is that they can supercharge the capacity and sophistication of modern weaponry, ranging from conventional arms to weapons of mass destruction (WMD) and ballistic missiles. Thus, the irony with these advanced technologies is that are hoped to solve humanity's greatest challenges, but when weaponized they may turn into the greatest curse.
2. Off-the-shelf semiconductors of lower technology grades that are not restricted, but sophisticated software and AI applications can evolve them into serviceable weaponized electronics. The majority of this class of semiconductors which benefit from "performance elasticity", are routinely recovered by arms investigators from Russian weapons deployed in the war against Ukraine. Vast numbers of these unrestricted semiconductors are floating around the world, ready for weaponized applications.

The European Union (EU) [1] and the United States (US) [2] initially included electronics under their dual-use sanctions when it was discovered that they enabled communication technologies Iran's Islamic Revolutionary Guard Corps used for its repression against the 2011–2012 Green Movement youth protests. With Russia's 2014 invasion of Crimea in Ukraine, the EU released its first sectoral sanctions, targeting "specific, non-military, advanced technologies, including specialized electronics, components, and software intended for Russia's defenses, security, or strategic industries" [3].

Box 1: The implications of the "US Advanced Chip Ban"

Articulated and released in January 2026, the U.S. Department of Commerce Bureau of Industry and Security (BIS) issues its Final Rule by imposing the globally binding Foreign Direct Product Rule (FDPR), which stipulates:

A final product using US-origin software or US-origin manufacturing equipment is subject to US jurisdiction.

Non-US companies using these products must prevent violating US law, or risk prosecutions and sanctions designations.

By 2022, the threat to peace and security resulting from the weaponization of semiconductor technologies had become self-evident when military-artificial intelligence applications were deployed by well-resourced adversaries like China, Russia, North Korea and Iran. Hence, far more restrictive measures were adopted with coordinated strategic trade control packages. The US 2022 "Advanced Chip Ban" changed direction by not issuing sanctions but by putting in place unprecedented trade control measures against advanced chips used for AI and supercomputing, and corresponding semiconductor manufacturing equipment.

These most recent developments challenge the existing strategic trade controls, especially the Wassenaar Arrangement (for more, see below under The Current Strategic Control Systems).

Status of the Weaponization of Semiconductors

Wide Bandgap Semiconductors

Wide bandgap transistors and integrated circuits are essential for many of the most advanced weapon and communication technologies. Because they allow for smaller, faster and more powerful designs, these semiconductors power superior missile defenses, such as the Patriot system, or enhance internal transmitters and

guidance systems that make missiles more accurate. They also maximize power-usage and thanks to the superior energy efficiency, power loss is reduced, which allows for the unleashing of low-cost UAV swarms that overpower expensive air-defenses.

Wide bandgap semiconductors can be manufactured out of various materials whose power and frequency limits yield different applications. These materials enable high power devices which can handle high voltage break down. Some popular options are listed below:

- GaAS devices (Galium Arsenide) often grown by Molecular Beam Epitaxy (MBE) operate at very high frequencies and appropriate for RF Low Noise Amplifiers and Power Amplifiers used for RF communications but also has applications in radars.
- Gallium Nitride using Metal-Organic Chemical Vapor Deposition (MOCVD) in a reactor with Gallium-based precursors such as Trimethyl Galium (TMGA), Ammonia (NH3) capped off by Silance-based precursors have also superior properties.
- Silicon Carbide (SiC) chips are epitaxially deposited on high-purity crystals of Silicon Carbide. These devices operate at lower frequency but offer the highest breakdown voltage protection making them ideal for EV traction inverters and onboard chargers.

Over the past decade, Gallium-Nitrite (GaN) technology is rapidly replacing silicon materials as a cornerstone of next-generation electronics, especially military-grade radar and EW systems. Its advantages stem from the physics of the material itself:

- Wide Bandgap Performance: GaN can handle higher voltages and power densities than silicon or GaAs.
- High Power Density: More watts per square millimeter translate directly into smaller, lighter, and more powerful transmitters.
- Thermal Efficiency: GaN devices run cooler at equivalent power levels, reducing the burden on bulky cooling systems.[4]

These strengths make GaN ideal for active electronically scanned array (AESA) radars, high-power jammers, and SATCOM uplinks. Modern radar platforms rely on GaN transmit/receive modules to deliver long-range detection and simultaneous electronic attack. In short, GaN is enabling defense systems to see farther, react faster, and pack more power into smaller footprints.[5]

GaN radar technology has become the preferred choice for high-power military radar applications, including long-range surveillance radars, fire control systems, and active electronically scanned arrays (AESAs). The technology's high-power density enables compact, lightweight radar systems suitable for airborne platforms, ships, and mobile ground systems. [6]

The dual use nature of GaN technology complicates compliance and enforcement. The technology is widely used in cell phone handsets and base stations (albeit GaAS for now) by civilian-commercial manufacturers Skyworks (Spin off from Rockwell), and Broadcom who are supplied with components manufactures by Taiwanese foundries WinSemi, Wavetech and others. For military-grade components, Raytheon, Northrup Grumman, ELTA (Israel), Thales (France) are market leaders, soon to be challenged by competitors from many other countries. Astra Microwave in India, designer and manufacturer of high-tech microwave and RF subsystems is an early example of the emerging global military and dual-use electronics ecosystem.

AI Processors and Advanced Memory Technology

Semiconductor building blocks for the next weaponization jump will likely include AI-guided hypersonic missiles that overcome navigation-jamming while flying at five times the speed of sound hitting its target with deadly accuracy. Here too, a suite of semiconductor qualities is needed, such as advanced thermal management materials and radiation-hardened silicon to withstand intense heath, and potential exposures to high-energy particles or

electromagnetic waves. Additionally, parallel processing capabilities capable to run complex machine learning that can manage trajectory optimizations and moving target acquisitions at hyper-speed.

These are among many other technical breakthroughs that advanced semiconductors powered by enabling software and AI either already master or are about to deliver computing capacities that will make weapons far more effective. The following weapons systems already deployed, are examples for applications of advanced hard/software:

- South Korea operates electronic sensors that trigger prepositioned and hard-mounted sentry guns when any invader, vehicle or human crosses into its crosshairs. The U.S. Task Force 59 is the leading entity for operational deployment of military-grade, AI-supported unmanned surface vessels (USV), unmanned underwater vehicles (UUV), and unmanned ground vehicles (UGV) [7]. They not only enhance maritime domain awareness but also detect suspicious behaviors in operational zones of its fleet.
- The prototype Sea Hunter is currently tested as part of Ghost Fleet Overlord design efforts of large, autonomous surface vessels.; and Project Overmatch is intended to integrate AI across the U.S. Navy's fleets. [8]
- The U.S. Army, partly building on developments from German defense contractor Rheinmetall, is building and testing UVGs for logistics, reconnaissance, and combat support [9].
- Turkey's Savunma Teknolojileri Mühendislik ve Ticaret A. Ş. (Defense Technologies Engineering and Trade Inc.) is producing the Kargu-2 drone, an AI-enabled loitering "kamikaze drone" can detect and target humans using facial recognition and real-time decision-making algorithms. It has been deployed in Libya, Syria, Nagorno-Karabakh (Azerbaijan), and with other, undisclosed military organizations [10] [11].

The Conundrum of Controlling Software and Artificial Intelligence

Semiconductor capacity results not only from sophisticated hardware designs but is massively amplified by knowledge, software, automation, information management, AI analytics, and other types of ongoing optimizations. Periodical updates of software shape and maximize the capacities of semiconductors, especially those for military applications, throughout the chip's lifecycle. While hardware design sets the ultimate generic computational limits, customizing software layers to the desired application maximizes hardware performance for specific military tasks. This is how less advanced chips can be repurposed to achieve a "good enough" performance at far lower costs than advanced chip designs.

Furthermore, software tools and knowledge that enable the design and manufacturing of chips are intangible –- hence, far harder to control -- but are as essential as silicon to bring chips to life.

Box 2: Regulating "Strategic Performance" or "Strategic Elasticity"

Policy frameworks will have to recognize the semiconductor lifecycle as a sequence of software-governed layers. Each layer can add an additional capability to gain knowledge, develop, use and reuse hardware; offering a room for open innovation and flexibility in the ecosystem, which we call "strategic elasticity"; where evolving software and logic leads to evolving mission capabilities and reduced know-how gaps.

Four key takeaways emerge:

1. The right software and knowledge can enhance capability, including for military and security applications.
2. Limiting access to advanced general-purpose hardware does not prevent extracting higher, task-specific performance from less advanced chips, which highlights the need to focus on software and knowledge as key strategic performance enablers.
3. Access to intangible tools and logic can iteratively narrow the know-how gap, which remains a central concern in strategic security-risk competition.

4. Data lifecycle and, open-source algorithms are as crucial as other assets in an AI-powered era.

While full control through strict regulatory approaches is often viewed as neither feasible nor desirable, policymakers may consider selective governance. Such governance can be achieved by identifying and addressing critical elasticity enablers within the semiconductor software stack.

Semiconductor Lifecycle Software Stack

Pre-Silicon Layer

Chips are virtually built and tested. Using electronic design automation (EDA) software and simulation tools ensure design efficiency before manufacturing. Process design kits (PDKs) and library characterization are other important components that encode physical manufacturing feasibility and limits. Strategic sensitivities are based on three aspects:

1. The outputs are digital data and intangible technical knowledge that can be transferred across international borders with minimal risk of discovery.
2. The software tools and PDKs used for commercial purposes are often the same as those used in sensitive applications – which classifies them as "dual-use" technology. Restricting the trade in specific software features helps, but it is not a full solution. People can bypass limits by using legacy versions or creating custom plugins.
3. Cloud-based design tools, operating in vague jurisdictional spaces, increase the likelihood for unauthorized entities gaining access and exfiltrating them in impunity.

Possible Solution:

Proactive management of these risks before and after distribution and address circulation of intangible knowledge and design outputs, while tightening collective and selective governance for cloud security.

In-Fab Manufacturing Layer

Thanks to AI, the manufacturing process is becoming a self-optimizing ecosystem, where tools such as agentic AI analyze real-time sensor data and adjust process parameters, such as etch uniformity and lithographic recipes, at the atomic level without human intervention. The shift here is that AI-supported manufacturing is moving from being led by humans using machines to being managed by algorithms, which introduces these new risks:

1. Fabrication expertise built into trained AI models can, among many other tasks, improve the performance of older chips. But it is hard to audit these manufacturing processes for security, essentially the work of autonomously operating software that can keep changing the manufacturing outcome, for example to build high-spec, restricted components while appearing to optimize commercial chips. How will it be judged for its decisions, or rather who should be judged?
2. AI model training and retraining in modern fabs rely on cloud services, creating a digital twin outside the physical fab and making manufacturing secrets vulnerable to unauthorized access.

Possible Solution:

To contain the manufacturing AI, controls must cover the physical equipment, algorithms, data, and knowledge that dictate how equipment behaves.

Post-Silicon Optimization Layer

Chip's efficiency is managed through software such as firmware, hardware abstraction layers (HALs), and intermediate representations (IRs). These tools guide resource allocation and direct data flow, boosting processing for a specific task. Other development tools and technical documents can demonstrate how hardware behaves and

its limits. This allows even deeper software-level optimization, but leave these risks unanswered:

1. Performance can be enhanced using advanced compilers and optimization tools that task a general-purpose chip with a specific mission.
2. A chip can be exported across international borders as a low-end item, then upgraded locally with appropriate programming into a high-performance, task-specific asset.

Possible Solution:

The use of immutable firmware and on-chip tracking can improve baseline security. However, other optimization and open-source tools, compilers, and human skills can still reshape hardware use, enabling multiple chips to be repurposed for restricted uses such as drone swarms and similar military applications.

Orchestration Layer

Ultimate computational capability depends not only on a single unit but also on how multiple hardware units are managed in real time. Distributed execution frameworks, orchestration runtimes, low-latency interconnect drivers, and virtual clustering technologies are crucial to control workload scheduling, memory, and data movement across different types of semiconductors. Software runtimes enable performance improvements by combining components into an orchestrated, unified system, still leaving however, these concerns:

1. Combining multiple mid-tier or legacy chips into a single virtual high-performance system can enable capabilities comparable to high-end systems. Effective controls can only be applied by shifting from hardware to software coordination and its tools.
2. Deep knowledge of these tools enables users to improve communication between units and eliminate delays, raising performance above normal hardware limits.
3. Runtime tools can hide the physical identity of hardware, making it harder to track where sensitive, potentially strategic computation is enabled.

Potential Solution:

Software-defined multi-chip systems must be controlled by targeting the runtime frameworks and logic.

Operational and Information Layer

The supporting functions across the full semiconductor lifecycle rely on data, metadata, and management systems, including product lifecycle management tools, supply chain systems tracking material flows, telemetry systems, and failure data. Important but overlooked knowledge and metadata are captured by those systems that, if accumulated, can reveal design priorities, manufacturing limits, and supply weaknesses. Protecting this knowledge reduces potential intelligence gaps and helps track key suppliers and logistics.

“Elasticity” Multipliers

AI and Data

Across the full lifecycle, artificial intelligence emerges as an amplifier of semiconductor capacities. They lend “elasticity” that can speed up design, manage fabrication in real time, while AI-compilers and tools optimize computing power based on workloads. Furthermore, AI studies design and manufacturing data, creating feedback that guides future work. It also helps analyze large data from open research. The emergence of AI is now highlighting the power of data, logic, and models, making it crucial to address AI tools, datasets, and automation capabilities.

The Confidential Gap in the Cloud

A second "elasticity" can occur with cloud services providing services to users that will perform strategic and potentially restricted computations. Even when the cloud service is configured for full compliance, the actual computations of clients remain invisible unless the cloud service owner breaks the confidentiality terms of the user contract. Hence, an existing array of hard/software can be exploited for illegal uses.

Table 1: "Elastic Capacities" that can Reduce Sovereign Controls.

Layer	Elastic capacity	Strategic impact
Pre-silicon (Design)	Knowledge and design efficiency	Design tools are dual use and can enable sensitive designs such as custom crypto/anti-jamming ASICs– that can be shared digitally. While some features can be restricted, access to them is still possible through legacy tools or plugins. These tools come with knowledge and libraries that encode manufacturing feasibility; offering some understanding into the manufacturing brain beyond just design.
In-Fab (Manufacturing)	Manufacturing expertise & uplift	AI-powered manufacturing can be harder to audit; offering the capacity to tuning fabrication recipes to military-grade specs. Relying on cloud-based AI machines to analyze manufacturing data creates digital twins (fab replica) exposing manufacturing secrets to potential unauthorized access.
Post-silicon (Optimization)	Performance uplift	Low-end chips performance can be uplifted to carry specific tasks such as upgrading commercial GPUs for cryptographic cracking or targeting-specific AI workloads for intelligence, surveillance.
Runtime & Orchestration	Aggregated compute	Create shadow supercomputers with advanced computational capacity using a network of hidden nodes and devices dispersed geographically while their locations remain masked. This computational power is useful for missile guidance simulation or large-scale war-game modeling and it's harder to identify or track across the network.
Operational & Information	Operational intelligence	Important information and metadata about the ecosystem, the actors, and the operations can be accessed and accumulated over time, leading to reduced know-how gap. Supply chain insights extracted from metadata can be weaponized through identifying weak suppliers or bottlenecks to apply pressure or sabotage military supply chains

Implications for Compliance

In the accelerating semiconductor environment where "performance elasticity" poses a security threat, traditional compliance frameworks should adopt dynamic strategies. Corporate and policy teams are encouraged to shift their actions from a one-time compliance set to a continuous lifecycle monitoring-due diligence model to manage risks proactively (see Conclusion for more details). Today's challenge is to monitor and manage the software, data, and AI systems that can transform ordinary hardware into strategic assets.

Box 3: Definition of miliary items and dual use-goods and technologies

A military item is defined as an item, goods or technology that is designed, developed, produced and used for military purposes.

A dual-use item is an item that is developed or produced for civil use but can be used for military purposes. Used for military purposes means that it can be used for the design, development or production of a military item, i.e. an item included in the military list.

The Current Strategic Control Systems

Purposes and Functions of Nonproliferation Regimes

Even during the Cold War, the transfer of semiconductors was restricted under the Coordinating Committee for Multilateral Export Control (COCOM) [12]. Similarly to today's strategic trade controls (STC), COCOM targeted semiconductors primarily as a dual-use technology and restricted the transfer of chips, electronic equipment containing chips, and related manufacturing tools. Since the end of the Cold War and with the accelerated WMD proliferation and development of very smart delivery systems such as ballistic missiles, cruise missiles, UAVs and others, but also the production of advanced conventional weapons, far more complex controls have been instituted. These controls are based on the evaluation of threats to national and international security which are implemented by laws and regulations at the national level and are formulated by:

- Multilateral decisions by the UN provide only broad and relatively generic restrictions, while EU, US, and other sanctions regimes add very specific definitions and guidance.
- In international nonproliferation regimes composed of states with advanced technological capabilities formulating lists of controlled items in considerable technical detail.
- National nonproliferation laws spell out in legal terms rules and regulations implementing sanctions and export controls adopted by international, and regional organizations and the international non-proliferation regimes.

Box 4: The authoritative nonproliferation regimes are:

Zangger Committee - nuclear items that require International Atomic Energy Agency safeguards [13].

Nuclear Suppliers Group (NSG) – all restricted nuclear-related technologies [14].

Australia Group – all restricted chemical and biological substances and related dual use technologies that could be used for weapons of mass destruction (WMD) [15].

Missile Technology Control Regime (MTCR) –restricted components used in delivery systems for WMD such as ballistic missiles and unmanned aerial vehicles (UAV) [16].

Wassenaar Arrangement (WA) – restricted conventional arms and related dual-use goods and technologies [17].

The consensus-based technical definitions and guidance of the regimes provide a valuable component to safe and secure international transfers of weapons technologies. However, with Russia blocking urgently needed consensus for the controls of semiconductors, the regimes' ability to provide guidance is disrupted.

The Split in the Wassenaar Arrangement

One of the most important – if not the most important - task of the Wassenaar Arrangement is to define the conventional arms and dual-use technologies which are subject to control before they are exported. These products and technologies are included in the Arrangement's Munitions List and List of Dual-Use Goods and Technologies. The decision on amending the lists - including adding new items to control - requires consensus. Following the adoption by the Wassenaar Plenary of amendments to the control lists, it is up to the member states to incorporate them in their national legislation to make them legally binding on exporters. This, however, does not exclude the right of member states to apply exports control also on items outside the Wassenaar control lists which are deemed important to control.

Following the Russian invasion of Ukraine, the work of the Wassenaar Arrangement became polarized. Russia refused to accept any new controls on new sensitive technologies, especially on semiconductors and digital technologies. In this situation, several Wassenaar member states decided that high-end semiconductors and other sensitive items could not be left outside exports control. For this reason, several states, including the US, UK, and others, decided to include exports control - on a national basis - on items where consensus had not been possible to reach in the Wassenaar Arrangement because of Russian opposition.

The dual-use list of the EU member states is adopted by the EU, and following the disagreements with Russia, it has adopted the same solution now sometimes referred to as "Wassenaar minus One" to account for Russia's exclusion. This has been explained with the following public statement: "the EU has included in its control lists, export controls that are agreed at multilateral level, but where formal adoption is blocked by Russia. It is much better to have one set of uniform EU controls, especially in our internal market where goods controlled by one Member State can freely be transferred to others where they may not be adequately controlled and subsequently exported. This helps to avoid risky loopholes." [18]

Over the last ten to fifteen years a global standard of strategic trade control has been emerging based on the control lists built and regularly updated by the non-proliferation regimes. By incorporating the control lists of all the regimes in its Common Military List and its Dual Use List, the EU has greatly contributed to the establishment and /or updating of national strategic control systems in many non-EU-nations.

The provisional "Wassenaar Minus One" solution's inclusion of advanced sensitive technologies such as semiconductors and related software/AI is instructive for many nations but may not prove to be as effective as Wassenaar Arrangement designation. On the other hand, with the EU Control Lists representing an emerging global standard, the EU decision of September 2025 to update of its Control Lists and to align it with "the commitments that Member States have accepted, as members of the Wassenaar Arrangement" may mitigate the international discord on advanced technologies [19].

Chinese Weaponization of Advanced Semiconductors

Chinese semiconductor, software and AI development result from a network of the world's most advanced scientists, extremely efficient R&D efforts, and manufacturing facilities that present a very serious strategic threat to the rest of the world.

Under China's Military-Civil Fusion (MCF), systems are either in an advanced stage of development or already delivering autonomous, self-optimizing combat systems that can out-decide any opponent.

These networks consist of hundreds of entities, with the following mostly State-owned-Enterprises (SOE) forming the backbone for the progress in critical technologies:

- HiSilicon (Huawei) whose Ascend semiconductors are the backbone of the tactical AI integrated into the most advanced weapons deployed by the Peoples Liberation Army (PLA).
- Baidu (Kunlunxin) produces Kunlun AI chips that the PLA uses for real-time target recognition and "automated battle management" systems.

- DeepSeek AI algorithmic efficiency helps to weaponize “cheap but good-enough” chips to enhance the lethality of conventional weapons.
- Shanghai Fudan Microelectronics supplies PLA with Field Programmable Gate Arrays (FPGA) to increase the reliability of the guidance systems of the Chinese DF-17 hypersonic glide vehicle.
- Gowin Semiconductor tailors FPGA technology for secure communication and drone control links, which enables unmanned swarm-weapons.
- Semiconductor Manufacturing International Corp (SMIC) is China's premier foundry and assumed to be the only one capable of fabricating the chips designed by HiSilicon.
- Jiangsu Changjiang Electronics Technology Group (JCET) is the global leader in Advanced Packaging (Chiplets) that allows the merging of several less-powerful chips into a single powerful unit as elaborated in the previous section which is a critical skill for the “Cheap but good enough” strategy.

The following five Chinese weapons systems, are considered the most advanced currently fielded, and are enabled by the most sophisticated semiconductor technologies and AI:

DF-61 and DF-5C Intercontinental ballistic missiles whose guidance, targeting and flight controls, and anti-jamming operate thanks to high-reliability, radiation-hardened semiconductor components, while AI provides pre-launch targeting analysis, threat modeling, and counter-interception prediction.

Hypersonic YJ-17, YJ-20, DF-17 missiles are built with the most advanced thermal-resistant semiconductors to compute its sensors that must navigate the chaotic airflow triggered during hypersonic flight and hit the intended target. The AI provides critical evasion options when the missile is targeted by incoming defensive fire or counter-missile attack.

Liaoyuan-1 or OW5 laser weapons are directed high-energy systems designed as anti-drone defense. They require semiconductor-based laser diodes whose combination of size, efficiency, precision, and speed enable high-efficiency power conditioning electronics and precision optical tracking systems. To guide, shape and stabilize the directed energy (laser) these lasers depend on the computational power of FPGA/ASIC-based beam control modules, another class of very advanced electronic processors. The AI enables the predictive flightpath tracking and hitting of fast-moving targets, like drones, and missiles, and is being trained for targeting also hypersonic missiles.

Type-100 main battle tank heavily relies on advanced semiconductors and AI to operate its 360-degree multi-radar detection of opponents’ radars, drone and other attack weapons, and to deploy its lasers that disrupt the guidance of incoming missiles and drones. The tanks most advance feature is its ability to be electronically networked into the broader battlefield optical, thermal, and radar sensors to gain “see-through armor" views and beyond-visual-range and its AI assists in automatic coordination with unmanned aerial and ground vehicles.

Cheap but “Good-Enough”

The above discussed expensive highest technology systems do not present the most significant threat to peace and security. The cheap but “good-enough” strategy, built on semiconductors that are often classified as below dual-use restrictions, present an even more intractable challenge. UN sanctions investigators keep finding and reporting for more than 10 years, for example, with the Houthi insurgency in Yemen how they fabricate with off-the-shelf, and some Iranian technology, UAVs and ballistic missiles. With their cheap but good enough approach, their missiles and UAVs have been effectively terrorizing maritime traffic through the strategic Strait of Aden [20]. Chinese ingenuity and as “leader in low-end microchip manufacturing and the world’s top chip importer, has advance this method which among others, has now become the foremost supplier of semiconductors to Russia.” [21]

This class of semiconductors can be purchased often in bulk from online retailers for a few U.S. Dollars, with no end-use certification or licensing requirements. A more expensive sourcing alternative, reportedly practiced by Russia, is the extraction of chips from household and consumer electronics like smart phones, dishwashers, cameras, watches, binoculars, electro-microscopes. But the fact that these semiconductors are found in weapons should serve exporters as clear evidence that these electronics can have lethal applications. Hence, exporters must

practice due diligence, examine both, the end-users through Know-Your-Customer practices and, just as importantly apply to their own products, the principle of Know-Your-Product.

Table 2: Cheap but "Good-Enough" Semiconductors or Electronics Include.

Components are intended for:	But are also used to:
Microcontrollers (MCUs)	Power flight controllers, guidance boards, fusing systems, and telemetry.
Electronic speed controllers (ESCs) and motor drivers	Operate UAVs, loitering munitions, and makeshift cruise-missile engines.
GNSS modules (GPS/GLONASS/BeiDou)	Navigate and target.
MEMS sensors or inertial sensors	Stabilize and provide basic guidance for UAVs
Radio Frequency transceivers and telemetry modules	Assist as command links, video downlinks, or one-way triggering devices
Power-management integrate circuits	Serve as flight controllers, proximity fuses, and guidance boards.
Commercial Field programmable gate array (FPGA) and Complex Programmable Logic Device (CPLD)	Be used for flexible signal processing, simple digital logic which is very useful for changing or testing with new hardware designs.
Analog-to-digital / digital-to-analog converters (ADCs/DACs)	Act as sensor integration devices.

The Special Challenge of Free Trade and Special Economic Zones

The question is whether semiconductor-manufacturing nations have established and are enforcing credibly and effectively STC and international embargoes on their trade, export, import, transit or transshipments of electronic components. International sanctions do not distinguish between jurisdictional differences that some countries create with special laws and exemptions in their special economic (STZ) or free trade zones (FTZ). These zones are long recognized for their enforcement vulnerabilities as the table below demonstrates that breaks down the relevant jurisdictions and the presence and quality of their STC mechanism.

Table 3: Jurisdictions with Significant Semiconductor Production and STC.

Country	STC Yes/No or "?" when Uncertain	Country	STC Yes/No for Uncertain
Jurisdictions with advanced semiconductor design, manufacturing or related technologies		Other jurisdictions with significant semiconductor design, manufacturing or related niche technologies	
United States	Yes **	China	No
Bureau of Industry and Security		Ministry of Commerce of the People's Republic of China	
Netherlands	Yes (Central Import and Export Office)	Germany	Yes
Central Import and Export Office		Federal Office for Economic Affairs and Export Control	
Taiwan	Yes	France	Yes
Office of Trade Security Controls		Interministerial Committee for the Study of Export of War Materials	
Japan	Yes	Italy	Yes
Ministry of Economy, Trade and Industry		Unit for the Authorizations of Armament Materials	
South Korea	Yes	Singapore	Yes
Ministry of Trade, Industry and Energy		Singapore Customs / Ministry of Trade and Industry	
Jurisdictions with specialized design, manufacturing and assembly/testing niches or semiconductor intellectual property (IP)			
India		Switzerland	Yes
Directorate General of Foreign Trade		State Secretariat for Economic Affairs	
Malaysia	?	United Kingdom	Yes

Strategic Trade Secretariat		Export Control Joint Unit	
Vietnam	?		
Ministry of Industry and Trade			
Selection of jurisdictions with strong industry of SEZ/FTZ *			
Azerbaijan	?	Mexico	Yes
State Service for Mobilization and Conscription		Directorate General for International Trade Rules	
Estonia		Panama	No
Strategic Goods Commission			
Chile	No	Poland	Yes
		Department of Trade and International Cooperation	
Ireland	Yes	Thailand	
Trade Licensing and Control Unit		Department of Foreign Trade	
Israel	?	Turkey	?
Defense Export Control Agency		Export Controls Unit	
Hong Kong	?	United Arab Emirates	?
Strategic Trade Controls Section		Export Control Office	

* A complete list of countries exceeds the space available. The UNCTAD World Investment Report 2019 offered the most comprehensive discussion on the subject and did conclude that nearly 75% of UN member states operated in that year some version of an SEZ/FTZ.

** 1. Sufficient control exists on sale of advanced processors-AI processors build with 2nm technology and very high-speed RF chips and MEMS accelerometers for missile guidance-need verification.

2. Sufficient control exist on sale of advanced processing equipment-such as lithography equipment (EUV lithography tools needed for 2nm node made by ASML Netherlands).

3. Almost no control on sale of mixed signal analog, Si Photonics or MEMS chips.

4. Almost no control on sale of equipment needed to make mixed signal analog, III-V analog, Si Photonics or MEMS chips. DRIE etchers, MOCVD reactors, chemical precursors, substrates -Silicon carbide of high-purity grade, gases of high purity grade photoresist can be made raw materials that will need export control clearances with end-user verification and safeguard regimes in place (Advanced Protocol) just like enriched uranium is controlled for civil nuclear power reactors. Such system not in place today. This is do-able as probably not more than 500 wafer fabs worldwide. PRC participation in such a global regime a must.

Violations of Autonomous or Unilateral Sanctions and STC

International sanctions and STC mechanisms adopted by individual countries (often referred to as unilateral or autonomous sanctions) are often based on the professed need to protect national security and enforced unilaterally. That is why the US [22], sometimes also the EU, and many other countries, have adopted and are enforcing their unilateral restrictions against the transfer of semiconductors to Russia, North Korea, and Iran.

China, often reported as both, the biggest client of and the biggest competitor in semiconductor technology development, it is also dominating global rare earth minerals processing, a critical commodity to produce semiconductors. While it has expanded its own semiconductor manufacturing industries enormously, the country still consumes almost half of global production. Its procurement agents are often described to resort to every conceivable tactic to gain access to the most advanced semiconductors, related IP and manufacturing tools. Consequently, sanctions and STCs were imposed by the US, EU and other countries, and are continuously upgraded to blunt China's access to these cutting- edge technologies, especially if they enable military applications.

Even though countries who impose semiconductor sanctions not only have the political weight to enforce them but are also technologically the most competent as they tend to be part of the global supply chain, their enforcement efforts have yielded at best mixed results. The effects of their restrictions have achieved four impacts:

- Buyers of high-performance processors and advanced manufacturing tools on behalf of sanctioned countries (China, Russia, North Korea, Irania) are forced to take circuitous detours via third countries, with Chinese entities often serving as their most reliable suppliers of the black-listed technologies.
- These target countries often resort to the "cheap but good-enough" strategy, by acquiring lower-grade, unrestricted technologies, amply their capacity with advanced software designs, and reverse-engineer their weapons systems to match the capacity of their electronic components.

- Credible reports show that Russia is forced to extensively cannibalize old military stock but also industrial and household equipment to secure sufficient quantities of semiconductors for its war effort against Ukraine.
- When attempting to develop their domestic semiconductor manufacturing capacities they often fail [23].

Compliance Failures Enable Illegal Transfers of Semiconductors

And yet, Russia is not losing its war against Ukraine, even as the country pays a high price in blood and for a ruinous amount of its scarce treasury for the procurement of advanced weapons. North Korea and Iran are also paying a high price to acquire semiconductors. But North Korea continues to expand its WMD arsenal, and Iran has at its disposal a fearsome arsenal of ballistic missiles and UAVs. Both countries have apparently secured sufficient semiconductors to serve now Russia as important ballistic missile and UAV suppliers.

Investigators continue to find on Ukraine's battlefields evidence of Western semiconductors in Russian weapons. A 2025 report, titled "Parts of the Problem: Tracing Western Tech in Russia's Deadliest Jets" provided evidence for the presence of 1,115 verified microelectronic components manufactured by 141 Western firms, including Intel, AMD, Texas Instruments, and Analog Devices. [24].

The poor effectiveness of international sanctions against North Korea and Iran is even more disconcerting. Notwithstanding that they have been in force for 19 years the merger of digital technologies with evolving WMD, interceptions and seizures of chips destined to the arms factories of North Korea and Iran are rare.

Reported examples are Iran's sale of 400 surface to surface Fateh-110 missiles to Russia in early 2024 [25]. Even more dramatic evidence was delivered by the Multilateral Sanctions Monitoring Team that consolidates the intelligence of 11 countries and that has reported about North Korea having shipped "more than 20,000 containers of munitions since September 2023" to Russia [26]. The munition included missiles, artillery, rocket launchers and other ordinances that if not themselves containing chips, their mass-production almost certainly depends on the heavy use of digital technologies.

The trouble lies primarily in the fact that many of the smuggled semiconductors may or may not meet the technical standards for a classification as a controlled dual-use item. An additional factor is very poor awareness and generally insufficient enforcement by many states against transfers of semiconductors that should be controlled for their technical characteristics and end-use. This class of chips float around the world markets with little controls or accountability required. Investigations of the microprocessors built into Iranian unmanned aerial vehicles that Russia has been deploying against Ukraine confirm again the presence of products of most major Western manufacturers. They include in the Shahed-131 (Geran-1) and Shahed-136 (Geran-2) typically dual-use microchips such as Texas Instruments' TMS320 processors (voltage step-down converters); Analog Devices' signal processing semiconductors; Microchip Technology's LDO chips; Advanced Micro Devices' and Xilinx's field-programmable gate arrays used for signal processing and anti-jamming systems; and Nvidia's Jetson Orin and other AI-focused processors.

Products from European and other manufacturers include NXP Semiconductor's customizable integrated power management circuits, Infineon Technologies' transistors and integrated circuits; STMicroelectronics' microcontrollers, processors, flash memory, and voltage regulators; U-blox's GPS tracker chips and GNSS modules; Aura Semiconductor's PLL-based chips for anti-jamming. Finally, as Western companies are strengthening their compliance procedures, they are replaced by Chinese components such as products by Beijing Microelectronics Technology Institute.

A particularly vital black market for Russian and other semiconductor buyers are Chinese suppliers based in Hong Kong. An investigation by the New York Times revealed that Russia was able to procure from Hong Kong entities semiconductors with a value of USD 4 billion since the Ukraine invasion had begun [27], [28]. The article provided an initial glimpse behind the international sourcing efforts that Russia is now forced to undertake. Post-factum, the U.S. Department of the Treasury responded swiftly by announcing the targeting with sanctions 275 individuals and entities from 17 different jurisdictions that were "involved in supplying Russia with advanced technology and equipment that it desperately needs to support its war machine" [29].

Are Existing Controls and Blocking Mechanisms Effective with Semiconductor Technologies?

Multilateral and International Organizations

Sanctions decisions by the United Nations Security Council (UNSC) require the consent of 9 out of the 15 member states to avoid triggering a veto of the permanent 5 members (China, France, Russia, United Kingdom, United States). Therefore, any attempt to impose further restrictions to semiconductor technologies to existing sanctions or to add new ones will inevitably be stopped by Russia's veto power, and very likely China will exercise its veto too. The EU's "restrictive measures" can be stymied too because decisions must be voted unanimously by its 27 members. Hungary's Prime Minister Viktor Orbán, sometimes supported by others, has frequently abstained or voted against decisions that are not in tune with his alignment with Russian policies and interests.

The nonproliferation regimes are most directly affected by the geopolitical discord. They can add items to their lists only with a unanimous consent which for the WA requires the agreement of its 42 members. Similarly, the NSG requires the consent of 48 members, MTCR 35 partners and with the AG it's 42 members that must affirm their consent. Under the current geopolitical conditions, additions of semiconductor technologies and related dual use items are difficult to achieve in regimes because Russia is a member in all but the Australia Group and opposes any changes that would weaken its ability to acquire arms and related technologies.

Is there a Technological Shortcut?

In the absence of consensus-based decisions by members of the nonproliferation regimes, political and governmental initiatives, policy makers and technologists of Western think tanks such as the Center for New American Security (CNAS) or the RAND Corporation have been exploring over the past years how to imprint enforcement mechanisms directly onto the most advanced semiconductors. Effectively, they are expanding widely practiced commercial and general security technologies that manufacturers of chips have in use for a long time.

One widely accepted idea is to embed a Radio Frequency Identification (RDFI) tag on a sensitive semiconductor to discourage unauthorized end-uses/users [29]. Leaving aside the fact that even RFI tags on weaponized semiconductors require a STC license, far more elaborate tracking could be accomplished by embedding coded instructions with so-called "on-chip governance" approaches. These solutions not only track physically the whereabout of sensitive semiconductors, help to authenticate licensed users and uses throughout the lifecycle of a chip, measure and block transgressions of pre-defined performance benchmarks, and cryptographic protections add protections against unauthorized uses/users. Some also believe that "kill-switches" could be installed to render any device unusable [30]. However, these devices too will be subject to STC licensing.

While the manufacturers have a self-evident interest in security, trust, and supply chain integrity it does not automatically follow that they endorse the think tank's visions for their role in strategic security. It's noteworthy that neither the Semiconductor Industry Association (SIA) nor SEMI, the two global industry associations, have articulated their positions regarding these technologically enhanced trade control mechanisms.

SEMI is working with its industry partners on a systematic assessment, called Phase 0 Traceability. While SEMI supports its members' compliance with all existing laws, sanctions and trade controls, the objective of its assessment is to set its membership on a trajectory where no regulations will be required as the participating companies expect to outcompete its competitors, regardless from which political or geographic bloc they are originating.

Box 5: What is the purpose of RFID and On-chip Governance

Physical features that are imprinted into the silicon of each chip to provide a trusted platform for:

Verification with privacy-preserving attestation of chip usage, such as:

Total compute performed (e.g., FLOP counts for training runs).

Dataset or model properties.

Cluster configuration or approximate location.

Enforcement of restricted violations, such as:

Unlicensed end-uses

Fixed-set limits on restricted uses and operations.

Monitoring and detection of unauthorized uses and applications.

Location or anti-tampering checks to prevent illegal diversions and smuggling.

The designers of these technology solutions are missing fundamental issues that make many of their visions impractical. Unlike common criminal perpetrators who tend to be motivated by material gains and can often be deterred with stiff penalties and other punishments, strategic violators act on ideological motivations. However misguided, they are patriots or believers in their national interests and will not be discouraged by the risk of incarceration or other penalties. With these very determined actors, RFID traceability doesn't change anything. They measure success by how well they execute the order of their superiors – which is capturing an elusive technology or semiconductor. Consequently, the post-factum traceability of stolen semiconductors via technologies like RFID is irrelevant.

Table 4: Distinctions between criminal perpetrators and strategic state-sponsored actors.

Type of Violator	Motivation	Deterrent Effectiveness
Common Criminals	Greed and material gains.	High. They calculate the benefits of their actions against potential costs; thus, the risk of incarceration and loss of ill-gotten gains is an effective deterrent.
Strategic Actors	Patriotism, national security, ideology	Low/None. Their success is measured by meeting the expectations of their leaders and service to their nation.

Conclusions

Preventing irresponsible nations from acquiring advanced semiconductors and related dual-use AI/software technologies is a matter of common sense and global security. The recent breakdown of consensus-based Wassenaar Arrangement represents a significant setback for efforts to curb the illicit weaponization of digital technologies, to avert the catastrophic escalation of digitalized warfare that threatens humanity, and to protect orderly international trade. It perhaps foreshadows a future that will be very reminiscent to the Cold War style strategic trade control that was not based on global and consensual agreements.

At the same time, excessive restrictive controls risk denying societies the broad benefits of the digital transformation. Effective governance of these technologies must therefore go beyond traditional arms control objectives and ensure that they harness their innovative power for the advancement of all humanity, while robustly safeguarding against misuse.

With this background in mind, possible technological solutions have emerged for example with the use of Radio-Frequency Identification devices (RFID), and "on-chip-governance" solutions. (for definition see Box xx). They seem

to answer to the traceability challenges – tracking from point of origin to effective end-use of arms and weaponized technologies - that have bedeviled all enforcement of embargo decisions. They could buttress the frequent gaps between licensed user/uses and actual end-use/user.

If the costs of embedding these technologies on chips can be reduced to be applicable even to the 'cheap-but-good-enough" chips, they might just present an elegant solution to an intractable problem. However, the mass application of RFID and "On-Chip Governance" technology raise a host of new problems, many seem as intractable as the original enforcement challenges with semiconductors they aspire to resolve (see Box xx).

Box 6: The challenges with RFID and "On-Chip Governance"

Who will control the data collected with RFID and "on-chip-governance" technologies?

What predicate facts must be present to force a sharing of the data with national or international enforcement authorities?

Do technology include a "kill-switch" to disable the device – and if yes, on whose authority will it be triggered?

Could a non-cooperative manufacturer who does not abide by data-sharing rules with relevant government entities, be held liable for secondary sanctions or criminal prosecutions?

Which nation will govern these technologies and their use – the one where the chip is manufactured, where the IP is registered, or where the chip is used?

Who will ensure that these technologies are not turned against the interests of the buyer?

Even with the integration of RFID or "On-Chip Governance" technology into international sanctions and strategic trade controls of semiconductors, and their enabling software and AI, these fundamental requirements must be still met by policymakers, the industry and any international or multilateral control mechanism:

- Technical definitions or characteristics of semiconductor technologies that can be weaponized.
- Methods to assess technical terms for software/AI upgrades that can weaponize semiconductors.
- Make KYP effective by linking it to above technological definitions.
- Supply-chain integrity from point of origin to the point where outdated chips are rendered useless.
- Definition of hard/software and AI engineering skills and intangibles that could be used to weaponize semiconductors.

In the interim, the following KYP due diligence checklist could be helpful to government agencies and the private sector, keeping in mind that the checklist only serves a useful purpose if combined with:

- Know-Your-Customer (KYC) vetting;

- End-user/end-use vetting

- Apply due diligence during the entire life-cycle of a semiconductor, especially when software/AI upgrades or changes are made.

Appendix A: Know-Your-Product (KYP) Due Diligence Checklist

Applicable for High-Performance Integrated Circuits (ICs), GaN/SiC Power Electronics, and AI Accelerators.

1. Technical Capability Thresholds (ECCN 3A090/4A090 Audit)

Before assessing the customer, the exporter must certify the "Strategic Footprint" of the hardware:

TPP Verification: Does the item's Total Processing Performance exceed 4,800? (If >21,000, verify non-D:5 destination).

Performance Density: Is the performance density ≥ 5.92?

DRAM Bandwidth: Is the aggregate DRAM bandwidth $> 6,500$ GB/s?

Interconnect Audit: Does the chip include proprietary low-latency interconnects (e.g., NVLink-equivalent) that enable "virtual clustering" or "shadow supercomputing"?

Hardware "Kill-Switch" Verification: Does the firmware include immutable on-chip tracking or remote-disable features?

2. Software & Orchestration Elasticity

Firmware Analysis: Can the firmware be field-upgraded to bypass native TPP limits?

Compiler Compatibility: Are the associated compilers/SDKs (e.g., CUDA-equivalent) capable of task-specific "uplift" for cryptographic or targeting workloads?

Digital Twin Risk: Does the sales agreement include cloud-based "optimization services" that create a digital replica of the user's manufacturing or operational environment?

3. Supply Chain "Health" (BIS 2026 Requirement)

For exports to Country Group D:5 (including China), the exporter must now certify:

Domestic Supply Reserve: Verified that aggregate shipments to China do not exceed 50% of total product shipped to U.S. customers for U.S. end-use.

Foundry Capacity Impact: Certified that the production of these units will not divert foundry capacity (e.g., TSMC/Intel nodes) from U.S. national security requirements.

Third-Party Testing: Has the shipment been verified by a U.S.-based testing lab to confirm technical specs match the license application?

4. End-User Compliance Verification

KYC Security Procedures: Has the customer provided written proof of their internal "Restricted Party Screening" (RPS) protocols?

AI-as-a-Service (AIaaS) Clause: If the customer provides cloud computing, have they signed the "No Prohibited Remote Access" commitment for their model weights?

Physical Security Audit: Documented the physical security measures of the ultimate consignee to prevent hardware theft or unauthorized reverse engineering.

Conflict of Interests

The authors have no conflict of interests with any aspect discussed in this article.

Funding

No funding from any party supported the research or the drafting of this text.

References

[1] With EU Council Decision 359/2011 applied in April 2011 Human Rights Sanctions with a "prohibition on the export, sale, or supply of equipment which might be used for internal repression", that were followed in 2012 with EU Council Decision 2012/168/CFSP and Council Regulation 264/2012 that prohibited exports of telecommunications monitoring and interception equipment, along with related technical assistance, and financing for such technologies.

[2] The first sanctions on electronics and semiconductor were imposed by the US government in April 2012 with the U.S. Executive Order 13606 to "target hardware and software used for surveillance, monitoring, and censorship of the Iranian people".

[3] EU Council Regulation 833/2014 and EU Council Decision 2014/512/CFSP, and U.S. President's Executive Orders 13661 and 13662, but they were preceded by UN sanctions resolution 1718 on North Korea, and resolution 1737 on Iran, both adopted in 2006, whose embargoed military supplies and related dual use technologies automatically included military applications of semiconductor technologies.

[4] RAYPCB: IPC 4203B-2018: Standard for Cover and Bonding Materials in Flexible Printed Circuits; Military and Defense Applications p 7. https://www.raypcb.com/author/admin/page/7/#:~:text=GaN%20radar%20technology%20has%20become,active%20electronically%20scanned%20arrays%20(AESAs).

[5] Utilitarian Technology: GaN vs GaAs: Why Both Still Power the Defense RF World; September 8, 2025, https://utilitarian.technology/2025/09/08/gan-vs-gaas-why-both-still-power-the-defense-rf-world/

[6] RAYPCB: GaAs Vs. GaN Radar: What is the Difference; https://www.raypcb.com/gaa-vs-gan-radar/

[7] SailDrone: Integrating USVs & AI into an Operational Maritime Environment; 2021-2023 US Department of Defense (DoD)

[8] Integrating USVs & AI into an Operational Maritime Environment -- The US Navy's 5th Fleet and its regional partners created a network of unmanned systems, networks, and AI tools to detect abnormal maritime behaviors and cue manned ships to respond; Saildrone 2023 (https://www.saildrone.com/missions/task-force-59-unmanned-integration#:~:text=Human%20operators%20cannot%20pick%20out,behaviors%20and%20cue%20manned%20ships)

[9] Arun Seraphin, Emerging Technology Horizons: AI, Quantum and Naval Warfare's Future;

[10] National Defense, NDIAS's Business and Technology Magazine, October 2025

[11] Rossetti Livio, Manned-Unmanned Teaming; Joint Air Power Competence Centre, January 2020

[12] COCOM was established in 1949 as an informal agreement among NATO members, excluding Iceland and Spain, plus Japan and later others to coordinate the control of exports to the Soviet Union, Warsaw Pact countries, and China.

[13] Updated Consolidated Trigger List, as agreed to by the Zangger Committee on November 28th; 2023; Link: English

[14] Link to NSG Control Lists and guidance documents: https://nuclearsuppliersgroup.org/en/

[15] Link to Australia Group Common Control Lists and guidance documents: https://www.dfat.gov.au/publications/minisite/theaustraliagroupnet/site/en/controllists.html

[16] Link to the Missile Technology Control Lists and MTCR Annex Handbook: https://www.mtcr.info/en/mtcr-annex

[17] Link to the Wassenaar Arrangement lists of dual use goods and technologies and munitions list: https://www.wassenaar.org/control-lists-previous-years/

[18] Statement by Executive Vice-President Dombrovskis at the EU Foreign Affairs Council (Trade) press conference 30 May 2024.

[19] On 8 September 2025, the European Commission adopted a Delegated Regulation updating the EU dual-use export control list in Annex I of Regulation (EU) 2021/821. The new EU control list provides for the addition of new dual-use items, including: controls related to quantum technology (e.g. quantum computers, electronic components designed to work at cryogenic temperatures, parametric signal amplifiers, cryogenic cooling systems, cryogenic wafer probers); semiconductor manufacturing and testing equipment and materials (e.g. Atomic Layer Deposition equipment, equipment and materials for epitaxial deposition, lithography equipment, Extreme Ultra-Violet pellicles, masks and reticles, Scanning Electron Microscope equipment, etching equipment); Advanced computing integrated circuits and electronic assemblies such as Field Programmable Logic Devices and Systems

[20] Final reports of the Panel of Experts on Yemen; United Nations Security Council Report S/2020/326, p. 25 ff, and S/2021/79, Annex 20; S/2024/731, Annex 37

[21] Brian Kot, Hong Kong's Technology Lifeline to Russia, Carnegie Endowment for International Peace, May 2023, p.1

[22] U.S. sanctions prohibitions banned the provision of certain information technology, cloud services, and related software to Russia under Executive Order 14071 that came into force in September 2024. These EU and U.S. measures were designed to degrade Iran's and Russia's repression of civilians and military activity.

[23] Baikal Electronics: Die Hälfte der russischen Prozessoren ist defekt, Johannes Hiltscher, Golem.de April 2024

[24] Parts of the Problem: Tracing Western Tech in Russia's Deadliest Jets, International Partnership for Human Rights (IPHR), The Independent Anti-Corruption Commission (NAKO) and Hunterbrook Media; 2025

[25] Iran sends Russia hundreds of ballistic missiles, Parisa Hafezi, John Irish, Tom Balmforth and Jonathan Landay; Reuters; February 21, 2024. See also a series of field dispatches by Conflict Armament Research, including Documenting a North Korean missile in Ukraine; CAR Ukraine Field Dispatch, January 2024; or North Korean missile relies on recent electronic components, CAR Ukraine Field Dispatch, February 2024.

[26] Ukrainian cities 'terrorised' by North Korean weapons in Russian hands; Justin McCurry, Reuters; 30 May 2025.

[27] The Illicit Flow of Technology to Russia Goes Through This Hong Kong Address, New York Times; July 2024

[28] Treasury Takes Aim at Third-Country Sanctions Evaders and Russian Producers Supporting Russia's Military Industrial Base, Press Release of the U.S. Department of the Treasury; October 2024

[29] See for example https://www.getfactorysense.com/resources/understanding-rfid-tracking-what-is-it-and-how-does-it-work

[30] Onni Aarne, Tim Fist, and Caleb Withers; Secure, Governable Chips -- Using On-Chip Mechanisms to Manage National Security Risks from AI & Advanced Computing; Center for a New American Security; January 2024