Anticipatory governance of emerging and disruptive technologies with dual-use potential

Georgios Kolliarakis (German Council on Foreign Relations)

Abstract

New technologies, the research, development and innovation (RDI) policies accompanying them, as well as their commercialization and international diffusion patterns, are increasingly under pressure to address sustainability, welfare and resilience of societies. Besides efforts to lever technologies for the SDGs, the global disruption due to the Covid-19 pandemic, and not least the eruption of militarized conflict, highlight the urgency of coordinating national and multilateral policies toward more shock-proof societies in the future. Traditional technology governance strategies and established instruments are facing unprecedented challenges: How to ensure that technological innovations are used to the benefit of societies, without jeopardizing global peace and stability? The current volatile global environment, where technology increasingly becomes an instrument for geo-economic rivalries among major powers, creates major opportunities, but at the same time severe risks for international security and human rights out of the illicit diffusion of critical technologies and their misuse in novel weapons, incl. nuclear, biological, chemical and cyber weapons with mass destruction potential.

World-wide efforts toward “building back better” in the aftermath of the Covid-19 pandemic will intensify the quest for emerging and disruptive technologies (EDTs). Research and Innovation policies, public procurement and marketing strategies, including stakeholder partnerships for transfer and diffusion, need to ensure not only that EDTs will have beneficial and sustainable applications and not further exacerbate inequalities within societies and among regions, but also put safeguards in place to prevent their misuse. Bio-, nano-, and quantum technologies, micro-electronics and semi-conductors, position, navigation and timing technologies, as well as additive manufacturing and artificial-intelligence can be key enablers to welfare, particularly in less privileged parts of the globe. However, such technologies have both civil and military applications, and they bear the risk of accidental or intentional transfer and usage for malicious purposes. This includes, among others, intercepting vital functions of national critical infrastructure, building components for weapons of mass destruction, hybrid warfare, terrorist attacks, and severe violations of human rights.[1]

At the same time, the governance of RDI, especially of EDTs with a broad range of potential applications, is becoming increasingly thorny. The challenge is growing more complex and tricky if we conceive technology not merely in terms of hardware, software, or tools, but also from the perspective of business models, international transfer of necessary know-how, globalized trade flows, institutional set-ups at national and international level, and interference with other policy areas.[2] The above constitute the framework conditions that are questioning the effectiveness of traditional technology governance strategies and established instruments, such as export controls.[3] The current volatile global environment, where technology increasingly becomes an instrument for geo-economic rivalries among major powers, together with the persisting global health, financial, and militarized conflict crises, pose an unprecedented challenge to the simultaneous governance of technology, industrial, trade, and not least security and human rights policies.[4]

[1] Roca, J. B. et al. (2017): When risks cannot be seen: Regulating uncertainty in emerging technologies. In: Research Policy, vol. 46, no. 7, p. 1215-1233; Kanetake, M. (2021): Dual-Use Export Control: Security and Human Rights Challenges to Multilateralism. In: European Yearbook of International Economic Law (EYIEL) 2020 (Springer). Available at: https://ssrn.com/abstract=3792973.

[2] Tucker, J. B. (ed.) (2012): Innovation, Dual Use, and Security. MIT Press; Taeihagh, A. et al. (2021): Assessing the regulatory challenges of emerging disruptive technologies. In: Regulation & Governance, vol. 15, p. 1009-1019.

[3] Michel, Q. et al. (2020): A decade of evolution of dual-use trade control concepts: strengthening or weakening non-proliferation of WMD. European Studies Unit. University of Liege. Available at https://orbi.uliege.be/bitstream/2268/246711/1/full.pdf .

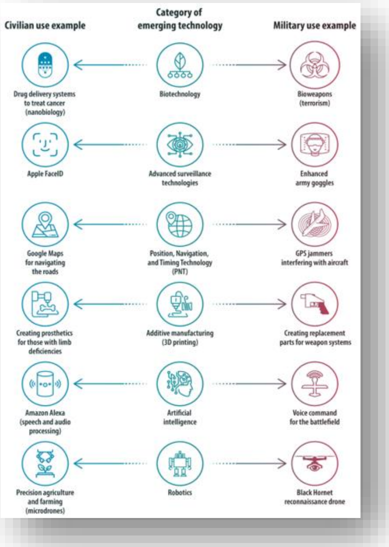
[4] Montgomery, A. H. (2020): Double or Nothing? The Effects of the Diffusion of Dual-Use Enabling Technologies on Strategic Stability. Center for International and Security Studies at Maryland. Available at https://cissm.umd.edu/research-

The Meanings of Dual-Use

Dual use of technology encompasses a number of implications. Most definitions stress the civilian versus the military purposes of usage. This distinction is sometimes extended to include benevolent versus malevolent, and, also illegitimate usages, as in the context of international non-proliferation arms control frameworks.[5] Additionally, in national anti-terrorism and anti-criminal legislation, dual-use encompasses aspects of human and national security. Recently, in the context of the European Union's regulation update (EU 2021/821) setting up an "EU regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items", public security, safeguarding human rights, and counterterrorism measures are taken up, additionally, as reference objectives of dual-use controls.[6] The above nuances in the definitions of dual use, however, may result in different governance approaches, especially when it comes to blurred lines of distinction between civilian and military use.

The table above picks up only a small number of characteristic technologies that find already disruptive usages in both civilian and military domains. For instance, advances in life sciences research, such as in nano-biology, have the potential to provide new and improved ways to support public health at a worldwide scale, targeting communicative and non-communicative diseases, such as cancer. However, the same research can pose severe risks to public health if misused, either inadvertently or deliberately, to build pathogens as bio-weapons, e.g. in the form of a disease-causing agent or a toxin threatening not only human health but also agricultural or environmental targets.[7]

Figure 1. Examples of dual use of emerging technologies


Civilian use example
Category of emerging technology
Military use example
Drug delivery systems to treat cancer (nanobiology)
Biotechnology
Bioweapons (terrorism)
Apple FaceID
Advanced surveillance technologies
Enhanced army goggles
Google Maps for navigating the roads
Position, Navigation, and Timing Technology (PNT)
GPS jammers interfering with aircraft
Creating prosthetics for those with limb deficiencies
Additive manufacturing (3D printing)
Creating replacement parts for weapon systems
Amazon Alexa (speech and audio processing)
Artificial intelligence
Voice command for the battlefield
Precision agriculture and farming (microdrones)
Robotics
Black Hornet reconnaissance drone

Source: European Parliamentary Research Service (2019)[8]

Additive manufacturing (3D-printing) showcases a further ambivalence between beneficial and risky applications, since it gets increasingly applied in an array of sectors, such as automotive and machinery (e.g. low cost production of new and spare parts), electronics (conductive plastic filaments, wearable sensors), pharmaceuticals (e.g. printed tissue and organoids for drug testing) and medical technologies (e.g. customized implants and prosthetics, tissue engineering for regenerative medicine, a.o.). Military applications overlap with the above mentioned sectors (e.g. manufacturing spare parts, repair-on-spot, cure burn injuries) and render the distinction among civil and military usages increasingly blurred.[9]

Successful innovation processes are premised upon transfer of know-how, technologies, and their adjustment to specific missions, in order to deliver innovative breakthrough solutions. However, the more successful R&D spin-offs and world-wide transfer,

impact/publications/double-or-nothing-effects-diffusion-dual-use-enabling-technologies.

[5] Rath, J. et al. (2014): Evolution of Different Dual-use Concepts in International and National law and its Implications on Research Ethics and Governance. In: Science and Engineering Ethics, vol 20, no. 3, p. 769-790.

[6] European Union (2021): Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items. Available at: https://policy.trade.ec.europa.eu/help-exporters-and-importers/exporting-dual-use-goods_en.

[7] Sevini, F. et al. (2018): Emerging Dual-Use Technologies and Global Supply Chain Compliance. In: IAEA Symposium on International Safeguards: Building Future Safeguards Capabilities. Available at: https://inis.iaea.org/search/search.aspx?orig_q=RN:51003639 .

[8] European Parliamentary Research Service (2019): United States: Export Control Reform Act (ECRA) | Think Tank | Europäisches Parlament (europa.eu).

[9] Volpe, T. A. (2019): Dual-use Distinguishability: How 3D-printing shapes the Security Dilemma for Nuclear Programs. In: Journal of Strategic Studies, vol. 42, no. 6, p. 814-840.

triggered both by governmental policies and by business entrepreneurship the more probable is the accidental or intentional illicit diffusion of certain technologies that may have undesirable malicious applications. Such risks are often low-probability, high-impact events, such as runaway algorithms to intercept national critical infrastructure, bio-engineering of pandemics, usage of nano-technology and additive manufacturing for weapons of mass destruction.

A Moving Target for Strategic Trade Control Regimes

Debates The principal challenge here is practically to find a balance between unrestricted R&D and access to EDTs for fostering their beneficial uses, on the one hand, and restricting their intended or non-intended misuse, on the other. Export controls, established over the past decades in the context of regimes and treaties, in order to prevent or, decelerate the diffusion of items (i.e., materials, technologies, components, equipment, but also software) that could be misused in nuclear, chemical, biological, and cyber-driven weapons. Objective thereby is to detect and preempt accidental or purposeful illicit procurement or and trafficking of such items, by assessing the risk of misuse, assessing the track record of the importer, and by interfering in the link between exporter and importer.

States impose export restrictions and licensing procedures to companies concerning transfer of the controlled items, making export licenses mandatory. Four regimes, the Nuclear Suppliers Group (1975)[10], the Australia Group (1979)[11], controlling chemical and biological agents, the Missile Technology Control Regime (1987)[12], and the Wassenaar Arrangement (1996)[13], controlling conventional munitions, and dual-use goods and technologies, are currently operating. The existence of United Nations Security Council Resolution 1540 (2004)[14], aiming to limit the unauthorized access to strategic technology and goods, does raise strategic export controls as a barrier against proliferation, yet, there is no independent mechanism responsible for the enforcement of the above rules, despite regular reviews.

Also, the above four regimes are, informal, voluntary international associations of states, and, more often than not, manifest considerable lag in updating the critical items, as well as lack of agreement as of which items need to be uptaken, at all, on the control lists. Those are processes that do not easily achieve unanimity at multilateral level, since national interests by some technologically advanced countries may intervene, aiming to keep the technological competitive advantage of their industries and R&D sectors. In technology domains that are rapidly evolving, such as in the EDTs described above, the cutting-edge changes too fast for trade controls to follow swiftly in time.

Furthermore, risk assessment in the context of the above regimes has been so far predominantly focusing upon tangible components, and equipment, that could be traded physically as “product” across borders. The transfer of software, tacit knowledge via researcher exchanges, codified knowledge shared in digital infrastructures such as clouds, foreign investment in companies handling sensitive technology, especially when associated with forced technology transfer, are posing novel challenges around what is “transfer”, when electronic transmission is involved, and what is an “item”, when intangible software is the key technology, that existing regimes do not seem fully equipped to tackle.[15]

[10] See: Nuclear Suppliers Group - Home.

[11] See: The Australia Group (dfat.gov.au).

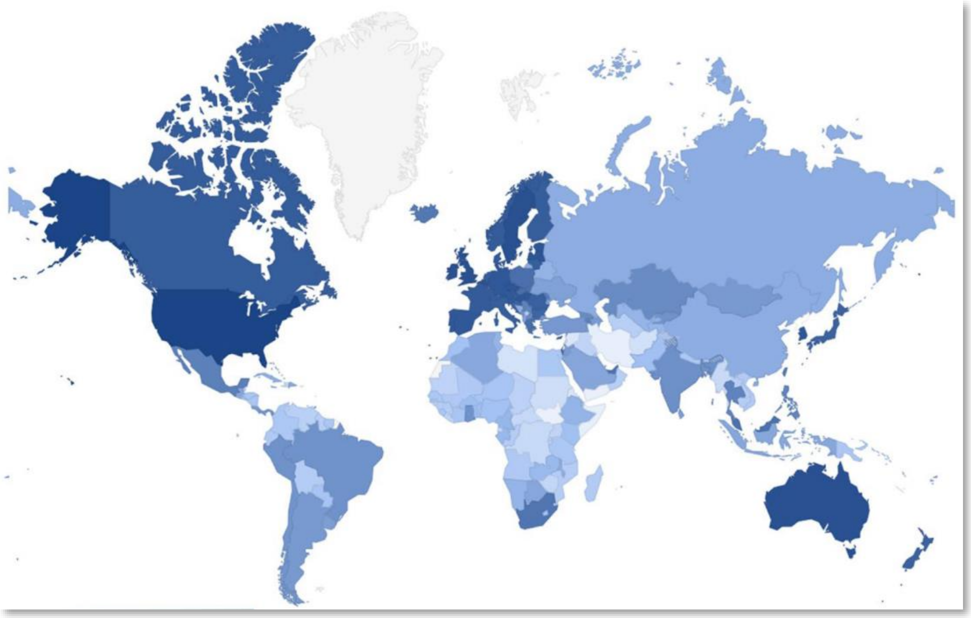
[12] See: MTCR – Missile Technology Control Regime.

[13] See: Home - The Wassenaar Arrangement.

[14] See: UN Security Council Resolution 1540 (2004) – UNODA.

[15] Suri, N. (2020): Emerging Technologies and the Challenges of Controlling Intangible Technology Exports. In: Strategic Trade Review vol. 6 no. 9, p. 137-159.

Figure 2. Strength of strategic trade control systems for all countries (darker blue: higher score along the five pillar criteria)



Source: Peddling Peril Index 2021/2022[16]

A snapshot of the performance of the export control regimes is provided by the Peddling Peril Index. The Index has ranked 200 countries, territories, or other entities according to their success in deploying of control instruments against trafficking of strategic commodities along five criteria: *1. International Commitment to preventing strategic commodity trafficking; 2. Legislation in place that regulates and oversees trade in strategic commodities, and criminalizes and aims to prevent strategic commodity trafficking; 3. Ability to Monitor and Detect Strategic Trade; 4. Ability to Prevent Proliferation Financing;* and *5. Adequacy of Enforcement against strategic commodity trafficking.*[17] The "heat" map above depicts the global discrepancies in controlling the illicit diffusion of critical technologies. One, among many, conclusions of the index, is that technologically developing countries, which are about to adopt and deploy EDTs, will need to drastically strengthen capacities to control illicit transfer and usage of technologies.

EDT Governance for Sustainability and Security as a Wicked Problem

As At global level, the UN have taken important steps in order to align technology-driven remedies with current diagnoses of post-crisis management, sustainability and welfare. For example, in the recent resolution adopted by the GA on 17 December 2021 on "Science, technology and innovation for sustainable development"[18], and also in UN Secretary-General's Roadmap for Digital Cooperation from 2020[19], the key role of STI activities is highlighted together with the risk of EDTs exacerbating inequalities. Nevertheless, the issues around national and international security risks, and human rights violations out of misuse of technologies, as raised in this policy brief, are not yet explicitly or sufficiently on the radar of policymakers. It is crucial to put all necessary safeguards in place in order to ensure that technological innovation will deliver on its promises, including making the benefits from EDTs into a *global public good*, while not backfiring by transforming them into a *global risk*.

[16] Institute for Science and International Security (2021): Peddling Peril Index. Under https://isis-online.org/ppi/detail/peddling-peril-index-for-2021-2022.

[17] Institute for Science and International Security (2021): Peddling Peril Index. Under https://isis-online.org/ppi/detail/peddling-peril-index-for-2021-2022.

[18] Available under: https://unctad.org/system/files/official-document/ecosoc_res_2021d29_en.pdf.

[19] Available under: https://www.un.org/en/content/digital-cooperation-roadmap/assets/pdf/Roadmap_for_Digital_Cooperation_EN.pdf.

The “wicked” character of the EDTs consists not merely in the fact that technologies and their applications are a *moving target*, hard to foresee in their beneficial and harmful effects. A major policy dilemma lies in that innovation policies, particularly in their claim to leave no one on the globe behind, raise, in a non-intended manner, the probability of illicit diffusion and misuse of technological advancements. International responsibility for regional and international security and stability, e.g. by preventing acquisition of critical technologies by extremist and terrorist groups, needs to be factored in in upcoming technology governance designs, and most crucially, help balance innovation, industrial competitiveness, and national security mantras, which often have competing and mutually undermining objectives.

This has been the main motivation behind this policy brief, that is, to sketch out the challenge, raise awareness about the urgency for action, and point to a number of governance options. Besides the existing regimes for export controls, which are a necessary, yet not sufficient instrument to prevent illicit diffusion and usage, this brief points to a mix of approaches that could be deployed in the context of existing forums and platforms and beyond.

Outlook and Recommendations

The design and governance of STI policies is critical in facing the major challenges ahead for achieving the 2030 SDG agenda, bearing particularly in mind the promotion of peace, justice and strong institutions (SDG 16), as well as building resilient infrastructure, fostering inclusive and sustainable industrialization and innovation (SDG 9). The UN Technology Facilitation Mechanism, and the Interagency Task Team on STI for SDGs may see value in taking notice and accommodate the Dual-Use problematique in their future agendas, creating the necessary traction at political level.

This brief aimed at mobilizing towards the integration of key approaches and instruments into the workings of the 2030 Connect Platform, including the Global Pilot roadmaps on STI for SDGs. Those forums and initiatives may well provide at a hands-on, stakeholders´ level the necessary multilateral leverage for generating awareness about the Janus-faced EDTs, and promote institutional capacity building, and responsible and accountable governance as governance principles to guide their transfer and application also in the technologically developing parts of the globe.

Establish rigorous anticipatory STI criticality assessments

Criticality assessments need to define thresholds for “*Dual-Use mission creep*” after which beneficial civilian technology usages may turn into a potential, e.g. in the form of a cyber attack against critical infrastructure, illicit surveillance against human rights, or components in a lethal weapon. Such assessments need to be anticipatory and deploy also a future “use-case” methodology for fleshing out key parameters for acceptable use. The International Standard Organization and the International Electrotechnical Committee have piloted that for Artificial Intelligence applications.[20]

To prevent weaponization of technologies, a number of factors need to be taken account of in risk assessment: For example, nuclear technology has very high *accessibility thresholds*, it requires highly specialized skills in order to get applied, the pace of advance is not high, and its availability world-wide is rather limited. These characteristics do not necessarily apply to off-the-shelf ICT technologies, that can be misused for cyberwarfare, or to biotechnologies, such as pathogen research, synthetic biology, genome editing, or neurobiology. Besides the accessibility threshold, the *skills and expertise* necessary to apply the technology, the *geographical dispersion of actors*/laboratories or industries that develop such technologies, the *magnitude and the imminence of potential harm*, the *maturity* of technology, and the *rate of its advance* need to be continuously assessed.[21]

Strengthen a “Whole-of-value-chain” stakeholder engagement

Monitoring and oversight mechanisms for the potential applications of EDTs are either fragmented or missing. Collaborative international technology sharing platforms belong to the appropriate venues for streamlining *inclusive technology-watch programs*, by engaging *key stakeholders from the whole value chain*, that is, from R&D, to commercial manufacturers and international exporters, to civil society and public authorities as end users. Bringing different stakeholders, from research, development and export industry together will merge the contexts of invention (upstream) and those of application (downstream),

[20] ISO/IEC 24030, Information technology — Artificial intelligence —Use cases. Under https://etech.iec.ch/issue/2021-03/iec-and-iso-publish-over-130-emerging-ai-use-cases.

[21] Harris, E. D. (ed.) (2016): Governance of Dual-Use Technologies: Theory and Practice. American Academy of Arts & Sciences.

helping to foster a kind of prospective „*situational awareness*“ about high-risk non-intended applications, that usually outpace hard regulation.[22] Transnational and cross-sectoral information sharing would facilitate "*early warning*" against misuse potential, but equally, also point to innovative beneficial applications. The platforms can be advised by an Open-Ended Working Group (OEWG), as similar to the UNODA Open-ended Working Group on developments in the field of information and telecommunications in the context of international security (2019-2021)[23].

Rethink EDTs for SDGs from the perspective of Responsible Research and Innovation

UNESCO has adopted in 2017 a recommendation for Science and Scientific Researchers, updating the one from 1974, and in 2018 the UN Secretary-General identified responsible research and innovation (RRI) in science and technology, as an approach for academia, the private sector and governments to work on the mitigation of risks that are posed by new technologies.[24] Responsibility, mutual responsiveness and commitment of stakeholders in the research & innovation value chains are increasingly principles promoted by the OECD and by World Economic Forum initiatives.[25] This constitutes an "upstream" way of governing technological risks through due diligence checks already in the stages prior to marketization and international trading via globalized supply chains. Responsibility of stakeholders in RDI processes reinforces accountability and fosters systematic reflection about non-desirable, and even catastrophic consequences of research and innovation, promoting a "by-design" inscription of certain rules and red lines in the application of technology.

[22] Hagemann, R. et al. (2018): Soft Law for Hard Problems: The Governance of Emerging Technologies in an Uncertain Future. In: *Colorado Technology Law Journal.* Under https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3118539 ; Merchant, G. E. and Wallace, W. (2015): Coordinating Technology Governance. In: ISSUES in Science and Technology, vol. XXXI, No. 4. Under https://issues.org/coordinating-technology-governance/ .

[23] See under: https://www.un.org/disarmament/open-ended-working-group/.

[24] Available under: https://unesdoc.unesco.org/ark:/48223/pf0000259256.

[25] OECD (2021): Recommendation of the Council for Agile Regulatory Governance to Harness Innovation. Under https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0464 ;
World Economic Forum (ed.) (2020): Ethics by Design: An Organizational Approach to Responsible Use of Technology. Available at https://www.weforum.org/whitepapers/ethics-by-design-an-organizational-approach-to-responsible-use-of-technology .