IV. Controls on intangible transfers of technology and additive manufacturing

MARK BROMLEY, KOLJA BROCKMANN AND GIOVANNA MALETTA

Controls on transfers of conventional arms and dual-use items apply not just to tangible transfers—that is movements of physical goods—but also intangible transfers of certain types of technology and software. These transfers, generally referred to as intangible transfers of technology (ITT), include the electronic or oral transfers of software, technical data, knowledge and technical assistance. Many of the physical items that are the subject of arms and dual-use export controls are far less useful to possess if the owner does not also have access to related software, technical data, knowledge or technical assistance. Controlling ITT is thus widely viewed as an essential component of a state's export control system. As a result, the main export control regimes, the controls of the European Union (EU), and United Nations and EU arms embargoes all include requirements to impose and enforce controls on different types of ITT. However, controls on ITT pose a particular set of problems, both for regulators when seeking to detect illicit transfers and for companies and research institutes when seeking to comply with regulations.

The difficulty of enforcement and compliance is only likely to grow. In particular, developments in areas such as cloud computing are increasing the volume of software and technical data that can be transferred electronically and raising difficult questions about if and when export controls should apply. Meanwhile, the greater ease with which individuals can travel internationally is making it harder to track and control in-person transfers of knowledge and technical assistance. Moreover, additive manufacturing (AM)—also known as 3D printing—has the potential to increase the range and complexity of controlled goods that can be produced based mostly on transferred software and technical data. AM also has the potential to change the skills and engineering expertise required compared to traditional manufacturing processes and to decrease the reliance on transfers of controlled goods. However, it is unlikely that the spread of AM will lead to a general deskilling of the production of arms and dual-use items.

During 2017 controls on ITT continued to be a major focus of discussion in the export control regimes and in the ongoing review of the EU Dual-use Regulation.[1] Within the export control regimes, states continued to try to establish common standards for the implementation of controls on ITT and examined if and how controls on AM machines and related software,

[1] Council Regulation (EC) no. 428/2009 of 5 May 2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items, *Official Journal of the European Union*, L 134, 29 May 2009.

technology and materials could be extended (see section III). In the EU, discussions focused on how to facilitate ITT that posed a reduced proliferation risk—such as transfers between different branches of the same company—and on establishing a clear and harmonized approach to how controls should apply to cloud computing. This section describes the main challenges associated with controls on ITT, the implications for non-proliferation efforts of developments in AM, and recent discussions about these issues within the export control regimes and the EU.

Intangible transfers of technology

Controls on ITT are required—using more or less uniform wording—by all four export control regimes: the Australia Group, the Missile Technology Control Regime (MTCR), the Nuclear Suppliers Group (NSG) and the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-use Goods and Technologies (Wassenaar Arrangement, WA).[2] For example, the WA controls technology and software that is required or designed for the development, production or use of a controlled item. In turn, it defines technology as consisting of both technical data (e.g. blueprints, plans, diagrams and models) and knowledge and technical assistance (e.g. instruction, skills, training, working knowledge and consulting services).[3] Each regime also specifies that certain types of technology and software are not controlled, particularly those 'in the public domain'.[4] Certain types of technology and software can be transferred using tangible means. For example, technical data can be included in published technical manuals and training materials or software can be loaded on to a CD-ROM or pre-installed on a computer and the physical items moved from one country to another. However, many transfers of technology and software take place through intangible means.

Intangible transfers of technical data and software

An intangible transfer of technical data and software, such as blueprints, schematics, diagrams or software, can take place via email, server upload or download, cloud computing or other Internet-based sharing platform. In addition to being subject to control because it is required or designed for the development, production or use of a controlled item, some types of technical

[2] Wassenaar Arrangement, 'List of dual-use goods and technologies and munitions list', WA-LIST (16) 1 Corr. 1, 17 Feb. 2017; Missile Technology Control Regime, 'Equipment, software and technology annex', 19 Oct. 2017; Nuclear Suppliers Group, 'Guidelines for nuclear transfers', annexed to IAEA document INFCIRC/254/Rev.13/Part 1, 8 Nov. 2016; Nuclear Suppliers Group, 'Guidelines for transfers of nuclear-related dual-use equipment, materials, software, and related technology', annexed to IAEA document INFCIRC/254/Rev. 10/Part 2, 8 Nov. 2016; and Australia Group, 'Australia Group common control lists', [n.d.].

[3] Wassenaar Arrangement (note 2), pp. 3, 227.

[4] E.g. Missile Technology Control Regime (note 2), p. 7.

data and software can also be subject to specific controls in their own right without reference to another controlled item. For example, systems that employ a certain standard of cryptography are controlled under category 5 of the Wassenaar Arrangement dual-use list.[5] These controls cover a vast array of tangible goods that employ a certain level of cryptography in their associated systems and that are produced in a diverse range of sectors, such as telecommunications, transport and energy.[6] However, they also include goods that can be transferred electronically—particularly different forms of computer software—that are used in banking, information technology (IT) security and other areas.

The application of export controls to cryptography has long been one of the most contentious and hotly contested areas of trade controls, particularly in the United States and the EU. In the 1970s and 1980s the application by the USA of export controls to cryptography led to the so-called crypto-wars. At the time, many in the information and communications technology (ICT) sector argued that the extension of export controls to cryptography harmed commercial competitiveness, was a violation of free speech and posed a threat to IT security.[7] In response, the USA progressively eased controls on exports of cryptography through the use of exemptions and 'open licences' that allow for multiple shipments under the same authorization.[8] However, many of these exemptions and open licences do not exist in the EU.

Controls on transfers of software have recently expanded to cover the trade in so-called cyber-surveillance systems. Cyber-surveillance technologies enable the monitoring and exploitation of data or content that is stored, processed or transferred via ICT, such as computers, mobile phones and telecommunications networks.[9] From 2012 onwards the WA and subsequently the EU expanded their dual-use export controls to cover a wider array of cyber-surveillance technologies. Many of the items covered—particularly mobile telecommunications interception equipment and internet protocol (IP) network surveillance systems—are tangible goods. However, intrusion software, which is used to remotely monitor computers and mobile phones and which became subject to control by the WA in 2013 (see section III), is

[5] Controls on such systems have been part of the Wassenaar Arrangement dual-use list since the 1990s. See Saper, N., 'International cryptography regulation and the global information economy', *Northwestern Journal of Technology and Intellectual Property*, vol. 11, no. 7 (fall 2013).

[6] European Commission, 'Impact assessment: Report on the EU export control policy review accompanying the document Proposal for a regulation of the European Parliament and of the Council setting up a Union regime for the control of exports, transfer, brokering, technical assistance and transit of dual-use items', Commission staff working document, Brussels, SWD(2016) 315 final, p. 34.

[7] Grimmett, J. J., *Encryption Export Controls*, Congressional Research Service (CRS) Report for Congress RL30273 (Library of Congress, CRS: Washington, DC, 11 Jan. 2001).

[8] Grimmett (note 7).

[9] See Bromley, M., Steenhoek, K. J., Halink, S. and Wijkstra, E., 'ICT surveillance systems: Trade policy and the application of human security concerns', *Strategic Trade Review*, vol. 2, no. 2 (spring 2016).

transferred electronically.[10] Moreover, many cyber-surveillance systems require almost constant software updates in order to remain undetected and to function effectively.[11]

The application of export controls to intangible transfers of technical data and software has long been difficult for regulators and companies. However, the difficulties have become increasingly acute as a result of the ever larger volumes of data that are routinely transmitted electronically during marketing, production and sales processes. A company working in one of the sectors that is subject to arms and dual-use export controls may transfer controlled technical data or software numerous times a day as it moves data around its different branches and between itself and other companies in a particular supply chain.[12] When the items involved are subject to arms or dual-use export controls, every stage in this process becomes potentially subject to licensing procedures.

The challenges are likely to become more acute—for both regulators and companies—with the expanding use of cloud computing for the streamlined storage and retrieval of data. Cloud computing, which emerged in the early 2000s, can be broadly defined as 'using shared rather than private local computing resources to store software or technology and handle applications', and those shared resources can be geographically distant from the user.[13] As the use of cloud computing increases the volume of transferred technical data, it creates compliance-related challenges for both regulators and companies. One particular problem is that, depending on the model used, data may end up being physically stored in multiple locations, some of which may be subject to export control restrictions. Another problem is determining who exactly is subject to export controls, particularly when—as is increasingly common—companies outsource the provision of cloud services to a third party.

The development of more streamlined and harmonized controls on transfers of technical data has emerged as a key focus of the ongoing review of the EU Dual-use Regulation.[14] A proposal published by the European Commission in September 2016 attempts to bring greater clarity to the application of ITT controls by specifying that controls should only apply when the technology is made available to 'legal and natural persons and partnerships'

[10] Bauer, S. and Mićić, I., 'Export controls regimes', *SIPRI Yearbook 2014*, pp. 471–72.

[11] Page, K., 'Six things we know from the latest FinFisher documents', Privacy International, 15 Aug. 2014.

[12] Bromley, M. and Bauer, S., *The Dual-Use Export Control Policy Review: Balancing Security, Trade and Academic Freedom in a Changing World*, Non-proliferation Papers no. 48, EU Non-proliferation Consortium, Mar. 2016.

[13] Tauwhare, R., 'Cloud computing and export controls', Tech UK, Feb. 2016.

[14] Council Regulation (EC) no. 428/2009 (note 1), Article 2.2(iii). On the review see Bauer, S. and Bromley, M., 'Developments in EU dual-use and arms trade controls', *SIPRI Yearbook 2017* pp. 622–26.

outside the EU, rather than simply 'a destination' outside the EU, as is currently the case.[15] It also proposes a new EU general export authorization for 'Intra-company transmission of software and technology'.[16] The intention of the new language is, in part, to 'facilitate the use of cloud services'.[17] However, Digital Europe, an industrial organization representing European digital technology companies, has argued that the language needs to be further clarified, particularly by 'deleting the element of "making available" . . . software and technology in electronic form'.[18] The concern appears to be that, even under the Commission's proposed language, it is the company providing cloud services that would be responsible for who downloads information, rather than just the user of the cloud services.

The review of the EU Dual-use Regulation has also created an opportunity to revisit debates about the application of export controls to cryptography. The Foreign Affairs Committee of the European Parliament emphasized in its opinion on the Commission's proposal that 'not every technology requires controls' and argued that 'exports of technologies that actually enhance human rights protection, such as encryption, should be facilitated'.[19] However, for the time being EU member states appear to be broadly in favour of retaining the existing controls on cryptography. One of the appeals of the existing controls appears to be that they enable governments to have oversight of—and the potential to control—technologies and systems that are not directly subject to export control but which are nonetheless of potential interest from a national security or human rights perspective. For example, before they were added to the Wassenaar Arrangement control list, exports of intrusion software and other cyber-surveillance systems were subject to export controls on the basis of the level of cryptography that they employ.[20]

Intangible transfers of knowledge and technical assistance

Transfers of knowledge and technical assistance can occur through a range of intangible means, including via academic courses in sensitive disciplines,

[15] European Commission, 'Proposal for a regulation of the European Parliament and of the Council setting up a Union regime for the control of exports, transfer, brokering, technical assistance and transit of dual-use items (recast)', COM(2016) 616 final, 28 Sep. 2016, p. 19.

[16] European Commission (note 15), p. 8.

[17] European Commission (note 15), p. 7.

[18] Digital Europe, 'European Commission proposed recast of the European export control regime: Making the rules fit for the digital world', Feb. 2017.

[19] European Parliament, Committee on Foreign Affairs, 'Opinion of the Committee on Foreign Affairs for the Committee on International Trade on the proposal for a regulation of the European Parliament and of the Council setting up a Union regime for the control of exports, transfer, brokering, technical assistance and transit of dual-use items (recast) (COM(2016)0616—C8-0393/2016—2016/0295(COD))', 2016/0295(COD), 31 May 2017, p. 3.

[20] 'British Government admits it has already started controlling exports of Gamma International's FinSpy', Privacy International, 9 Sep. 2012.

skills training and consulting services.[21] Activities aimed at the promotion of peaceful application of dual-use technologies (e.g. capacity building, national implementation assistance, training to respond to an attack or an incident involving hazardous materials) could also involve this type of in-person transfers of knowledge that might be used to develop, produce or make use of one of the items included in the control lists of the export control regimes.[22]

The language commonly used in most UN Security Council resolutions imposing arms embargoes also requires controls on technical assistance, mostly related to military activities or the provision, maintenance or use of arms and related materiel.[23] In the case of the Democratic People's Republic of Korea (DPRK, or North Korea), the UN Security Council specifically called on all UN member states 'to exercise vigilance and prevent specialized teaching or training of [North Korean] nationals within their territories or by their nationals, of disciplines which could contribute to [North Korea's] proliferation sensitive nuclear activities and the development of nuclear weapon delivery systems'.[24]

In the EU Dual-use Regulation, the definition of 'export' includes 'the oral transmission of technology when the technology is described over the telephone' to legal and natural persons and partnerships outside the EU.[25] Since the regulation forms part of the EU's common commercial policy, it cannot be used to regulate the cross-border movement of people. As a result, certain forms of 'in person' technical assistance are regulated separately by Council Joint Action 2000/401/CFSP.[26] However, the Joint Action only imposes controls on technical assistance provided outside the EU which is related to WMD, their related delivery mechanisms or military end-uses and provided in countries subject to EU, Organization for Security and Co-operation in Europe (OSCE) or UN arms embargoes.[27] Consequently, technical assistance and knowledge associated with other controlled dual-use items is left outside the scope of EU controls. This may change as the Commission's draft

[21] Rebolledo, V. G., *Intangible Transfers of Technology and Visa Screening in the European Union*, Non-proliferation Papers no. 13, EU Non-proliferation Consortium, Mar. 2012, p. 5.

[22] Hunger I. and Meier, O., 'Between Control and Cooperation: Dual-Use, Technology Transfers and the Non-Proliferation of Weapons of Mass Destruction', *Friedensforschung DSF,* no. 37, Deutschen Stiftung Friedensforschung (DSF), 2014, p. 11.

[23] E.g. UN Security Council Resolution 2216, 14 Apr. 2015, para. 14; and UN Security Council Resolution 2127, 5 Dec. 2013, para. 54.

[24] UN Security Council Resolution 1874, 12 June 2009, para. 28. See also UN Security Council Resolution 2270, 2 Mar. 2016, para. 17. The Security Council used the same language in Resolution 1737 on Iran, which was terminated on the implementation day of the Joint Comprehensive Plan of Action. UN Security Council Resolution 1737, 27 Dec. 2006, para. 17.

[25] Council Regulation (EC) no. 428/2009 (note 1), Article 2.2(iii).

[26] Council Joint Action of 22 June 2000 concerning the control of technical assistance related to certain military end-uses (2000/401/CFSP), *Official Journal of the European Union*, L 159, 30 June 2000.

[27] Council Joint Action (note 26).

revision of the EU Dual-use Regulation of September 2016 provides a legal definition of technical assistance and clarifies applicable controls.[28]

Another challenge in this field relates to transfers of knowledge or technical assistance that may occur through the arrival of a foreign citizen attending, for example, a university course or participating in an industry training programme. In the USA, this situation is covered by controls on 'deemed exports', which cover transfers of controlled technology to a foreign national.[29] In the EU this is covered by neither the Dual-use Regulation nor Joint Action 2000/401/CFSP on technical assistance, and so these legal instruments need to be complemented by other policies, such as visa policies.[30] Visa-screening mechanisms to grant short-term visas for the Schengen area (which largely overlaps with the EU) do not take into account concerns over the proliferation of weapons of mass destruction as they mainly address 'the risks of illegal immigration, terrorism and crime'.[31] Moreover, since 'long-term visas are an exclusive national competence in all EU member states, irrespective of their adherence to Schengen', controls may vary from one EU member state to the other, especially for schemes to vet foreign students.[32] For example, the United Kingdom uses the Academic Technology Approval Scheme (ATAS) to screen applications by postgraduate researchers from abroad for studies in potentially proliferation-sensitive fields.[33]

The application of controls on transfers of knowledge and technical assistance has always been difficult for regulators, companies and researchers. In particular, the provision of knowledge and technical assistance may involve the movement of people across borders carrying with them specific sensitive information in their minds. This makes it a cross-cutting issue where effective controls cannot simply be addressed by export controls, but may need to be complemented by other tools such as visa policies. For companies and research institutes, complying with controls can involve keeping track of individuals with knowledge of controlled technology and their nationalities, which can prove particularly hard.

[28] The legal basis of this possible extension in the scope of the regulation is the provision of the 2007 Lisbon Treaty, which makes 'the supply of technical assistance services involving a cross-border movement' an EU competence. European Commission (note 15), p. 13; and Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, signed 13 Dec. 2007, entered into force 1 Dec. 2009, *Official Journal of the European Union*, C 306, 17 Dec. 2007.

[29] US Department of Commerce, Bureau of Industry and Security, 'Guidance on reexports/transfers (in-country) of US-origin items or non-US-made items subject to the Export Administration Regulations (EAR)', 30 Oct. 2015.

[30] Rebolledo (note 21), p. 8.

[31] Rebolledo (note 21), p. 11.

[32] Rebolledo (note 21), p. 11.

[33] British Foreign and Commonwealth Office, 'Guidance: Academic Technology Approval Scheme (ATAS)', 3 Mar. 2017.

Additive manufacturing

AM describes certain types of manufacturing process that can form an object of practically any shape by depositing and bonding together successive layers of material. AM machines are capable of producing a variety of export-controlled items—ranging from basic small arms to key components of rocket engines—using such materials as polymers, metals or alloys.[34] Simple AM machines using polymers are often referred to as '3D printers' because of their similarity to common inkjet printers; but this term is insufficient to describe more advanced machines, particularly industrial-grade metal AM machines. AM technology has the potential to produce components required for nuclear weapons, uranium enrichment facilities, missiles and other conventional weapons. However, most of these sensitive applications are still in an experimental phase and the technology has not yet matured enough to realistically present a scenario in which an individual could simply push a button and be presented with a finished high-performance product.[35] Depending on the technology in question, additional finishing processes are often required in order to achieve key performance characteristics, such as the ability to withstand high mechanical stress. The need to specially engineer the designs for AM-produced objects may pose further hurdles for someone wishing to use these technologies to manufacture controlled items. Nonetheless, concerns have been raised about the impact of this technology on export controls and other non-proliferation efforts and the possible future impact of the technology in this area is a topic of active discussion.[36]

AM machines rely on digital build files to provide the information required to automatically produce an object of a certain shape and with certain performance characteristics. These build files can easily be transferred or made available using digital transfers, cloud computing or other types of file-sharing application. AM technology both uses intangible transfers and—by increasing the automation of manufacturing process that can be used in an attempt to bypass export controls and engage in proliferation-relevant activities—helps to reduce the knowledge barriers to producing controlled items.[37] These features of AM increase the benefit that an actor seeking to circumvent existing export controls can gain from exploiting the challenges

[34] Walther, G., 'Printing insecurity? The security implications of 3D-printing of weapons', *Science and Engineering Ethics*, vol. 21, no. 6 (Dec. 2015), pp. 1435–45; and Aerojet Rocketdyne, 'Aerojet Rocketdyne successfully tests engine made entirely with additive manufacturing', 23 June 2014.

[35] Kelley, R., *Is Three-dimensional (3D) Printing a Nuclear Proliferation Tool?*, Non-proliferation Papers no. 54, EU Non-proliferation Consortium, Feb. 2017.

[36] See Kroenig, M. and Volpe, T., '3-D printing the bomb? The nuclear nonproliferation challenge', *Washington Quarterly*, vol. 38, no. 3 (fall 2015), pp. 7–19; and Nelson, A., 'The truth about 3-D printing and nuclear proliferation', War on the Rocks, 14 Dec. 2015.

[37] Christopher, G., '3D printing: A challenge to nuclear export controls', *Strategic Trade Review*, vol. 1, no. 1 (autumn 2015), p. 18.

with controlling ITT.[38] Advances in AM thus illustrate the necessity of implementing effective controls on ITT.

AM has the potential to decentralize the production of export controlled goods. As the technology matures, the rate at which digital transfers replace transfers of goods in a product's supply chain is likely to increase.[39] By reducing the need to move controlled goods across borders, this trend will reduce the opportunities to subject a controlled item to checks and verification measures. These types of control may therefore become less effective as the opportunities to impose physical controls are reduced to transfers of AM machines and the feedstock that they use, such as special metal powders. National licensing authorities and the multilateral export control regimes have therefore considered how to apply or possibly expand existing export controls on goods and technology to address AM. For example, the 2016 MTCR plenary acknowledged that AM poses 'a major challenge to international export control efforts'.[40] In response, export controls could potentially be enhanced and expanded in three areas: (*a*) controls on the transfer of build files and other required technical data; (*b*) controls on the export of AM machines and their software; and (*c*) controls on the materials used in the AM process.

Controls on technology already cover transfers of build files if the item that the file describes is covered by export controls. However, the implementation of these controls varies between states, particularly in terms of the scope and complexity of information in the build files that triggers licensing requirements. No export control regime has yet produced guidance on how such controls should be enforced.

Similarly, no export control regime covers AM machines, with the exception of one specific type of production equipment in the Wassenaar Arrangement control list. However, some of the elements of AM machines, such as certain high-powered lasers, are covered by controls. Across the regimes a number of proposals have been made to include AM machines with certain dimensions and performance characteristics in the control lists, but they have all been rejected.[41] Introducing new controls may seem straightforward, and the introduction of controls on subtractive computer numerical controlled (CNC) machine tools has routinely been referred to as an example, but this example also demonstrates some of the challenges. These include

[38] Brockmann, K. and Bauer, S., '3D printing and missile technology controls', SIPRI Background Paper, Nov. 2017.

[39] Palmer, M., 'Ship a design, not a product! Is 3D printing a threat to export controls?', *WorldECR*, no. 43 (Sep. 2015), pp. 30–31.

[40] Missile Technology Control Regime, 'Public statement from the plenary meeting of the Missile Technology Control Regime (MTCR)', Busan, 21 Oct. 2016.

[41] Finck, R., French Secretariat-General for National Defence and Security, '3D printing', Presentation at the 20th Anniversary Practical Export Control Workshop of the Wassenaar Arrangement, 27–28 June 2016.

the potential problems of imposing controls on machines that are mainly used in the civilian field and the drawbacks of the various regimes' control lists using different metrics to define the machines subject to control.[42]

Moreover, no export control regime specifically controls materials designed for use as AM feedstock. The Wassenaar Arrangement dual-use control list covers a range of metals and alloys, some of them in powder form, but these are defined according to the specific chemical and physical properties required for other production processes and therefore only partly overlap with materials specially designed for use in AM. As AM feedstock is inherently dual-use, it will be difficult to impose new controls without affecting legitimate civilian uses. However, one possible way of expanding controls on AM feedstock is to limit new controls to powders with narrowly defined characteristics for use in high-performance metal printing.

Conclusions

The issue of how to formulate and implement effective controls on ITT is currently the subject of significant debate and discussion within the export control regimes and in the context of the review of the EU Dual-use Regulation. The fact that many of the companies and research institutes that rely on or use ITT are often operating on the cutting edge of their respective fields increases the proliferation-related risks but also strengthens the economic arguments against imposing burdensome regulations. The difficult nature of this balancing act is underscored by the extent to which effective implementation of controls on ITT relies on internal compliance and effective self-regulation by the companies and institutes involved. In particular, ITT occur in ways that leave no physical evidence. This makes it hard to prevent unauthorized transfers from taking place and to generate the evidence needed to demonstrate that controls have been violated.

In many cases, this is not necessarily a problem, since the non-proliferation concerns of regulators and the commercial confidentiality interests of companies often closely align. For example, when supplying technology to a foreign customer, many companies will have a commercial interest in ensuring that it reaches its intended destination and is not re-exported without permission. These goals would be shared by the company's national export licensing authority. The issues become more difficult when the interests of the licensing authority and the company or research institute in question do not align. For example, companies have limited commercial interest in maintaining detailed records of the cross-border movement of technology if it is passing between locations that are under its ownership and control.

[42] Brockmann and Bauer (note 38).

However, export licensing authorities may require the company or research institute to keep records of these movements.

More challenging is the fact that ITT bring within the scope of export controls some sectors and actors that have limited experience of these controls or where traditional methods of work are most at odds with established practices in this area. Tensions with the ICT sector with regards to cryptography indicate that export controls are unlikely—on their own—to be able to solve the proliferation-related problems that states want to address. Moreover, developments in AM and other emerging technologies look set to transform traditional models of trade and production in ways that may pose additional challenges to state-based export control frameworks. Expanding the dialogue between the export control regimes about approaches to ITT and AM would help them to develop more coordinated controls.[43]

[43] Brockmann and Bauer (note 38).