EMERGING DUAL-USE TECHNOLOGIES AND GLOBAL SUPPLY CHAIN COMPLIANCE

F. SEVINI
European Commission Joint Research Centre
Ispra, Italy
Email: Filippo.sevini@ec.europa.eu

C. CHARATSIS, X. ARNES NOVAU, E. STRINGA, J. BARRERO, A.S. LEQUARRE, P. COLPO, D. GILLILAND, W. JANSSENS
European Commission Joint Research Centre
Ispra, Italy

Q. MICHEL
ULG Liege university
Liege, Belgium
Email: qmichel@ulg.ac.be

Abstract

With the progress of technologies for telecommunication, synthetic biology, chemistry, additive manufacturing and nanoscale processes, many opportunities arise, allowing more effective and innovative production and the achievement of results with great potential both on the technical and commercial sides.

At the same time however, rapid technological developments may create opportunities and vulnerabilities that can be exploited for illicit procurement activities seeking sensitive items for proliferation programmes.

The strategic trade control framework should evolve with the same pace. Enforcement and traceability of intangible technology transfer controls may become much more challenging, while at the same time improved approaches to internal compliance must be developed by suppliers and technology holders.

1. INTRODUCTION

The history of nuclear, chemical, biological, missile-related proliferation has shown how the piecemeal illicit procurement of dual-use strategic goods and technologies, rather than of turn-key facilities, has become a key concern in the development of competences and capabilities for the development of weapons of mass destruction, particularly since the 80’s and 90’s.

In a broader context, strategic, or "dual-use", are items with both civil and military applications, including systems, equipment, components, materials, software and technologies for manufacturing, aerospace, electronics, chemical, biological and medical, nuclear, telecommunications, cyber-security, marine, navigation, avionics, laser applications, energy production, human rights protection and many other applications.

A complex system of export controls, safeguards and physical protection has been put in place to address nuclear proliferation. Separate ones, with their legal framework and technical aspects, address chemical, biological and missile technology, and more broadly dual-use strategic trade controls.

The evolution of technologies and processes allows discovering new areas and opportunities, but may also bring about more challenges to the non-proliferation framework, which therefore needs to adjust and evolve to address them, while safeguarding research and legally authorised trade and exchanges. The IAEA is paying a lot of attention to the matter as summarised in the "Emerging Technologies Workshop Trends and Implications for Safeguards" held in 2017.

With the evolution of techniques and methods, as well as the globalisation of the supply chain, continuously new challenges are posed to stake-holders, national authorities and also the international legal framework. Classical controls may be bypassed, or become obsolete, by applying new approaches as those offered e.g. by additive manufacturing or nanotechnologies.

Illicit trade's proliferation financing and the means used by illicit financing networks may also benefit from the evolution of technologies and cryptography enabling them to bypass more efficiently the processes and

traceability of classical banking system. At the same time, blockchain and distributed ledgers could greatly facilitate the global supply chain.

The following sections address some of the most interesting evolutions in various areas examining their proliferation potential and export control challenges.

2. NANO-TECHNOLOGY

Nanotechnology, commonly defined as "the design, characterisation, production and application of materials, devices and system by controlling shape and size at the nanoscale level'' has the potential to revolutionize many technological and industrial sectors. On the nanoscale, materials exhibit a very high surface reactivity thanks to their very large surface area to volume ratio resulting in high percentages of atoms exposed at their surface that confer unique properties such as catalytic, thermal, electrical and mechanical and optical properties which are not present in their bulk form are observed.

These unique properties are bringing numerous new advances and innovations in many domains of applications such as informatics and telecommunications, automotive industries, environment and healthcare and more [1]:

- Information communication, digitalisation: development of more powerful and smaller computers and electronic devices thanks to the use of transistors and integrated circuits based on semiconductor nanowires.
- Healthcare: more sensitive medical diagnostic tools, more efficient medical devices and drug delivery systems to fight against serious diseases.
- Lightweight vehicle, improved vehicle fuel efficiency, reduction of vehicle pollutant emissions by using nano-filters.
- Mechanical and electronic applications, cosmetic and food quality: Improved material properties using nanofibers, carbon nanotubes, nanostructures and nanoparticles.
- Advanced filtering systems using graphene based filters for water quality and water re-use. Nanostructured surfaces based devices for water harvesting in arid regions.
- Wearable nanosensors for emergency preparedness, biosecurity, healthcare applications.
- Healthier foods using nanostructured salt which permits lower salt content without reducing taste.
- Anti-fraud labelling or identification of goods or currency by using nanoparticles.

Military based applications benefit as well from nanotechnology technology development. For instance, (nano-) technologies previously listed can be used to improve medical care for soldiers, to produce lightweight and resistant vehicles and smart materials for developing protective equipment and devices for early detection of chemical biological and explosives threats. Nanomaterials have as well a high potential to enhance radio frequency and microwave absorbing material properties for civil and military aerospace applications to make airplanes or other transport means near-invisible to radar detection [2].

Nevertheless, the misuse of some of the nanotechnologies by terrorism and criminal organisations is a real concern. For instance, potentially toxic nanoparticles [3] can be used intentionally as toxic compounds in water distribution systems or even in humans for poisoning purpose. Many technologies developed for defence could potentially be used for in support of illegal activities e.g. smuggling using aircraft and ships made undetectable through the use of radar absorbing materials.

The pace of innovation of nanotechnology, supported by the constant increases of publications in scientific journals must be considered with attention since publications provide a considerable source of information for the potential proliferation of dual use technologies.

Whereas, most of categories of products and technologies are already listed in Annex I to Regulation 428/2009 as amended [4] which includes the Wassenaar Arrangement, the Missile Technology Control Regime (MTCR), the Nuclear Suppliers' Group (NSG), the Australia Group and the Chemical Weapons Convention (CWC), no clear mentions are made on nanotechnology based items that would outperform standard ones.

While large worldwide investments in nanotechnology are made for the development and commercialization of safe nanotech-based products and technologies, regulation and ethical issues must be addressed to prevent their malicious uses.

3. ADDITIVE MANUFACTURING

Additive manufacturing (AM), known also as 3D printing, is considered a disruptive technology with high potential to boost productivity and efficiency across many industrial sectors and hence receives attention as a strategic enabling technology e.g. in the EU Industrial Policy Communication (COM(2014) 14 final) and Horizon 2020 programme as it provides basis for innovation. The broad-based deployment of AM might have a broad impact and can transform the industry concept and value chain (manufacturing on demand and on spot, reducing transport needs and minimizing raw material storage and waste production).

Ideally AM allows the construction of any shaped part/object/product starting with its digital model design, followed by the conversion into a build file, a successive printing process - deposition of layer after layer the selected material/s- and a concluding finishing step leading to the creation of the desired 3D functional product. AM is an umbrella term covering seven process categories (ISO/ASTM52900-15): material extrusion, powder bed fusion, vat photo-polymerization, material jetting, binder jetting, sheet lamination and direct energy deposition. The selection of the material/s depends on the nature and functionality of the 3D printed component or end-use object, thus metals and alloys, ceramics, glass, (bio)polymers and cells are among current materials used for AM and 3D-bioprinting.

AM is increasingly gaining applications in a variety of sectors notably: aerospace and automotive (e.g. production of new parts such as fuel nozzle and valves); machinery and tools (e.g.low cost robot arms, heat exchangers); electronics (conductive plastic filaments, wearable sensors); pharma (e.g. printed tissue and organoids for drug testing) and medical technologies (e.g. customized implants and prosthetics, tissue engineering for regenerative medicine, 3D-printed models for surgical education and training). Military applications may overlap also with those of the above mentioned sectors (e.g. simplification of logistics, manufacturing spare parts and/or repair on spot, cure burn injuries). However, while there are great advantages that 3D-printing can bring, to accelerate the market update of AM, aspects including standardisation, costs, skills, intellectual property rights, ethics, liability as well as qualification and certification procedures should be considered for each specific sectorial application.

3D-printing is being broadly spread, both geographically and socially, by the Maker Movement and Fabrication Labs (FABLABS). The Maker movement match modern relatively inexpensive digital manufacturing tools with a Do It Yourself (DIY) mentality underpinning the "personal manufacturing" with employment of online tools, open source databases and 3-D printing. The availability of the tools and knowledge of manufacturing production to the global user community can create some threats, e.g. weapons and arm manufacturing could become easier, metal or plastic malfunctioning parts of strategic instrumentation could be printed in untraceably manner; 3D models can help better understanding of the structure and functioning of critical instrumentation.

The possibility to make 3D printed guns at home is a reality behind current US gun control debate and discussions on whether the emergence of 3D-printed plastic guns (and public available digital files to produce them) presents an immediate safety threat for the community as these firearms can be untraceable. The legal debate on "wiki guns" both from the perspective of gun control as well as from access to data and information online, is attracting public attention and exemplifies well some potential concerns and the complexity for controls. Brockmann and Kelly [5] have recently reported on AM key proliferation challenges (small arms and light weapons, missiles, nuclear weapons, centrifuges for nuclear enrichment) as well as on potential controls and national plans and key challenges in applying export controls to AM. Similarly Bromley and Maletta [6] have recently described the challenge of software and technology transfers to non-proliferation efforts. Specific roles and concerns of the use and misuse of the most recent 3D bioprinting technology as well as the evolving trends should be fully addressed e.g. in biodefence and bioterrorism field.

4. SYNTHETIC BIOLOGY

Synthetic biology gathers the design and construction of new biological parts, new systems or even new organisms with predictable and reliable functional behaviour that do not exist in nature or the re-design of existing, natural biological systems for useful purpose. A set of methods was developed to that aim such as the creation of standardized genetic parts, DNA assembly methods and rationally designed genetic circuits with rapid testing. Exponential improvements in DNA sequencing with the characterization of many organisms provide crucial raw material and bioengineering is accelerated by central developments such as high fidelity large genome synthesis,

genome editing with performing tools such as CRISPR/Cas9 and liquid- handling robot high-throughput characterization platforms [7].

Newly built microorganisms can produce nearly any desired chemical. Bacteria, fungi or yeasts were first designed to produce enzymes to transform natural products in bio-industries (paper mill, food processing or waste agricultural residues factories) and in detergent making, textile and pharmaceuticals companies. Engineered proteins have advantages over natural ones due to lower cost, high production rate, availability, stability, and diversity. They can also be used for ecological purpose such as the treatment of industrial effluents with hazardous chemicals (textile dyes, phenols and other xenobiotics).

Synthetic systems have progressively evolved from simple transcriptional regulatory networks in prokaryotes to complex multimodal biological circuits in mammalian systems both in vitro and in vivo. Recent advances promise a new generation of gene and engineered-cell therapies based on sophisticated methods (e.g. engineered transplanted cells detecting cancer or maintaining insulin homeostasis) [8]. These prospects are strong economic drivers for a rapid growth and spread of synthetic biology approaches.

Regarding dual-use concerns the manipulation of biological functions, systems, or microorganisms may lead to the production of a disease-causing agent or a toxin threatening not only human health but also agricultural or environmental targets. Opiate, a controlled narcotic, is now efficiently produced by yeasts and systems for other potentially problematic compounds will certainly follow.

The biological production of traditional chemical weapon agents should be hampered by their biocidal activity making precursors more likely targets. Modifying a pathogen to facilitate its spread through a population, introducing antibiotic resistance into an infectious microorganism, or deliberately weakening someone's immune system are examples of the potential malicious uses of synthetic biology.

Recent publications about the sequence requested for the transmission of the deadly bird-flu virus H5N1 to mammals [9] or the synthesis of the horsepox virus, a relative of smallpox, from genetic pieces ordered by mail have raised worrying questions about misuse and generated a debate on the applicability of export controls.

Additionally the emerging of do-it-yourself (DIY) biology communities and of the student iGEM competition can speed up the access to the necessary tools. These elements argue for the development of a robust international regulation and surveillance of rapidly evolving biotechnologies [10], [11].

5. CHEMICAL ITEMS

Among Weapons of Mass Destruction (WMD), nuclear weapons cause the largest amount of destruction, but there is a little likelihood of being used. However, Chemical Weapons (CW) are the ones which raise more concern due to their use evidenced by recent events like the chemical attacks in the Syrian civil war, the assassination of Kim Jong-nam by a nerve agent called VX at the Kuala Lumpur airport, and finally, the Skripal affair in Salisbury (UK) where a Novichok agent was used.

The International Export Controls Regimes for Dual-use items aim at mitigating as much as possible the proliferation of WMD and in particular the Organization for the Prohibition of Chemical Weapons (OPCW) and the Australia Group (AG) prohibit the manufacture, storage and use of CW, but also restrict the supply of certain chemical precursors and processing equipment.

The Chemical Weapons Convention (CWC) entered into force in 1997 and currently has 193 states-parties [12]. One state has signed but not ratified it (Israel) and three states have neither signed nor ratified (Egypt, North Korea, and South Sudan). The AG was established in 1985 as a response to the massive chemical weapons use in the Iran-Iraq war, and consists of states which have an interest in harmonising export controls to prevent the use of Dual-use goods in chemical and biological weapons programmes.

Since the war in Syria began in 2011, chemical weapons have been used indiscriminately against civilian population, causing hundreds of deaths and injuries due to the exposure to these toxic chemicals, such as Chlorine (choking agent), Sarin (nerve agent) or sulphur mustard (blister agent), all of them included in the list of CW by the OPCW. Despite the inclusion of these chemicals to the OPCW list, the evidence of several chemical attacks perpetrated in Syria sustain that Chemical Weapons continue to be used.

Most of the episodes linked to the use of CW which have occurred over the last year in Syria, have been reported after the outcome of the official Joint Investigative Mechanism (JIM) carried out by OPCW inspectors:

— Unclear, still under investigation (7 April 2018, Douma, Syria)

— Chlorine (4 February 2018, Saraqib, Syria) [13]
— Sarin (4 April 2017, Khan Sheykoun, Syria)[14]
— Sarin (30 March 2017, Al-Lataminah, Syria) [15]
— Chlorine (24 March 2017, Al-Lataminah, Syria) [16]

In 2017 another event related to the use of chemical weapons occurred: the assassination of Kim Jong-nam (the half-brother of the current President of DPRK Kim Jong-un), at Kuala Lumpur Airport in Malaysia. Kim Jong-nam was attacked by two women who splashed a liquid on his face which contained a nerve agent called VX, and as a consequence he died in the ambulance on the way to hospital.

Last but not least, another shocking event occurred in Salisbury (UK), when a former Russian military intelligence officer called Sergei Skripal was victim of a chemical attack by a toxic chemical. After different independent investigations (UK officers but also OPCW inspectors), it was conclude that the alleged nerve agent used belonged to a family of compounds called Novichok, whose existence was known but had never been used up to then. Novichok agents were developed in the former Soviet Union in the 1970s hidden under a secret program of research on defoliant agents [17] conducted by the Russian research institute GOSNIIOKhT [18]. In terms of toxicity, it is reported that Novichok is around 5-10 times more lethal than the well-known VX agent, according to the information provided by a Russian chemist who worked in the Novichok program. Besides the toxicity, another significant feature of Novichok is the capability of being used as binary weapon, which suppose an extra bonus for the proliferators. A binary weapon consists of two substances (precursors) that must be combined in order to trigger their lethal effects by the generation of the CW in situ, thereby improving two important features with respect to the classic CW:

- Improve safety: the precursors are not lethal, so easier to handle and to transport.
- Avoid controls: since the precursors are not included in any Export Control list or Regulation.

The main concern about Novichok agents is not only their powerful toxicity, but also the fact that most of their chemical precursors are not currently included in the Export Control lists. This might generate new opportunities for the proliferators, despite the lack of technical information available to exporters and common people.

6. NUCLEAR TECHNOLOGY

The Generation IV Forum identifies six new reactor concepts that could better help meeting the world's future energy needs using fuel more efficiently, reducing waste, being economically competitive and respecting high standards of safety and proliferation resistance. The concepts more advanced towards the near-term demonstration are the Sodium Fast Cooled and the Very High Temperature Gas reactors. Another concept expected in 2020's is the Lead-cooled Fast reactor [19].

A recent development is the new floating reactor developed in Russia. The first prototype *Akademik Lomonosov* is loaded on a barge and hosts two pressurised water reactors for a total of 70 megawatts of electricity. Mobility is its primary technical novelty, of course not new in the history of nuclear naval developments. But the nuclear reactor is deputed to output electricity ashore and not for the propulsion of the ship itself. The advent of this type of reactors has a great potential for the supply of electricity to remote areas, but also brings about different perspective for what concerns "exporting" turn-key nuclear reactors, which could be towed away and moved to different locations, save of course the fulfilment of export controls and international safeguards obligations.

For what concerns reprocessing, the most widely used technique remains the aqueous PUREX process, so far applied to about one third of the total used fuel discharged from all commercial power reactors. The total annual reprocessing civil capacity is about 5300 tonnes, with La Hague in France at 1700 tonnes/year and Sellafied in UK respectively at 600 tonnes/year of LWR fuel and 1500 tonnes/year of Magnox Fuel [20]. Aqueous reprocessing allows separate extraction of fissile isotopes from spent fuel, reducing long-lived waste and allowing the fabrication of MOX fuel. The separation of plutonium has of course proliferation risks, reason why some countries do not reprocess civil fuel.

Pyroprocessing has also an important potential for reprocessing without separating uranium, plutonium and minor actinides. Its technical feasibility has been proven by the Argonne national lab in the US. South Korea

has built in collaboration with the US a pilot facility called PRIDE which entered in operation in 2012 with the purpose of studying its relevance as waste management option. A full-fledged pyro-reprocessing is currently prohibited by the U.S.-ROK 123 Agreement, as well as enrichment. From an export control perspective, pyroprocessing is not explicitly mentioned by the Nuclear Suppliers Group guidelines, which report only PUREX.

Striving for nuclear waste reduction, transmutation of long-lived radioactive waste can be carried out in an accelerator-driven system (ADS), where neutrons produced by protons spallation are captured by heavy isotopes contained in the waste blanket along with fissionable fuel and undergo fission. A number of research facilities exist which explore ADS based transmutation, e.g. SCK-CEN in Belgium is building MYRRHA (Multipurpose Hybrid Research Reactor for High-tech Applications). ADSs could also be used to breed thorium 232 into fissile U-233, using lead bismuth molten salt as spallation target and coolant. This concept is explored e.g. by India [21].

As for enrichment, progresses are made in gas-centrifuge designs but the related information is confidential and sensitive. Among other techniques, the interest for commercial application of laser-based isotope separation seems to have lost steam with the slowing down of the SILEX program following the exit of GE-Hitachi. A pilot test loop has been built in North Carolina in 2012, but the plans for the construction of a laser enrichment plant at Paducah are idle due to the decrease in demand of enriched uranium following the Fukushima accident [22].

Thermonuclear fusion continues to be pursued by large investments and efforts. The ITER reactor is being built in Cadarache France by a large international consortium where the EU has a predominant part. The tokamak concept has been studied since the 60's when it had been developed by the Russian Kurchatov institute. Important milestones have been reached over the decades but a lot of work and investments are still needed. Recently, an important success was achieved by the Weldenstein 7-X Stellarator, which is a competing concept adopting twisted magnets around the same shape as a tokamak. The two designs are expected to bring important results towards the achievement of power breakeven and related technologies. Research is on-going also on inertial confinement fusion, relying on high power lasers. Fusions machines are explicitly excluded from the scope of NSG's controls, nevertheless they employ various types of special materials (structural ones like carbon fibres; radioactive isotopes like tritium), electronics, lasers and related dual-use technologies, listed or non-listed, that require export authorisations. Large international projects like ITER have important spin-offs and extended consortia involving many sub-contractors, research institutes and universities involved. They are therefore important vehicles for the diffusion of knowledge and intangible technology transfers that must be made aware of export controls and informed by authorities.

7. CYBERSURVEILLANCE AND CRYPTOGRAPHY

The rapid expansion of information digitalization and internet communications that took place in the last two decades is having a positive impact in in our society facilitating social, economic and cultural life. On the other side, this expansion represent a threat for the society as it is relatively easy to intercept, capture and disseminate sensitive information related to organizations, individuals or companies. Advanced cryptographic techniques allow protecting data and communication from unauthorized diffusion, but, at the same time, represent a means for hiding data and communication regarding illicit trafficking or terroristic plans.

7.1. Cybersurveillance tools

Storage and communications systems can be violated by cybersurveillance tool, that have been developed to permit communication providers to fulfil legal requirements. Examples of cybersurveillance tools, systems or components are:

- Internet Protocol (IP) network monitoring systems: systems able to monitor a computer network logging all captured data into a database and enabling a subsequent search and analysis of the data (packets)
- telephone (both cabled and mobile) interception equipment: systems for the extraction of the content of the communication (voice or data), subscriber identifiers or other transmitted metadata
- intrusion software (software that silently run a program in electronic device like computers or smartphone and/or extract data from them)
- data retention systems (systems that continually collect data for compliance or business purposes)

The systems reported above have a dual use nature as they can be used to comply with legal requirements but they become dangerous if misused by criminal organizations or by dictatorial regimes.

- IP monitoring systems are used by administrators to monitor the status of a network but they clearly can be seen as mass surveillance systems
- Telephone interception equipment and intrusion software can be legally used by authorities to find evidences of a crime
- Data retention systems are used to comply with legal requirements, e.g. the European Data Retention Directive (2006) that foresees that any public electronic communication operator capture most of communication information (including location) and store them for a period from 6 months up to two years; stored data can be misused

Several of the sensitive items mentioned above are listed by Wassenaar Arrangement's guidelines and hence also by EC Reg. 429/2009's Annex I as amended. However their technical parameters continuously evolve and attention should be paid to impose catch-all controls.

7.2. Cryptography

Cryptography is a method of storing and transmitting data in a particular form so that only those for whom they are intended can read and process. Basically, cryptography is the process of converting ordinary plain text into unintelligible text and vice-versa is used in any application where there is the need to protect data and communications.

Like cybersurveillance, also cryptography has a 'dual use' nature as it can be used for illicit activities. Sophisticated and robust cryptographic can be hardly intercepted and this can be an issue when police authorities needs to intercept communications or access data of terrorists or criminal organizations developing dangerous operations or illicit trafficking. There are different cryptographic techniques like symmetric-key cryptography and public-key cryptography, quantum and post quantum cryptography [23, 24].

The most innovative and emerging cryptographic technologies are represented by quantum [25] and post quantum [26] cryptography. Quantum cryptography uses quantum mechanical properties to carry out cryptographic tasks. An example of quantum cryptography is represented by Quantum Key Distribution (QKD) that enables two parties to produce a shared random key, known only to them, to encrypt and decrypt data.

Post quantum cryptography is based on mathematical algorithms that cannot be broken by quantum computers. The unauthorized decryption of data encoded with quantum and post quantum algorithms can be done using a brute-force search; anyway the process presents high complexity and, especially for post quantum technology, the computational power of computing systems is no yet mature to accomplish the task. This makes quantum and post quantum cryptography very dangerous if used for illicit purposes, like hiding the content of communications related to illicit traffics or operations.

Export controls have been introduced relatively to systems using symmetric and asymmetric key and quantum cryptography. However, post quantum cryptography is an emerging technique that has no export limitations but it could represent a serious danger as currently the computational power of existing processors is not yet sufficient to decrypt encoded data with this technique.

8. EXPORT COMPLIANCE IN THE GLOBAL SUPPLY CHAIN

Trade has a transformative impact given the significant transfers of funds, expertise and technologies it entails and the rapidity of transactions and the extensiveness of geographical scope it includes. At a time when economic activities have an increasingly transboundary character, exporters are eager to seize opportunities for reducing production costs by outsourcing non-core activities.

Technologies such as those mentioned above are already changing or bear a great potential to facilitate and change our way of living. However, not being yet subject to export controls, they may already pose also threats in terms of security and non-proliferation. Even more along complex supply chains involving actors including several actors (suppliers, clients, brokers, shippers, sub-contractors, banks, research, consultancy and others). Certain emerging technologies may also provide opportunities with regards to export compliance. Modern

approaches like Distributed Ledger and Blockchain could facilitate the logistics and document access all along the supply chain thus improving the processes and speeding up shipments across the controls [27]. However, these new tools could also bear some challenges such as data integrity and access controls that need to be taken into account when assessing their potential contribution.

Also the use of cryptocurrencies can have a great potential, but also create opportunities for illicit transactions [28]. It is against this background of rapid technological development and intense economic and scientific exchanges that exporters need to find efficient ways to comply with trade control laws. Industry is considered by authorities as "the first line of defence" since exporters are often times better positioned to identify sensitivities at an early stage of their Research and Development activities [29]. This is particularly valid for both firms and research organisations and universities who are in the forefront of new developments in cutting-edge technologies.

Export compliance is a two way process and it is within the remit of public authorities to promote an engaging and trusted relationship with the exporters and this can follow through an effective outreach strategy and open contacts and communication with the exporters [30]. Industry can apply due diligence procedures and develop Internal Compliance Programmes (ICPs) as one of the most effective ways in addressing proliferation risks and ethical sensitivities, also besides those foreseen in the law.

With this in mind, it is not strange that some exporters undertake voluntary additional commitments [31]. Suppliers know the technical parameters of their products and technologies including possible applications and they can therefore, identify suspicious orders and requests by applying risk assessment procedures prior to making a deal and agreeing to provide their services and products. A compliant exporter shall consider all actors involved in an organisation's supply chain as an integral part of this organisation [32]. In that regard, often times, it is thanks to already aware and compliant "exporters" of the supply chain that unware actors start realising and addressing obligations set in the export control law [33].

Increased and smarter awareness is a key to a successful control of possible sensitivities, save the need to not unduly hinder research and development, as well as licit trade. This is particularly important in the case of non-listed items either below control specifications or, completely out of the controls' scope, which might require an export license under the "catch-all clause" when exporters are informed or aware that their new developments could be sensitive.

9. CONCLUSIONS

The paper reviews the sensitive technologies with the most interesting evolutions and associated proliferation potential trying to be as comprehensive as possible, while not claiming to cover all possible relevant technologies, nor the completeness of the information available.

With the rapid evolution of techniques and methods, as well as the globalisation of the supply chain, new challenges are continuously posed to stake-holders, national authorities and also the international legal framework. Export controls may be bypassed, or become obsolete, by applying new approaches such as those offered e.g. by additive manufacturing or nanotechnologies.

Increased and smarter awareness is a key to a successful control of possible sensitivities, save the need to not unduly hinder research and development, as well as licit trade.

In particular, the role of research both in the development and compliance aspects is extremely important to foster due diligence in international collaboration controlling Intangible Transfers of Technologies.

Emerging technologies are generally not yet export controlled because deemed not mature by the international export control regimes, which may consider them anyway in watch-lists. While the "catch-all clause" may represent a useful instrument for assessing on a case by case basis particularly sensitive transfers of mot-listed emerging technologies, a continuous dialogue between authorities and suppliers, with incentives to defend their market and reputation, is extremely important to a successful outcome.

REFERENCES

1. Roco, C. M., Hersam, C. M., Mirkin, A. C., Nanotechnology Research Directions for Societal Needs in 2020**,** Springer, Dordrecht (2011), available in: 10.1007/978-94-007-1168-6.
2. Kumar et al, RSC Adv.**,** 2015,5, 20256-20264

3. Saura, C.S., Wallace, A. H., Toxicity of nanomaterials found in human environment: a literature review, Toxicology Research and Application (2017), available in: 10.1177/2397847317726352.
4. The latest version of Annex I was published as Commission Delegated Regulation (EU) No 2268/2017.
5. Brockmann K., Kelly, R., The challenge of emerging technologies to non-proliferation efforts. Controlling Additive Manufacturing and Intangible Transfers of Technology, SIPRI, 2018.
6. Bromley, M., and Maletta, G., (2018) The challenge of software and technology transfers to non-proliferation efforts. Implementing and complying export controls. SIPRI, 2018.
7. Kelwick R., MacDonald, J.T., Webb, A.J., Freemont P., Developments in the tools and methodologies of synthetic biology. Front Bioeng Biotechnol. 2014. 2:60, available in: doi: 10.3389/fbioe.2014.00060.
8. Bueso, F.Y., Lehouritis, P., Tangney, M., In situ biomolecule production by bacteria; a synthetic biology approach to medicine, M. J Control Release (2018). 275:217-228. doi: 10.1016/j.jconrel.2018.02.023.
9. Charatsis, C., Setting the publication of "dual-use research" under the export authorisation process: The H5N1 case, Strategic Trade Review – Issue 1 (2015) 56-72, available in: https://strategictraderesearch.org/wp-content/uploads/2017/11/STR_01.pdf.
10. Synthetic Biology: Latest developments, biosafety considerations and regulatory challenges. Biosafety and Biotechnology Unit. ISP-WIV. Brussels, 2012, available in: https://www.biosafety.be/sites/default/files/120911_doc_synbio_sbb_final.pdf.
11. Preparing for Future Products of Biotechnology. National Academies of Sciences, Engineering, and Medicine. 2017. The National Academies Press. Washington, DC. doi:10.17226/24605.
12. Status of the CWC, https://treaties.un.org/doc/Publication/MTDSG/Volume%20II/Chapter%20XXVI/XXVI-3.en.pdf.
13. Fact-Finding Mission (FFM) No. S/1626/2018, OPCW, 15 May 2018.
14. Fact-Finding Mission (FFM) No. S/1497/2017, OPCW, 12 May 2017.
15. Fact-Finding Mission (FFM) No. S/1548/2017, OPCW, 2 November 2017.
16. Fact-Finding Mission (FFM) No. S/1636/2017, OPCW, 13 June 2018.
17. Mirzayanov, S.V., State Secrets: An insider's Chronicle of the Russian Chemical Weapons Program, Outskirts Press, Inc (2009).
18. State Scientific Research Institute of Organic Chemistry and Technology (GOSNIIOKhT).
19. https://www.gen-4.org
20. http://www.world-nuclear.org, June 2018
21. http://www.world-nuclear.org, April 2017
22. http://www.world-nuclear.org, April 2016
23. Delfs, H., Knebl, H., Introduction to cryptography: principles and applications," Springer (2007). ISBN 9783540492436.
24. Katz, J., Lindell, Y., "Introduction to Modern Cryptography," CRC Press (2007). ISBN 1-58488-551-3.
25. Sharbaf, M.S., "Quantum cryptography: An emerging technology in network security", IEEE, 2011 International Conference on Technologies for Homeland Security (HST), Waltham, MA, USA (2011), available in : 10.1109/THS.2011.6107841.
26. Bernstein, J.D., and Lange, T., " Post-quantum cryptography", Nature Vol 549 (2017) 188–194.
27. For an overview of the role of blockchain theologies in the global supply chain including connecting challenges please see: Blockchain in the supply chain: where are we now?, Trade Security Journal, Issue 8 (2018) 9-11.
28. Tamminen, V., Cryptosanctions: Implications of sanctions regulations n virtual currencies, Strategic Trade Review-Issue 6 (2018) 29-44.
29. Several public debates and export control practitioners are increasingly refer to industry as "the first line of defence". Indicatively the EU Export Control Forum 2017 organised by the European Commission comprised a session entitled as: Industry as the "first line of defence": towards effective company compliance.
30. On the role of public authorities and private sector vis-à-vis export compliance see: Stewart, I., Brewer, J., Engaging the private sector in non-proliferation: reflections from practitioners, Strategic Trade Review- Issue 3 (2016) 143—152.
31. For example, some companies from the ICT sector are accustomed in applying risk assessment procedures when exporting certain technologies (e.g. for mass surveillance) to countries having a record of human rights violations regardless whether such technologies are included on the lists or not. Nokia confirmed such an approach in the EU Export Control Forum in Brussels, 2015.

32. Discussion with Jan Verreth, export compliance officer in Tradecc, December 2017, Belgium.
33. Charatsis, C., Doctoral Thesis: Interferences between non-proliferation and science: 'exporting' dual-use know-how and technology in conformity with security imperatives, 2016, 169-171, available in: 10.2760/26856.