

Appendix 12A. Transfers of digital communications system technology

IAN ANTHONY

I. Introduction

Any armed forces which acquire an effective and secure communications system will have enhanced their military capabilities very significantly. The USA and its allies are currently investing large sums of money in developing new and more effective communications systems. However, it is unlikely that any monopoly over such systems could be defended indefinitely.¹ The number of countries which are interested to acquire such systems is growing. According to the Ministry of Post and Telecommunications in China, engineers are constructing a 'rapid combat system' based primarily on 'satellite communications, and secondarily on mobile land receiving stations, digital microwave and remote-controlled switching systems and other such emergency components. This network will include 200 000 kilometers of high-grade fiber-optic cable, 50 000 kilometers of microwave transmission cable and 156 land-based receiving stations.'² Communications systems specially designed or adapted for military use are subject to export controls in most if not all countries where they are produced. However, to extend export controls over civilian products with potential military applications, three conditions have to be met.

1. There has to be a problem of national security that is sufficiently important to justify action.
2. The security benefits derived from controls must outweigh the economic and political costs involved in introducing them.
3. There must be a characteristic of the market or product which makes controls feasible.

II. An overview of the market for military and civilian telecommunications

One trend within both civilian and military market sectors is the move from analogue systems to digital systems. Both systems transmit information via waves. However,

¹ In this context a secure system means communication with minimal risk of either a technical breakdown in the system or the interception and reading of traffic. For a survey of recent investments in digital communications by the armed forces in North America and Western Europe, see 'The digital battlefield', Supplement to *Defense News*, Sep. 1995.

² Cited in 'Modern weapons enter production: PLA better equipped', *Inside China Mainland*, Jan. 1996, pp. 37–38. In 1995 the United States Defense Science Board concluded that future adversaries of the USA are unlikely to attempt to acquire major combat systems 'because they can't compete with us on tactical aircraft or stealthy submarines or stealthy aircraft. What do they buy? They buy information for information warfare, weapons of mass destruction and the capability to hide much of what they have'. White, J., 'The compelling case for modernization', *Defense Issues*, vol. 10, no. 89 (18 Sep. 1995). URL <<http://www.dtic.dla.mil:80/defenselink/pubs/di95/di1089.html>>.

2 NON-PROLIFERATION, ARMS CONTROL, DISARMAMENT, 1995

digital systems construct waves by converting information into binary language, the language of computers. Analogue systems, on the other hand, use vibration to modulate sound waves. The message is carried by reinterpreting the precise modulation of the wave. Although both digital and analogue systems can transmit not just sound but also pictures and text, digital systems are generally acknowledged to offer higher quality and greater reliability in transmission. Moreover, digital signals make it easier to exchange information between machines that in the past were separate—telephones, televisions and monitors, telefaxes and computers. This appendix is concerned only with digital systems.

Conventional cables or optical fibres carry the bulk of data and voice traffic in a national telephone system. Data and voice traffic can also be carried via satellites in microwave transmissions.³

In the future, land-mobile systems are expected to carry a higher percentage of the traffic. While digital land-mobile radio systems are generally contained among a specific group of users, digital mobile telephone systems have mostly been developed in collaboration with national telecommunications companies and depend on national telephone networks to carry a major part of the traffic. The emergence of satellite-borne cellular networks (such as the Iridium system based on 66 low-earth orbit satellites and other similar planned systems) may at some later date allow a global telecommunications system to compete with national networks.

Telecommunications systems that have characteristics normally associated with military applications can have civilian applications. For example, civilian police forces, trucking companies and taxi firms may use communications systems that have some features in common with military land-mobile radios. In the reverse case, it would be necessary to license telecommunications equipment and technologies that were developed entirely with civilian use in mind if such equipment could meet military needs or were sold to a military user.

The market for civilian telecommunications can be divided into two sectors: equipment suppliers and equipment operators. In the past, operators have mostly been state-owned monopolies. However, the structure of this market is beginning to change and is expected to change further. Equipment operators (i.e., providers of network services) need not own physical assets (such as cables, optical fibres or switches) but may be private companies that manage networks on behalf of the customer, which may still be a state-owned utility. Managing and operating equipment is a much larger economic activity than equipment supply, accounting for perhaps 90 per cent of total telecommunications sales. Most recent developments in digital telecommunications have been market driven and the market for civilian equipment is much larger than that for military equipment. Moreover, while the global military market is not growing, many observers anticipate significant future growth in the civilian market.

The fact that this civilian market is still very dynamic has meant that the outcome of discussions currently under way about technical standards for civilian digital telecommunications is having an impact on military systems. Martin Libicki has observed that in the absence of agreed technical standards an integrated system is reduced to a series of 'islands of connectivity' that raise costs and reduce flexibility

³ Satellites can offer a supplement to terrestrial civilian telephone networks but they are not an alternative. For example, using satellites would not be practical in heavily populated, built-up areas. Digital telecommunications satellites and the technologies central to their development are of great interest to military users. These satellites are also subject to export controls in many of the countries which produce them, although new producers—e.g., Brazil, Israel and South Africa—are emerging.

and ease of use.⁴ It is therefore likely that national and international standards will be developed (either by administrative decision or by decisions in the marketplace). Agreement on regulations affecting trade in the telecommunications sector is an important objective of the World Trade Organization (WTO) in 1996.⁵

Some of the most important customers for military equipment—notably the USA—have conceded the need for civilian markets to drive technology development in the future. Emmett Paige, Assistant Secretary for Defense for Command, Control, Communications and Intelligence, has observed that in building its future global command and control system the USA will reject proprietary systems even if they seem cost effective at the time of initial purchase. According to Paige, ‘we have learned our lesson—standardize the interfaces, using commercial standards whenever possible . . . so the component software (and hardware) systems can rapidly evolve and be integrated into a stable matrix of interoperable systems’.⁶

Whereas governments are likely to play an important role in negotiating and delivering major items of military equipment, the international trade in civilian technologies with potential military applications is more likely to be conducted by industry. From a supplier perspective, the market for telecommunications is dominated by a small number of companies in North America and Western Europe. For major systems the most important companies are Alcatel-Alsthom (France), Ericsson (Sweden), GEC-Plessey (UK), Motorola (USA), Northern Telecom (Canada) and Siemens (Germany). Other companies have a powerful position in specific sub-systems. For example, Nokia (Finland) provides handsets for mobile digital systems. At first sight, a market that is dominated on the supply side by a small number of companies located in industrialized countries should not create major difficulties to export control. However, significant barriers do exist.

Factors complicating export control

It would be of concern to industry if governments established regulations restricting international trade in telecommunications products and services on national security grounds.

Apart from the fact that the market is very large, telecommunications are recognized to be an important element in other economic activities. If export controls prevented the development of telecommunications infrastructure, networks and services for civilian purposes, they would significantly reduce the efficiency of economic activity in general.⁷ In addition, telecommunications companies tend to make a high investment in research and development (R&D) and can legitimately claim to be among the ‘technology drivers’ within their national economies. Therefore, the issue

⁴ Libicki, M., ‘Standards: the rough road to the common byte’. URL <<http://www.ndu.edu:80/ndu/inss/actpubs/act001/ai.html>>.

⁵ ‘Brittan sees bright future for US–EU partnership’, *Wireless File* (United States Information Service, US Embassy: Stockholm, 2 Nov. 1995), p. 6.

⁶ Paige, E., ‘Retaining the edge on current and future battlefields’, *Defense Issues*, vol. 10 no. 85 (22 Aug. 1995). URL <<http://www.dtic.dla.mil:80/defenseink/pubs/di95/di1085.html>>. The UK has taken a similar decision. Miller, D., ‘Rationalizing telecommunications: the British DFTS’, *Jane’s International Defense Review*, Jan. 1996, p. 35. For a discussion of national regulations in the USA, see Crandall, R. W., ‘Waves of the future’, *Brookings Review*, winter 1996, pp. 26–29.

⁷ UNCTAD Ad Hoc Working Group on Trade Efficiency, Draft Guidelines on Key Sectors for Trade Efficiency: Telecommunications, UNCTAD document TD/B/WG.2/11/Add.5 (Geneva, 2 May 1994). Apart from the reduction in economic activity, the market for civil telecommunications is regarded as a key growth area both by equipment manufacturers and by systems operators.

4 NON-PROLIFERATION, ARMS CONTROL, DISARMAMENT, 1995

of whether the costs of export controls outweigh the benefits is a very significant one for both suppliers and recipients. The political costs of technology denial are also likely to be high because a country that cannot acquire an efficient telecommunications system is likely to be disadvantaged in many ways.

The structure and certain aspects of the telecommunications market also raise questions about the feasibility of designing controls that can be effective without being a major barrier to legitimate civilian trade.

Companies that supply integrated systems tend to have a high dependence on materials and technologies that they buy from other countries and also a high dependence on sales outside the country in which they are incorporated. They also tend to be highly international in their organization with many subsidiary companies in other countries responsible for production, marketing and distribution of products.

By definition, telecommunications puts a high premium on systems. Telecommunications equipment suppliers not only provide larger customers with many individual items of equipment but also integrate that equipment into a system. The capacity for systems integration is regarded as an important product. It is likely that the supplying company and the recipient (probably a state-owned operator) will have to cooperate at many levels and for some time during and after installation.⁸ Moreover, to ensure that the equipment works properly and that a buyer is trained to use it effectively some human exchanges and training will be required. It is very unlikely that an operator can use equipment effectively if only written documentation is transferred.⁹ Moreover, as noted above, providing network services is also becoming a major business activity. As one observer has noted, 'if networks become "non-excludable" international public goods, then it is likely that the backward linkage into digital telecommunications technologies will also become more difficult to regulate'.¹⁰

In some of the largest potential new markets for digital communications—notably in Central and Eastern Europe and in parts of Asia—market access is likely to be conditional on at least a degree of transfer of technology and know-how. This may include not only technology related to equipment manufacturing but also systems integration skills.

As a result, export controls can only be effective if the telecommunications industry cooperates in implementation. No single country or group of companies has yet established an unassailable position either as a source of universally accepted technological standards or in market share. In this environment the competition between countries and companies is fierce and the incentives to open new markets are great. Nevertheless, the companies which dominate the market for digital telecommunications all adopt policies of full cooperation in export control. Although the fastest growing markets for advanced telecommunications products and services are outside North America and Western Europe, these are still by far the largest and most important markets. While acts of illegality by individual employees are always possible,

⁸ As noted above, the market for operating telecommunications systems is also beginning to change. In future it is likely that private companies will have a larger role in managing and operating civilian telecommunications networks.

⁹ The same arguments apply in market sectors such as computer hardware and software. Harvey, J. *et al.*, *A Common-Sense Approach to High Technology Export Control* (Center for International Security and Arms Control, Stanford University: Stanford, Calif., Mar. 1995); and Goodman, S., Wolcott, P. and Burkhart, G., *Building on the Basics: An Examination of High-performance Computing Export Control Policy in the 1990s* (Center for International Security and Arms Control, Stanford University: Stanford, Calif., Nov. 1995).

¹⁰ David Mussington, RAND Corporation, personal communication with the author, 26 Jan. 1996.

evading laws and regulations in force in Canada, the USA or the EU would not be a worthwhile general policy for any large company. As the Swedish company Ericsson has noted, 'such activities could result in export sanctions, including fines and denial of export privileges, against the employer involved, their company and possibly the Ericsson Group as a whole. Such sanctions could seriously affect not only the company's or operating unit's ability to obtain foreign-controlled technology, and to pursue export opportunities, but could also have far-reaching negative effects on the entire Ericsson Group'.¹¹

After assessing these factors, the European Union has decided to implement licensing procedures for telecommunications equipment. Category 5, 'telecommunications and information security', of the EU Regulation, which entered into force on 1 July 1995, lists those items that require an export licence before leaving the territory of the European Union. The category includes communications systems that employ digital technology and includes both mobile and fixed systems. While the category includes both digital radios and telephones, in the framework of the EU Regulation land-mobile radios are subject to stricter controls than telephones. Under the regulation 'portable (personal) radiotelephones for civil use, e.g. for use with commercial civil cellular radio-communications systems, containing encryption, when accompanying their users' are explicitly exempted from control.¹² For company licensing practices, this makes it necessary to determine whether or not a customer is a civilian end-user.

III. Similarities and differences in civilian and military telecommunications technology

Military command and control has traditionally been divided into strategic, tactical and unit levels. Strategic command systems usually involve communication between fixed sites or bases. This communication between bases can be (and in many countries is) an integrated part of the national telephone network, although there are usually special arrangements (such as the installation of redundant lines) to adapt the civilian system for military use. Tactical and unit-level military communications are more likely to be based on mobile systems.

The military applications of mobile, portable radios have long been acknowledged. However, the coordination of battlefield initiatives and the transmission of a stream of data about enemy activities have become progressively more important. Historically, most advanced industrial countries have pursued dedicated military R&D programmes to provide increasingly sophisticated communications systems to their armed forces.

Technology development is permitting the command and control hierarchy to be reorganized. The US, Canadian and many European armed forces are investing in new digital communications systems organized as networks within which information processed at higher levels of command can be passed directly to field commanders and vice versa. As these systems are introduced, military communications systems

¹¹ 'Ericsson internal export control procedures', Unpublished manuscript, Ericsson, Stockholm, 6 Nov. 1995. For similar points of view from other suppliers, see Ebata, K., 'Report on Japanese dual-use export controls: background, policy and prospects', Unpublished manuscript, Oct. 1995, pp. 22-24; and *The Export Control Manager* (Department of Trade and Industry: London, 1995).

¹² 'Council Decision of 19 December on the joint action adopted by the Council on the basis of Article J.3 of the Treaty on European Union concerning the control of exports of dual-use goods', *Official Journal of the European Communities*, vol. 37 (31 Dec. 1994).

should reflect what is considered to be optimal from a command perspective rather than what is technically possible.

To operate on the battlefield, communications systems must have certain characteristics not previously expected in civilian systems. The system must have a minimal failure rate and be easy to repair, maintain and support. The system must be 'user friendly' in its operation so that all members of a unit and not just specialists can quickly learn how to operate it. A military communications system must continue to function when one or more of its parts are disabled or malfunctioning and it must be able to withstand efforts to jam or disrupt signals. The messages transmitted must be secure—through encryption or frequency hopping—in ways that make it difficult or impossible for an enemy to read them.¹³ Military systems tend to require a very high level of physical durability or 'ruggedness'.¹⁴

Differences between military and civilian user requirements are becoming progressively fewer. Business users increasingly require enhanced security and there is growing interest in providing telecommunications services to civilian users in remote locations—where the costs of laying a terrestrial network of cables or optical fibres would be great. In these cases the requirements for a rugged civilian digital communications system could be as demanding as those in the military area.

Military users have become interested in taking advantage of commercial technologies and networks in cases where this could save them the cost and necessity of building parallel systems. In October 1995, US Admiral William Owens observed that by the year 2000 in the civilian area 'the data rate of communications [will go] up not by 10 per cent or by 20 per cent but by 20,000 times. Ten thousand times more data will be able to be exchanged. It is possible for the military to take good advantage of that, plug into that fiber optic network'.¹⁵

In addressing some manufacturing problems the civilian sector has also found solutions which appear to be superior to those adopted in specialist military programmes. For example, factory tests by Motorola in the USA suggest that the failure rate of micro-electronic components produced in the civilian facilities operated by the company are many times lower than in dedicated military production facilities.¹⁶

The convergence has not all occurred because of changes in civilian demand. The nature of military demand has also changed. Traditionally military establishments have stockpiled components to reduce their vulnerability to cut-offs in supply. Military establishments have also insisted on a high degree of independent capacity to repair and maintain the systems they operate. Under budget pressures both practices are being re-examined and closer collaboration with manufacturers and private service providers is a likely future trend.

¹³ Harbor, B., *Technological Divergence in the Development of Military and Civil Communications Systems: The Case of Ptarmigan and System X* (Centre for Information and Communication Technologies, University of Sussex: Falmer, July 1989).

¹⁴ According to its military specification, a US military radio must survive being dropped onto a concrete floor from a height of 1 metre and a 'splash test' using a water jet with a pressure of 2 kg per square centimetre.

¹⁵ 'Czech PFP exercise provides U.S. with good lessons', *Wireless File (Europe)* (United States Information Agency: Washington, DC, 12 Oct. 1995). URL <gopher://pubgopher.srce.hr:70/00/usis/casopisi/wf/European%20WF%20.12.10.95>.

¹⁶ This is attributed to the different regulatory environment for civilian and military production. In particular, it is suggested that technical specifications which must be followed if goods are to be sold to the military cannot keep pace with the rate of improvement being introduced in civilian products under pressure of market competition. Gansler, J., 'Transforming the US defence industrial base', *Survival*, vol. 35, no. 4 (winter 1993/94), pp. 135–36.

The escalating costs of R&D are also likely to make it more difficult for producer countries to support parallel military and civilian digital telecommunications programmes insulated from one another. In particular in areas such as switching systems and network development there are likely to be pressures for sharing R&D costs and perhaps also the costs of maintaining and operating telecommunications networks.

Civilian telephone networks require fully automatic and very powerful switching systems to handle the high and increasing volume of traffic. While peacetime traffic within a military network is much lower than in a civilian counterpart, the escalating need for rapid exchanges of large amounts of information during high intensity military operations also requires a high capacity for switching and traffic management.¹⁷ However, the specific nature of the demand is different. Civilian traffic consists of very large numbers of people sending messages through the system at random and the switching systems are designed to cope with this pattern of use. Military communications may require that a single message be transmitted to many recipients simultaneously or in a very short period of time. If the information cannot be transmitted rapidly then it may be of little or no use to the recipient. In this respect military communications are more similar to information broadcasting than civilian telephone communication.

IV. Summary and implications

This discussion suggests that, under economic and technological cross-pressures, some of the boundaries dividing military and civilian research, development, production and deployment in the area of digital telecommunications are becoming increasingly difficult to draw. It also suggests that this is most true at the level of components and certain individual manufactured goods. At the level of integrated systems, there are some more important differences between specific military and civilian requirements. However, military and civilian users share a growing need for skills that allow them to construct and manage complex telecommunications networks.

Close cooperation between buyer and seller is a normal practice in the area of civilian telecommunications. Therefore, it would be difficult for a recipient to conceal military applications. However, it is possible that skills learned from constructing and managing civil networks could be applied in the military sphere. For smaller items—such as handsets—which can be sold to operators, retail outlets or to other agents, it is technically much more difficult to monitor and control their transfer or use. However, because they are only a small part of a system, they cannot provide any useful capability to the recipient on their own.

It is also true that a purely civilian digital communications system could be of some military value. Against an advanced adversary this value would not be very high because key elements of even mobile networks—such as cellular base stations—are fixed and their location is known. Therefore they would be vulnerable to destruction or jamming. A civilian system could give greater military capabilities where a potential adversary did not have the capability to disrupt or destroy the system. Because of the limited range over which civilian cellular networks operate, such a communications system would mostly be of value to forces operating on their own national territory.

¹⁷ For example, the transfer of digital maps and digital images to forward units requires a very high capacity.

8 NON-PROLIFERATION, ARMS CONTROL, DISARMAMENT, 1995

The use of civilian mobile telecommunications by the military in these circumstances would be a lesser concern than their use by terrorists or non-state military forces. However, this would be a different kind of problem from those considered in this chapter.

Although it is not likely that a company could unknowingly provide a major communications system to an unauthorized user, there could nevertheless be cases where the need for licensing creates problems for a company. Such cases occur, for example, where the military owns or operates civil communications networks or companies in the buyer country. In some countries the military is also tasked with assisting in economic and technological development. Licensing problems can then arise where a ministry of defence or the armed forces own and operate manufacturing facilities that make products for both military and civilian markets. This is the case in, for example, China and some Latin American countries.

In these cases, sales could be to a military end-user even if the products are intended for civilian end-use and, without assurances and information from the buyer, it could be difficult for a supplier to receive authority to export. In cases involving transfers of production technology, the regulation of retransfers—the sale to third parties of products produced under a license agreement—will also become an important issue.

To operate successfully it is in the interest of telecommunications companies to comply with all the laws and regulations in all the countries where they operate. Therefore, because of their international structure, most major telecommunications companies have to invest a significant amount in developing and implementing export control compliance procedures. While a general framework for control procedures can be developed for the whole company, it is necessary for each subsidiary to tailor its procedures to the national regulations in force in the country where it is operating. Virtually all the major telecommunications companies either operate in the USA or import some parts, software or technical data of US origin.

These items may have to be licensed under US export law after they are incorporated into other products. Therefore, more than one set of export control procedures will often apply to certain advanced telecommunications equipment. The EU Regulation on export of dual-use goods has not removed the need to monitor national export regulations even in the European context as individual member states are still free to exert additional national controls if they choose.¹⁸

¹⁸ 'Ericsson internal export control procedures' (note 11).