Décembre 2011

Fiche de l'Irsem n°10

Controlling the Uncontrollable ?
U.S. Dual-Use Export Controls in the Post-Cold War Era

Hugo MEIJER

Pour citer ce document :

Hugo MEIJER, "*Controlling the Uncontrollable ? U.S. Dual-Use Export Controls in the Post-Cold War Era*"
Fiche de l'Irsem n° 10,
décembre 2011, 13 pages

http://www.irsem.defense.gouv.fr

Décembre 2011

Since the collapse of the Soviet Union, non-proliferation has come to the forefront of the academic and policy debate. However, while the proliferation of conventional weapons and of weapons of mass destruction (WMDs) – nuclear, biological, chemical and radioactive – are the subject of a rich body of academic literature,[1] the worldwide proliferation of dual-use technologies[2] as well as the efforts to control their diffusion are still under explored.[3] Dual-use technologies have nonetheless become increasingly critical for modern militaries. The Pentagon's *Military Critical Technologies List* (MCTL) – which describes those technologies considered to be "critical to maintaining superior US military capabilities" and whose acquisition by potential adversaries "would lead to the significant enhancement of [their] military-industrial capabilities […] to the detriment of US security interests" – includes dual-use items such as electronics, information and space systems.[4] These technologies are defined as "enabling" or "critical" in that they have become a fundamental pillar of military systems.

---

[1] On WMD proliferation see: Boutherin G., 2007, *La lutte contre la prolifération des armes de destruction massive*, La Documentation française; Busch N., Joyner D., 2009, *Combating Weapons of Mass Destruction: The Future of International Nonproliferation Policy*, London: University of Georgia Press; Cirincione J., Wolfsthal J., Rajkumar M., 2005, *Deadly Arsenals: Nuclear, Biological and Chemical Threats*, 2nd Edition, Carnegie Endowment for International Peace; Finel B., Finlay B., Nolan J., 2003, "The Perils of Nuclear, Biological, and Chemical Weapons," in Brown E. (ed), *Grave New World: Security Challenges in the 21st Century*, Georgetown University Press, pp. 62-90; Grand C., *et alii*, 2009, *US-European Nonproliferation Perspectives: A Transatlantic Conversation*, Center for Strategic and International Studies; Mattis F., 2009, *Banning Weapons of Mass Destruction*, London: Praeger Security International; Russell J., Wirtz J., 2007, *Globalization and WMD Proliferation: Terrorism, Transnational Networks and International Security*, Routledge; Schreier F., 2009, *WMD Proliferation: Reforming the Security Sector to Meet the Threat*, Washington D.C.: Potomac. On conventional weapons proliferation and arms sales see: Husbands J., 2003, "The Proliferation of Conventional Weapons and Technologies," in Brown E. (ed), *Grave New World: Security Challenges in the 21st Century*, Georgetown University Press, pp. 38-61; Pierre A., 1998, *Cascade of Arms: Managing Conventional Weapons Proliferation*, Cambridge, Mass.: World Peace Foundation; Stohl R., Grillot S., 2009, *The International Arms Trade*, Cambridge: Polity; Tan A. (ed), 2010, *The Global Arms Trade: A Handbook*, New York: Routledge.

[2] Dual-use technologies are technologies that have both commercial and military applications. They may be developed for military purposes and then be applied commercially or vice versa.

[3] The main academic works on post-Cold War export controls are mainly confined to the 1990s and, overall, do not specifically focus on dual-use technologies. See among others: Bailey K., Rudney R. (eds), 1993, *Proliferation and Export Controls*, Lanham: University Press of America; Beck M., Cupitt R., Jones S., Gahlaut S., 2003, *To Supply or toDeny: Comparing Nonproliferation Export Controls in Five Key Countries*, Kluwer Law International; Bertsch G., Cupitt R., Elliott-Gower S. (eds), 1994, *International Cooperation on Nonproliferation Export Controls: Prospects for the 1990s and Beyond*, Ann Arbor: University of Michigan Press; Bertsch G., Cupitt R., Yamamoto T. (eds), 1995, *US and Japanese Nonproliferation Export Controls: Theory, Description and Analysis*, University Press of America; Bertsch G., Elliott-Gower S. (eds), 1992, *Export Controls in Transition: Perspectives, Problems, and Prospects*, Duke University Press; Crawford B., 1995, "Hawks, Doves, But no Owls: International Economic Interdependence and Construction of the New Security Dilemma," in Lipschutz R. (ed), *On Security*, New York: Columbia University Press; Cupitt R., 2000, *Reluctant champions: US Presidential Policy and Strategic Export Controls*, Routledge N. Y.; Hofhansel C., 1996, *Commercial Competition and National Security*: *Comparing US and German Export Control Policies*, Praeger; Renelle G., 2000, "La gestion de la dualité sous l'administration Clinton," *Working Paper IMRI*, May. For journal articles on multilateral export controls, see footnote 17.

[4] "Military Critical Technologies List" (undated) available at http://www.dm.usda.gov/ocpm/Security%20Guide/T1threat/Mctl.htm. The other major technology categories

Décembre 2011

Two key interrelated trends have contributed to the growing importance of dual-use technologies in the new geopolitical environment brought about by the end of the Cold War. First, the reduction in defense budgets, the continuing growth in the costs of new weapons systems coupled with the higher innovation rates of the high tech commercial sector relative to the defense sector, have led to a growing reliance of the military on commercially-developed technologies, especially information and communication technologies (ICT).[5] Second, changes in strategic thinking – driven by the so called Revolution in Military Affairs (RMA) and in particular the concept of Network Centric Warfare (NCW) – have fostered a growing emphasis on the use of ICT in modern combat. NCW aims at turning information superiority into combat power by integrating C4ISR capabilities and long-range precision weapons into a "system of systems."[6] NCW relies on critical dual-use technologies – such as satellites, computer processor chips and software – in order to achieve command, control, communications, computers, and intelligence (C4I) capabilities,[7] interoperability,[8] and space dominance.[9] This growing reliance on dual-use technologies to network military forces however also constitutes a potential vulnerability of military systems. The proliferation of sources of supply of dual-use items lowers entry barriers for a wide range of actors to acquire advanced technologies that could be employed as an asymmetric means to disrupt the opponent's C4ISR networks in the framework of an anti-access/area-denial (A2/AD) strategy.[10]

In light of the growing importance of dual-use technologies in national force structures and of their vulnerability to disruptive attacks, this paper examines the key trends that have affected the efforts to control the proliferation of dual-use technologies in the post-Cold War era. It will be argued that, since the dissolution of the Soviet Union, multilateral, technological and industrial dynamics have eroded the ability of states – both unilaterally and multilaterally – to control the diffusion of dual-use technologies.

---

included in the MCTL are: Aeronautics systems, Armaments and energetic materials, Chemical and biological systems, Directed and kinetic energy systems, Ground systems, Guidance, navigation, and vehicle control, Information warfare, Manufacturing and fabrication, Marine systems, Materials, Nuclear systems, Power systems, Sensors and lasers, Signature control, Weapons effects and countermeasures. As of October 2011, the MCTL has been removed from the website of the Defense Technical Information Center (re-establishment date yet to be determined), see http://www.dtic.mil/mctl.

5 For more details, see Section III of this report.

6 C4ISR refers to Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance capabilities. On the RMA and NCW, see Dombrowski P., Ross A., 2002, "Selling Military Transformation," *Orbis*, Summer, p. 524-5; and Dombrowski P., Gholz E., Ross A., 2002, *Military Transformation and the Defense Industry After Next: The Defense Industrial Implications of Network-Centric Warfare*, Center for Naval Warfare Studies, US Naval War College, Chapter 1.

7 As stressed by a report of the Congressional Research Service, "C4I capabilities are the nervous system of the military." Wilson, 2007, *Network Centric Operations: Background and Oversight Issues for Congress*, Congressional Research Service, CRS Report for Congress RL32411, March 15, p. 15.

8 The US Department of Defense defines interoperability as "the condition achieved among communications-electronics systems or items of communications-electronics equipment when information or services can be exchanged directly and satisfactorily between them and/or their users." Department of Defense, 2010, *Dictionary of Military and Associated Terms*, Joint Publication 1-02, 8 November 2010 (as amended through 15 May 2011).

9 Space dominance, or superiority, is "the degree of dominance in space of one force over another that permits the conduct of operations by the former and its related land, maritime, air, space, and special operations forces at a given time and place without prohibitive interference by the opposing force." Department of Defense, 2010, *ibidem*.

10 Strategies of Anti-Access (A2) aim at impeding the deployment of the enemy's forces into the combat theatre while Area-Denial (AD) seeks to restrict its freedom of action.

Having first provided an overview of the Cold War multilateral framework governing export controls (Section I), this report will proceed to illustrate the decreased effectiveness of multilateral export controls in the post-Cold War era (Section II). The technological and industrial patterns that have affected states' ability to control the diffusion of dual-use technologies will then be examined (Section III). It will be shown that the commercialization of the defense industrial base, the worldwide technology diffusion, and the growing indigenous capabilities in countries subject to export controls pose fundamental challenges for the effectiveness of export controls.

To demonstrate this argument, we analyze the impact of these trends on US dual-use export controls. The need to find a proper balance between the economic interests involved in exporting dual-use technologies and the military implications of transfers of sensitive technologies to potential competitors is a common feature in the making of export control policy of any country. Nevertheless, several reasons justify a focus on the United States. First, since the early days of the Cold War, the United States has been, within NATO, the member state willing to impose the most stringent export controls in order to preserve its military and technological preeminence.[11] Furthermore, the US is both the world's largest exporter of military-related technology and among the first exporters of advanced technology products.[12] The United States is therefore a fruitful case study as it has been the country most affected by the decreased effectiveness of dual-use export controls in the post-Cold War era.

I. EXPORT CONTROLS DURING THE COLD WAR

In the aftermath of World War II, the US and its allies established a system of both national and multilateral export controls on the transfer of military-related items to the Warsaw Pact countries and to the People's Republic of China. At the multilateral level, the Coordinating Committee For Multilateral Export Controls (COCOM) was formed in 1949 to harmonize restrictions on conventional and dual-use items exports. It was based on a shared understanding by its member states of the need to control the export of sensitive technologies to Communist countries in order to delay the qualitative progress of their military capabilities. COCOM established three lists of controlled items: the International Munitions List, the International Atomic Energy List, and the Industrial List (for dual-use items). Under the rules of the Cold War multilateral framework, each member had a veto power over the export of controlled technologies by any other member.[13] Furthermore, during COCOM's more than forty years of existence, the ability of Western countries to effectively restrict the diffusion of dual-use technologies was facilitated by the fact that the suppliers of advanced technologies were mainly

[11] On the degree of convergence (or divergence) of interests between the US, Western Europe and Japan in the making of multilateral export controls throughout the Cold War, see Mastanduno, 1992, *op. cit.*

[12] The advanced technology products (ATPs) category is a classification developed by the US Census Bureau to track exports and imports that embody ten major leading-edge technologies areas: biotechnology, life science technologies, optoelectronics, information and communications, electronics, flexible manufacturing, advanced materials aerospace, weapons, and nuclear technology. For statistics on trade in ATPs, see National Science Foundation, 2010, *Science and Engineering Indicators*, Chapter 6: Industry, Technology, and the Global Marketplace. On US arms exports, see Grimmett R., 2010, *Conventional Arms Transfer to Developing Nations, 2002-2009*, Congressional Research Service, CRS Report for Congress R41403, and Grimmett R., 2010, *US Arms Sales: Agreement with and Deliveries to Major Clients, 2002-2009*, Congressional Research Service, CRS Report for Congress R41539.

[13] Grimmett R., 2006, *Military Technology and Conventional Weapons Export Controls: The Wassenaar Arrangement*, Congressional Research Service, CRS Report for Congress, p. 1.

concentrated among the NATO allies and the other members of COCOM (such as Japan), which enabled COCOM to function as a *de facto* oligopolistic cartel.[14]

Accordingly, during the Cold War, a common threat perception, the overall effectiveness of the multilateral framework as well as a Western technological oligopoly, allowed the US and its allies to control the diffusion of dual-use technologies to the Communist bloc. As Senator Joseph Lieberman (D-CT) explains, throughout this period the US and its allies "were pretty much able to keep our enemy from obtaining significant amounts of potentially harmful technology. We were able to do this because our allies broadly shared our concerns and our strategic views and because much of the technology that we wanted controlled was, in fact, capable of being controlled by our allies and us."[15]

II. A TRANSFORMED MULTILATERAL FRAMEWORK IN THE POST-COLD WAR ERA

With the collapse of the Soviet Union – the key target of the Cold War multilateral export control system – growing disagreements between the US and its COCOM partners arose on the rationale and scope of export controls. Pressures mounted from US allies for loosening export restrictions and to dismantle COCOM. The demise of the USSR therefore paved the way for a radical reform of the multilateral export control framework. COCOM formally ceased to exist on March 31, 1994, and negotiations started over its replacement with a new post-Cold War institution. Throughout the negotiations, several European states opposed a COCOM-type institution (i.e. with members' veto power) and did not want to target specific countries the same way COCOM targeted Warsaw Pact countries.[16] The US negotiating team was therefore compelled to agree, in 1996, to the establishment of a much weaker institution – the Wassenaar Arrangement for Export Controls for Conventional Arms and Dual-Use Goods and Technologies (hereafter Wassenaar).[17] Although it inherited from COCOM a common set of list of controlled items, several features of Wassenaar make it less effective than its Cold War predecessor in controlling the export of sensitive technologies.

First, unlike under COCOM, Wassenaar lacks the unanimity rule that provided each COCOM member with the right to veto the individual exports of other member countries. Second, as a consequence of the lack of agreement between member states on a common strategic threat, Wassenaar

---

14 See Cevasco F., 2001, "Survey and Assessment: Alternative Multilateral Export Control Structures," Working Paper No. 3, Study Group on Enhancing Multilateral Export Controls for US National Security, Henry L. Stimson Center, p. 7.

15 Testimony before the Committee on Governmental Affairs, United States Senate, Hearing on *The Wassenaar Arrangement and the Future of Multilateral Export Controls*, 106th Congress, Second Session, April 12, 2000.

16 Interviews with officials from the US departments of State, Defense and Commerce who participated in the negotiations that led to the replacement of COCOM with Wassenaar, Washington D.C., March-May and September-November 2010.

17 On the Wassenaar Arrangement, see Auer D. (ed), 2005, *Wassenaar Arrangement: Export Controls and its Role in Strengthening International Security*, Favorita Papers, Diplomatische Akademie Wien / Federal Ministry of Foreign Affairs, Vienna; Beck M., 2000, "Reforming the Multilateral Export Control Regime," *The Nonproliferation Review*, Summer; Craft C., Grillot S., 1999, "Transparency and the Effectiveness of Multilateral Nonproliferation Export Control Regime: Can Wassenaar Work?," *Southeastern Political Review*, Vol. 27, No. 2; Cupitt T., Grillot S., 1997, "COCOM is Dead, Long Live COCOM: Persistence and Change in Multilateral Security Institutions," *British Journal of Political Science*, Vol. 27, No. 3. (July), pp. 361-389; Lipson M., 1999, "The Reincarnation of COCOM: Explaining Post-Cold War Export Controls," *Nonproliferation Review*, Vol. 6, No. 2 (1999), pp. 33-51, Lipson M., 2006, "The Wassenaar Arrangement: Transparency and Restraint through Trans-Governmental Cooperation?," in Joyner D. (ed), *Non-proliferation Export Controls: Origins, Challenges and Proposals for Strengthening*, Ashgate Publishing. For a description of Wassenaar's working, see also www.wassenaar.org/introduction/index.html

has no agreed upon country-targets, such as the Soviet Union during the Cold War. Third, though Wassenaar allows member states to cooperate and harmonize their respective national export control systems, the ultimate application of export controls is left to national discretion. Fourth, the enlarged membership makes it more difficult to reach decisions on what items should be on Wassenaar's lists.[18] Finally, Wassenaar lacks a "no undercut" rule, as COCOM had. This means that a member state is not prohibited from exporting a controlled item to a particular destination that has been previously denied by another member state (i.e. undercutting).[19] As a consequence, relative to COCOM, the post-Cold War multilateral architecture is a much loser system and is less effective in establishing agreed-upon export controls.

III. TECHNOLOGICAL AND INDUSTRIAL DYNAMICS

Beyond the weakening of the multilateral framework, both technological and industrial trends have contributed to the erosion of the ability of states to control, unilaterally or in concert, the proliferation of dual-use technologies.

(A) The Commercialization of the Defense Industrial Base

Business Cycles, Innovation Rates, and the Bifurcation between Commercial and Defense R&D

Throughout the Cold War and until the mid 1980s, the development of state-of-the-art technologies applicable to military systems was most often driven by the defense sector, i.e. generated by defense contractors funded by governments and then transferred and adapted to the commercial marketplace. Examples of this so called *spin off* – from government funded defense projects to the commercial economy – are computer hardware, software, electronics, space advances and nuclear power.[20] In particular, the Global Positioning System (GPS) and Internet – both developed by the Pentagon's Defense Advanced Research Projects Agency (DARPA) – later found broad commercial applications.

However, since the 1980s and increasingly so after the end of the Cold War, commercial R&D expenditures gradually came to outpace the US government R&D funding and the gap between the two constantly widened in the post-Cold era (figure 1). Furthermore, as shown in figure 2, within the government R&D funding, the defense share – after an increase in the 1980s and its peak in 1987 (70%) – has shrunk in the post-Cold War period reaching between 55-60% of the total. As a consequence, the centre of gravity in the development of dual-use technologies – especially information and communications technology – shifted from State-led research to the commercial private sector.[21] In other words, the commercial sector has outpaced the military industrial sector in developing and adopting advanced technologies. As Amitav Mallik explains, while during the Cold War dual-use technologies were defined as military technologies that also had civilian applications, in the majority of

[18] While COCOM had, at the time of its dissolution, seventeen member states, Wassenaar today includes more than thirty countries. For a list of Wassenaar's participating states see http://www.wassenaar.org/participants/index.html

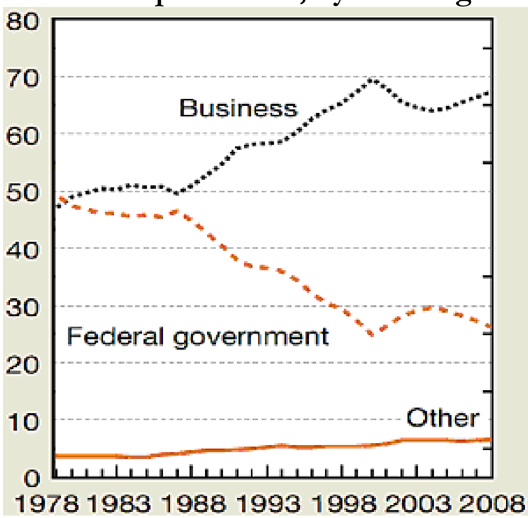
[19] Instead of an undercut rule – that exists in other international regimes such as the Missile Technology Control Regime and the Nuclear Suppliers Group – Wassenaar's member states have an informational requirement. They must notify all Wassenaar participants "preferably within 30 days, but no later than within 60 days" after they approve a license of an item on the dual-use list's Tier 2 "sensitive" annex. See Lipson M., 2006, *op. cit.*, p. 56.

[20] Walsh K., 2009, "The Role, Promise and Challenges of Dual-Use Technologies in National Defense," in Bitzinger R. (ed), *The Modern Defense Industry: Political, Economic, and Technological Issues*, Praeger, p. 127.

[21] Walsh K., 2009, *ibidem*, p. 133.

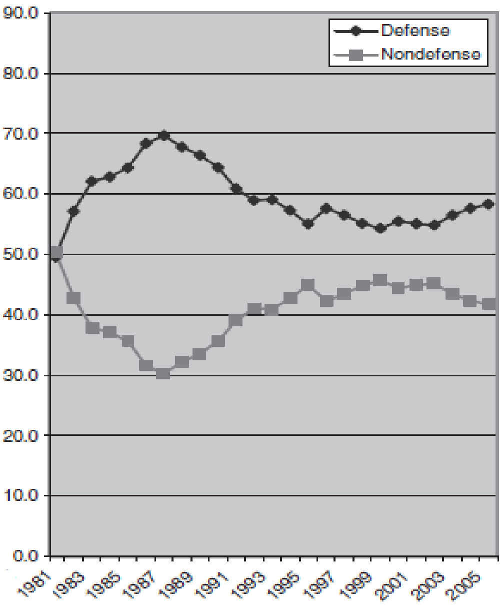
technologies that have military applications it is today the civilian (or commercial) research and development that has taken the lead.[22]

Figure 1: National R&D Expenditures, by Funding Source (percentage)



Source: Adapted from National Science Foundation, 2010, *Science and Engineering Indicators*

Figure 2: Defense & Nondefense Share of Government R&D Outlays (percentage)



Source: Adapted from Mowery D., 2009, "Plus ça change: Industrial R&D in the 'third industrial revolution'," *Industrial and Corporate Change*, Vol. 18, No. 1.

The 1995 White House report *Second to None: Preserving America's Military Advantage Through Dual-Use Technology* characterized this changing reality as follows: "in a number of important technologies, the defense industry is no longer in a position of technological leadership with respect to the commercial sector. In fact, the new technologies that are most critical to our military advantage – software,

---

[22] Mallik A., 2004, *Technology and Security in the 21st Century: A Demand-Side Perspective*, SIPRI Research Report No. 20, p. 120.

computers, semiconductors and telecommunications – all are being driven by fast growing commercial demand, not by military demand."[23] As the locus for state-of-the-art dual-use technologies – and especially information and communications technology – shifted toward the commercial sector, the Pentagon could not keep pace with the market-driven efficiencies, higher rates of innovations and shorter business cycles of the private sector.[24] With the computational capabilities of commercially-developed information technology doubling every 18 months – as stated by the so called Moore's law – the rapid innovation rates of the commercial industry "greatly outpace[d] the slow march of government-procured products, particularly within the Department of Defense's acquisition process, in which major defense acquisition programs are procured over the source of decades rather than years."[25] As a consequence, "the military have had to face the reality that their design process was such that the information technology components contained [in defense products] were obsolete before the final product was introduced and that the long life of the end products magnified that problem."[26]

From MilSpec to Commercial-Military Integration

This bifurcation between the innovation rates of the military and the civilian industrial base has led the US government to promote the integration of civilian and military R&D and production activities, the so called Commercial-Military Integration (CMI) or *spin on*. As defined by the National Research Council, CMI is the "use of the commercial manufacturing base to meet defense needs over the life cycle of a system. It encompasses a range of approaches, with commercial off-the-shelf (COTS) items at one extreme and products and processes unique to defense applications on the other" (see figure 3).[27] Secretary of Defense William Perry first launched this process of transformation of the US industrial base with the so called "MilSpec Reform", announced in a June 1994 memorandum entitled *Specifications and Standards – A New Way of Doing Business*.[28] Because of the proliferation of detailed military-unique requirements and of the consequent cumbersome procurement system, defense firms were unwilling to work with the Pentagon and this, in turn, created barriers to the Department of Defense (DOD) access to commercially-developed technologies. "The objective of the 'MilSpec Reform' was to break down those barriers to save money, remove impediments to getting state-of-the-art technology into [US] weapon systems, and provide better access to the commercial industrial base."[29] The reform effort focused on expanding the use of commercial products and practices to leverage the massive technology investments of the private sector and reap the benefits […] provided

[23] The White House, 1995, *Second to None: Preserving America's Military Advantage Through Dual-Use Technology*, p. 1.

[24] Although the concerns over the long cycles of the defense acquisition process are not a new phenomenon, the commercialisation of the Pentagon's industrial base has sharpened those concerns given the much shorter business cycles of the civilian industry.

[25] The Industrial College of the Armed Forces, 2010, *Electronics Industry*, National Defense University, p. 15. The Moore's Law, which takes its name from the co-founder of Intel, Gordon Moore, states that the capacity of microprocessing chips doubles every 18 months.

[26] Interview with a former high-level official of the US Department of Commerce, June 13, 2011.

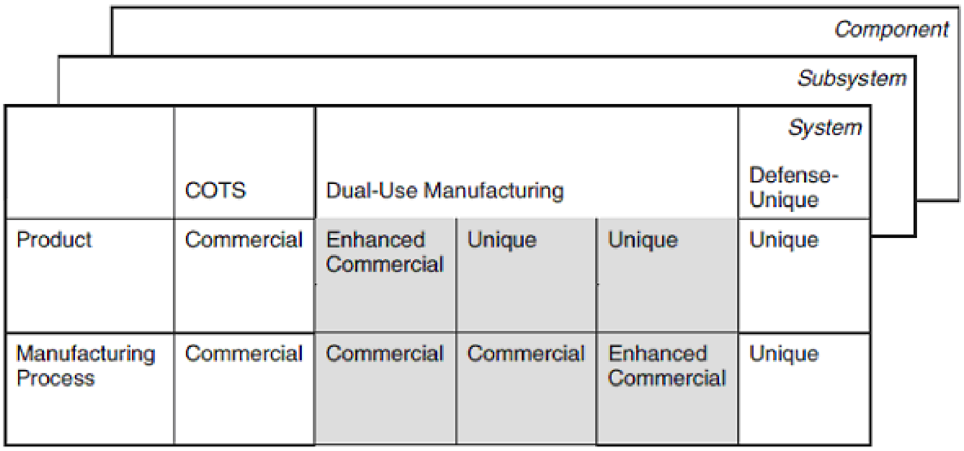
[27] National Research Council, 2002, *Equipping Tomorrow's Military Force: Integration of Commercial and Military Manufacturing in 2010 and Beyond*, Committee on Integration of Commercial and Military Manufacturing in 2010 and Beyond. On CMI see also Lorell M., Lowell J., Kennedy M., Levaux H., 2000, *Cheaper, Faster, Better? Commercial Approaches to Weapons Acquisition*, Santa Monica: RAND Corporation; Gansler J., Lucyshyn W., 2008, *Commercial- Off-The-Shelf (COTS): Doing It Right*, Maryland University, Center for Public Policy and Private Enterprise.

[28] Military Specification (or MilSpec) are the "technical requirements for purchased material that is military unique or substantially modified commercial items," see www.everyspec.com

[29] US Department of Defense, Office of the Under Secretary of Defense for Acquisition, Technology and Logistics, 2001, *MilSpec Reform Final Report. An Ending: A New Beginning*, April, p. 1.

from a robust commercial industrial base."[30] This reform was part of the broader so called Dual-Use Strategy, which aimed at "preserving the technological superiority of US forces" by placing "greater reliance on the commercial sector to reduce costs, shorten acquisition cycle times and obtain technologically advanced defense equipment."[31] Clearly, dual-use technology developed in the commercial sector cannot serve all military needs. No commercial counterpart exists for conventional munitions or nuclear attack submarines, for instance. But "a great many defense needs can be served better and less expensively by commercial firms."[32]

Figure 3: Commercial-Military Integration Framework



Source: National Research Council, 2002, *Equipping Tomorrow's Military Force: Integration of Commercial and Military Manufacturing in 2010 and Beyond*, Committee on Integration of Commercial and Military Manufacturing in 2010 and Beyond.

Impact on Export Control Policy

Since the 1990s, as stressed by a report of the Defense Science Board, the Pentagon has therefore gone "from relying almost exclusively on a captive US defense industry to depending more on the commercial market, both domestic and international."[33] The growing reliance of the Pentagon on civilian firms to supply state-of-the-art dual-use technologies has had a major impact on the making of export control policy given that "any significant restriction on exports would likely slow corporate growth and limit the extent to which profits can be put back into research and development on next-generation technology" and thereby weaken the technological and industrial base on which the DOD depends ever more.[34] And the continuing trend toward the globalization of high tech industries means that exports are now the key to the growth and good health of the US information and communications technology sector. This suggests that it has become untenable for the US to impose stringent export controls on dual-use ICT given that sustaining the commercial industrial base on which the Pentagon increasingly relies requires loosening the controls on the export of these advanced

[30] US Department of Defense, 2001, *ibidem*.
[31] US Department of Defense, 1995, *Dual Use Technology: A Defense Strategy for Affordable, Leading-Edge Technology*, February, Preface. See also Stowsky J., 1999, "The History and Politics of the Pentagon's Dual-Use Strategy," in Markusen A., Costigan S. (eds), *Arming the Future: A Defense Industry for the 21st Century*, Council on Foreign Relations Press, pp. 106-157.
[32] White House, 1995, *op. cit.*, p. 8.
[33] US Department of Defense, Office of the Under Secretary for Acquisition and Technology, 1999, *Final Report of the Defense Science Board – Task Force on Globalization and Security*, p. 27.
[34] US Department of Defense, 1999, *ibidem*.

technologies. As a former high-level official of the Department of Commerce puts it, "you have the situation where the Pentagon needs IBM more than IBM needs the Pentagon. […] So the next step is how do you keep IBM healthy and profitable? And there is only one way: exports."[35]

(B) Technology Diffusion and Growing Indigenous Capabilities

The previously described shift from *spin off* to *spin on* – i.e. to a situation in which it is advances in the commercial sector that are leading the technological innovation process and creating new military applications – has had major consequences for the proliferation of dual-use technologies.[36] As Markusen and Costigan put it, "the inclusion of more commercial components raises the potential for more rapid diffusion of the sophisticated weapons that are at the heart of America's security strategy. […] How can the Pentagon have access to commercial technologies, which have surpassed their military counterparts, without risking accelerated proliferation and erosion of America's technological edge?"[37]

The global diffusion of technological know-how and the commercial availability of critical dual-use information technologies has fundamentally challenged the making of national and multilateral export controls in two respects. First, it has led to the proliferation of alternative sources of supply (the so called "foreign availability" of a technology) thereby making export controls increasingly ineffective, all the more so in the framework of a weak multilateral architecture. As Adam Segal puts it, "the globalization and commercialization of R&D allows states that are potentially hostile to the United States to acquire off-the-shelf technologies for sensors, information processing, and precision guidance from suppliers in Europe, Japan, Korea, and Taiwan."[38] In the words of a former National Security Council official, "the technological advances simply made the [foreign] availability of computational capability so diffuse that it became impossible to control. […] You just lost control."[39] Second, and relatedly, technology diffusion and foreign availability have also facilitated the growth of indigenous technological capabilities in countries subject to export controls. This is apparent, for instance, both in the case of US controls on semiconductors and supercomputer exports to the People's Republic of China (PRC). In the semiconductor sector, the Government Accountability Office has concluded that:

> "Since 1986, the gap between US and Chinese semiconductor manufacturing technology has rapidly narrowed. […] Fifteen years ago, China was five generations of technology behind the United States' then-current commercial production capability. […] Today, China's advanced manufacturing facilities can make chips that are less than one generation behind the current, commercial state-of-the-art. […] The growing sophistication of China's semiconductor manufacturing facilities, which has improved its ability to develop more capable weapons systems and advanced consumer electronics, has been fuelled by China's success in acquiring manufacturing technology from abroad" (see figure 4).[40]

---

[35] Interview, March 12, 2010.

[36] See Mallik, 2004, *op. cit.*, pp. 117-121.

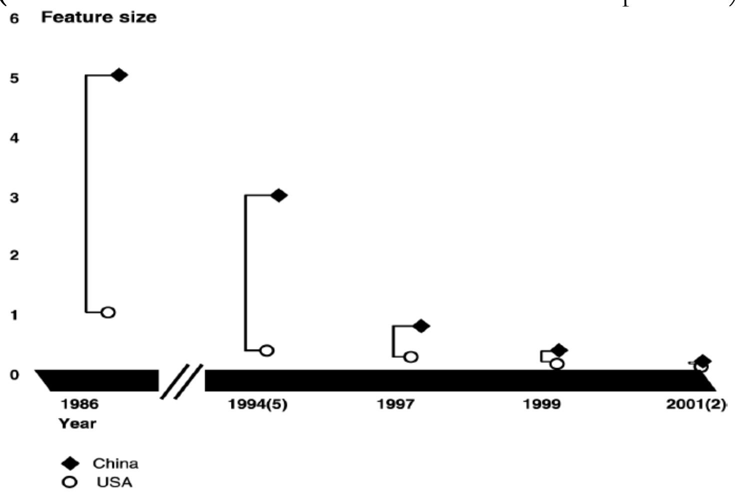
[37] Markusen A., Costigan S., 1999, "The Military Industrial Challenge", in Markusen A., Costigan S., (eds), *Arming the Future: A Defense Industry for the 21st Century*, Council on Foreign Relations, p. 5

[38] Segal A., 2004, "Practical Engagement: Drawing a Fine Line for US-China Trade," *Washington Quarterly* (Summer) p. 169. See also Segal A., 2004, "Is America Losing its Edge? Innovation in a Globalized World," *Foreign Affairs* (November/December).

[39] Interview, March 25, 2010.

[40] Government Accountability Office, 2002, *Export Controls: Rapid Advances in China's Semiconductor Industry Underscore Need for Fundamental US Policy Review*, GAO-02-620, pp. i-2-9.

Figure 4: Gap between US and Chinese Semiconductor Manufacturing Technology
(as measured in the feature size of the semiconductors produced)



Source: Government Accountability Office, 2002, *Export Controls: Rapid Advances in China's Semiconductor Industry Underscore Need for Fundamental US Policy Review*, GAO-02-620

In the case of supercomputer (or high performance computer) export controls, China surpassed the US in building the world's most powerful computer in 2010, the Tianhe-1A.[41] Given the growing capabilities of the PRC in the field of supercomputing, US controls on the export of supercomputers to China have essentially lost their *raison d'être*. In sum, the worldwide technology diffusion and foreign availability of advanced technologies as well as growing indigenous capabilities in controlled countries have made many export controls to such countries increasingly ineffective, if not irrelevant.

CONCLUSION
CONTROLLING THE UNCONTROLLABLE?

During the Cold War, the United States and its allies adopted a two-pronged strategy aimed at maintaining a quality edge of Western military equipment against Soviet quantitative preponderance through, on the one hand, major investments in military-related R&D (*leap ahead*) and, on the other, a national and multilateral system of export controls (*keep them behind*). In the post-Cold War era, the mutually reinforcing trends of the lack of a common security threat, a weaker multilateral framework governing export controls, and the globalization and commercialization of military-related technologies have significantly eroded the ability of states to control the transfer of dual-use technologies to potential adversaries. In the case of the United States, according to former Deputy Assistant Secretary of Defense and Senior Representative for Trade Security Policy Mitchell Wallerstein, dual-use export controls can today be effective only in a "limited number of situations – namely those in which the United States either is the sole supplier or enjoys overwhelming market dominance. Stealth technology,

[41] Vance A., 2010, "China Wrests Supercomputer Title From US," *The New York Times*, October 28. As of June 2011, Japan surpassed China and ranks first with a supercomputer capable of performing more than 8 quadrillion calculations per second (petaflop/s). For updates on the evolution of the ranking of the world's fastest supercomputers, see http://www.top500.org

very high-resolution satellites, and encryption software are among the few remaining areas in which the United States still enjoys such an advantage."[42] A major consequence of these evolutions is that in the post-Cold War era, the US and its allies can effectively rely on only one of the two pillars of their Cold War strategy (*leap ahead*). Furthermore, the fact that potential competitors have access to commercially-developed dual-use technology means that in order to outcompete their adversaries, it has become necessary for ministries of defense as well as for defense contractors to complement investments in R&D and production activities in military-related technologies with excelling at being the first to integrate advanced commercial technology into military systems.[43] The Cold War assumption that technology controls were a *conditio sine qua non* for maintaining military predominance *vis-à-vis* strategic competitors has collided with the geopolitical, economic and technological realities of the post-Cold War era.

This realization lies at the root of the current Obama administration's effort to reform US export controls. The review was initially inspired by the recommendations of the National Research Council report *Beyond Fortress America* (directed by former national security adviser Brent Scowcroft), which states that US export control system is "fundamentally broken" and is still rooted in what it labels a Cold War "Fortress America" mentality.[44] In August 2009, President Obama launched a broad-based interagency review (The President's Export Control Initiative) aimed at putting "higher fences around fewer items," that is on a narrowed down set of critical items that the US can effectively control (the precise content of which is still the subject of inter-agency negotiations).[45] Given the current acrimonious relations between the Executive Branch and Congress, the chances of this reform effort to succeed are all but certain. Nevertheless, the growing reliance of the US military on dual-use technologies, as well as the previously described evolutions at the multilateral, industrial and technological level, have brought to light the need to rethink the very nature of export controls in the post-Cold War era.

---

42 Wallerstein M., 2009, "Losing Controls: How US Export Restrictions Jeopardize National Security and Harm Competitiveness," *Foreign Affairs*, Vol. 88, No. 6, p. 18.

43 See National Research Council, 2002, *op. cit.*, p. 2.

44 National Research Council, 2009, *Beyond "Fortress America": National Security Controls on Science and Technology in a Globalized World*, p. 3.

45 Interview with a current senior official of the Department of State, July 2011. On the Congressional side, two bills have been introduced to reform the US export control regime: the Technology Security Act of 2011 (H.R. 2004), introduced by Representative Howard Berman (D-CA), and the Export Administration Renewal Act of 2011 (H.R. 2122), introduced by Representative Ileana Ros-Lehtinen (R- FL). For a description of the current export control reform effort, see Fergusson I., Kerr P., 2011, *The US Export Control System and the President's Reform Initiative*, Congressional Research Service, CRS Report for Congress R41916.