Piotr Sieńko
Maria Curie-Skłodowska University, Lublin, Poland

Methods of securing and controlling critical infrastructure assets allocated in information and communications technology sector companies in leading European Union countries

Introduction

Resources of strategic importance for national security have always been protected and controlled in a comprehensive manner. Whenever they became allocated in economic entities, these entities were also subject to close supervision.

As global economic systems changed – in the case of the socialist bloc, these changes consisted of moving away from a centrally planned economy and adopting free-market solutions – so-called State-Owned Enterprises (SOE) – were commercialized and underwent a gradual process of ownership transformations. The ultimate effect of these changes was partial or total privatization.

Enterprises with a strategic status, as well as enterprises whose assets included strategic resources, were largely also subject to transformation, often motivated by the need to increase competitiveness under free market conditions. The central authorities could not lose control over these assets, as this would negatively affect national security. Furthermore, they had to make even greater efforts to ensure that the strategic assets which had become partially released from state jurisdiction and, in the new reality, were generating profits for the benefit of public or private co-owners, would continue to serve the general good of the state and its society, simultaneously guaranteeing an appropriate level of security in the field of their operation.

In short, after subjecting strategic entities to "free market conditions", it was the state's duty to ensure that it would retain the ability to protect and control those entities to a sufficient extent, in order to maintain their importance and role in the national security system. The significance of these entities for public safety and public order remained the core objective of their functioning, although the commercial activity of

DOI: 10.5604/18984509.1210263 ISSN: 1898-4509 ISSN: 2449-7436 online pdf

privatized enterprises naturally "obscured" their true significance or sometimes even predominated over it.

At the turn of the 21st century, a number of highly dynamic changes occurred in the field of national security. This was caused by the emergence of new threats, such as terrorism, mass disasters and catastrophes, as well as the very real danger of cyber-attacks, which threatened not only states and their societies, but also economic entities operating in the fields/sectors considered crucial from the point of view of national security.

Thus, even more attention began to be devoted to all issues related to the control and protection of strategic assets allocated in economic entities. Basic concepts were redefined in order to create or clarify new catalogues of dangers, as well as methods of their eradication, prevention or possible countermeasures, among other things. The fields which required special protection and control also underwent precise redefinition. This was reflected in the most important documents and legal acts in many countries. Strategies, plans and instructions began to be prepared in order to provide plans for the protection and control of crucial assets.

For example, in the United Kingdom 10 areas were defined as strategic sectors. They were named in the following order:

1) communications,
2) emergency services,
3) energy,
4) financial services,
5) food,
6) government and public safety management,
7) health,
8) public safety,
9) transport,
10) ensuring drinking water supply (*The national infrastructure*).

There is a reason why communications and telecommunications systems (i.e. the ICT sector) were listed first. As many government documents emphasize, communications and telecommunications systems help control and manage the 9 remaining sectors. Thus, if these systems cease to function properly, in modern times this automatically paralyses the functioning of sectors which are equally important for the state and its citizens, but which occupy lower positions on the list. Any disruption of the functioning

of these systems would result in a significant threat to the British economy, social order and, in consequence, to the political order as well.

The National Security Strategy of the United Kingdom, published in 2010, emphasizes the importance of telecommunication in ensuring an adequate level of national security in the United Kingdom. It contains the following words: "In particular, protecting virtual assets and networks, on which our economy and way of life now depend, becomes as important as directly protecting physical assets and lives" (*A Strong Britain in an Age of Uncertainty: The National Security Strategy* 2010, p. 26).

Redefinition of strategic assets in EU legislation

To improve control over strategic assets located on EU territory and to increase their security, Brussels has also carried out the necessary legal changes in this field. In EU legislation, implemented in Poland as well, these assets are described as Critical infrastructure (CI). This term was defined in the Council Directive 2008/114/EC of 8 December 2008, published on 23 December 2008, on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.

Critical infrastructure (CI) was defined as "an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions" (Council Directive 2008/114/EC 2008, p. 77).

This directive names the energy and transport systems of EU member states, including systems for electricity generation and transmission and systems for production, processing, storage and transportation of energy resources, as crucial CI sectors[1].

Item 5 of the directive indicates the "need to include other sectors within its scope, *inter alia*, the information and communication technology ('ICT') sector". Article 3(3) mentions the particular importance of the ICT sector (Information and Communication Technologies) for maintaining security in a state of emergency (e.g. during terrorist attacks, natural disasters and catastrophes). It also mentions that "subsequent sectors to

[1] Item 7 of this directive mentions, among other things, that the disruption or destruction of Critical Infrastructure on EU territory would have serious consequences because of interdependencies between interconnected critical infrastructures of EU member states. Hence, European critical infrastructure (ECI) "should be identified and designated by means of a common procedure".

be used for the purpose of implementing this Directive may be identified. Priority shall be given to the ICT sector".

One of the provisions of this directive obliges EU member states to create Operator Security Plans (OSP) to protect critical infrastructure. These plans include all elements and systems of European Critical Infrastructure. Poland did not fulfil this obligation until 2013 (*Narodowy Program Ochrony Infrastruktury Krytycznej* 2013; *Przygotowanie systemu ochrony ludności przed klęskami żywiołowymi oraz sytuacjami kryzysowymi* 2013)

Knowing the possible consequences of dangers associated with the loss of control over key entities in strategic sectors, and aware of the need for their adequate protection, highly developed EU countries began to safeguard these entities, mostly in three parallel ways:

1) by introducing relevant acts and regulations defining critical state assets, as well as obligatory forms of their control and protection,
2) by exerting ownership control over strategic assets allocated in key economic entities,
3) by ensuring comprehensive counterintelligence protection of entities in which elements of strategic state assets are allocated.

Given the thematic scope of this paper, only the first two points listed above will be discussed in detail in its latter part. The third point is merely touched upon by listing the most important institutions responsible for the protection and control of strategic assets in the discussed countries. The article focuses on the telecommunications sector, which was chosen because of its impact on the functioning of other areas (energy, crisis management, the financial sector, rescue services, national defence).

Protection of telecommunications infrastructure in the Federal Republic of Germany

In Germany, responsibility for the protection of CI rests upon the Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik – BSI), answerable to the Federal Ministry of the Interior (Bundesministerium des Innern – BMI). In its official documents, this office indicates the dependence of all CI sectors on the effectiveness of security measures applied to entities from the ICT sector.

This pertains to the following sectors: transport (aviation, shipping, railways, transport, postal services); energy (nuclear, electric, gas, oil); hazardous materials (chem-

ical industry, biomaterials, arms industry); finance and banking (banks, insurance, financial services, stock exchange); crisis management and basic social needs (healthcare, rescue services, disaster monitoring systems, water and food supply, waste disposal); public administration (government, government agencies, administration, security and state authorities, Federal Armed Forces).

The leading economic entity associated with critical infrastructure in Germany's ICT sector is Deutsche Telekom AG (DT). The Federal Government possesses 14.5% of this corporation's shares (DT comprises such entities as the network operator T-Mobile, which includes Polish Digital Telephony (Polska Telefonia Cyfrowa) S.A. – T-Mobile Polska, formerly Era GSM). Another stake in DT (17.4%) is controlled by the German government through the KfW (Kreditanstalt für Wiederaufbau) bank, all of the shareholders of which are state institutions. 80% of the shares of that bank belong to the Federal Republic of Germany. The remaining 20% belong to German federal states. The bank's management board, comprising five members, is answerable to the Supervisory Board, led personally by the minister of economics and technology in the Federal Government. This gives state institutions the certainty that their decisions regarding issues related to all aspects of the corporation's functioning will in fact be implemented. (*KfW receives new shares in the course of Deutsche Telekom AG's scrip dividend* 2013) Thus, the Federal Republic indirectly and directly owns 32% of the shares of DT AG; in other words, it is the largest and most influential shareholder in the company (*Annual Report 2010*, p. 41)

Wishing to avoid the interference of EU institutions (especially of the European Commission) which oppose the excessive influence of member states on the sphere of control over economic entities, the German government has avoided direct legal provisions referring to this issue. However, in accordance with German law, the Federal Ministry for Economic Affairs and Energy (formerly the Federal Ministry of Economics and Technology, and earlier, the Federal Ministry for Economics and Labour) is responsible "for the telecommunications sector, including, among other things, telecommunication security, public interests and planning for emergency situations" (*Telecommunication security, public interest, contingency planning – OECD Reviews of Regulatory Reform. Regulatory Reform in Germany* 2004, p. 13).

In 2004, during a review of the regulatory reform of telecommunications, a provision was placed in British legislation stating that the government authorities consider that the dominant entity on the market has a duty to share links (with operators that enter the market) "except when there is a need to maintain network security" (ibidem,

p. 32). Following the British example (discussed below), this gave government institutions a legal instrument enabling them to control and influence economic entities. This happens when the actions of their boards are contrary to the national interest in matters of IT security.

The first analyses regarding CI protection were prepared in the BRD as early as 2003-2004 (Analysis of Critical Infrastructures – The ACIS methodology – Analysis of Critical Infrastructural Sectors – 2004). In 2005, the Federal Government adopted the National Plan for Information Infrastructure Protection (*Nationaler Plan zum Schutz der Informationsinfrastrukturen* – NPSI), while the Federal Ministry of the Interior adopted the Baseline Security Strategy for the Protection of Critical Infrastructures (Bundesamt für Sicherheit in der Informationstechnik (BSI)[2] (*Nationaler Plan zum Schutz der Informationsinfrastrukturen* 2005).

In 2007, a supporting document for the NPSI was adopted – the Critical Infrastructure Protection Implementation Plan (Umsetzungsplan KRITIS – UP KRITIS). Ca. 30 operators and other entities functioning in the field of information infrastructure participated in its creation and realization. In parallel, another CIP implementation plan (Umsetzungsplan Bund – UP Bund), dedicated for the federal administration, was also adopted Bundesamt für Sicherheit in der Informationstechnik.

This document names not only telecommunications infrastructure, information technologies or the arms industry as CI; this label is also given to media and buildings that are important for social reasons, as well as historical monuments (sic!). However, ICT infrastructure security is given the highest priority (ibidem).

In 2009, as the culmination of several years' work on security of CI systems, the National Strategy for Critical Infrastructure Protection was adopted. In accordance with this strategy, the state regulates the means for protecting the entire national system, along with security measures and the procedures for that area. It functions as a moderator (coordinating activities in the fields of business, industry, state administration etc.) and when necessary, it creates legal regulations that address these issues. (*National Strategy for Critical Infrastructure Protection* 2009)

Telecommunications service providers are subject to the legal regulations mentioned above and it is their duty to protect telecommunications and information systems in

[2] The NPSI states that information infrastructure may possibly become the target of an attack of organized crime groups or terrorists. Its protection is a key priority in the BRD's politics of national security. The most critical scenario of such actions could lead to the breakdown of the entire information system, causing significant damage to the economy. Implementing the Plan will make Germany a much more attractive location for entities conducting their business (*Nationaler Plan zum Schutz der Informationsinfrastrukturen* 2005).

Germany from unauthorized access. Furthermore, telecommunications system operators are obliged to provide a specially established Federal Network Agency with safety concepts that define possible dangers. It is also their duty to demonstrate the technical precautions or other protective measures that have been taken or their implementation is planned to ensure the security of the given system.

In the Federal Republic of Germany, the following units of public administration are responsible for infrastructure protection: Federal Ministry for Economic Affairs and Energy (Bundesministerium für Wirtschaft und Energie – BMWi), Federal Ministry of the Interior (Bundesministerium des Innern – BMI), Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik – BSI), Federal Network Agency (Bundesnetzagentur – BNetzA), Federal Ministry of Justice (Bundesministerium der Justiz – BMJ), Federal Ministry of Defence (Bundesministerium der Verteidigung – BMVg), Federal Intelligence Service (Bundesnachrichtendienst – BND), Federal Office for the Protection of the Constitution (Bundesamt für Verfassungsschutz – BfV).

Critical infrastructure of the ICT sector in France

The national telecommunications operator in France is Orange (formerly the France Télécom Group). Until 2004, this company was fully state-owned. As a result of privatization, the state reduced its stake in the group and now indirectly controls 26.99% of the company's shares (Orange is also the majority shareholder of Polish companies: the former TP S.A. and indirectly, through shares of TP S.A., the former PTK Centertel, which now operate in Poland under the Orange brand).

The French government exerts control over Orange through majority ownership of the company"s shares, split between:

- the Government of France – 13.24%
- the French state enterprise ERAP (Entreprise de Recherches et d'Activités Pétrolières) – 0.24%
- the Strategic Investment Fund (Fonds Stratégique d'Investissement) – 13.50%

The Strategic Investment Fund is a sovereign wealth fund created in order to safeguard the capital of strategic French enterprises. It promotes the development of companies with a high innovative potential. The FSI's co-owners are: the state Deposits and Consignments Fund (Caisse des Dépôts 51%), controlled by the parliament, and the French Treasury (Trésor public) (49%) (*France – Fonds Stratégique d'Investissement* 2009).

With 26.99% shares in Orange, the French government is able to effectively control the company's strategic assets. It influences the decisions of its organs, as well as processes carried out in subsidiary companies. Moreover, no other shareholder in the company, with the exception of the French government and the FSI, may directly or indirectly own a larger stake in the operator than 5%. The same regulation pertains to voting rights arising from shares held (*2009 registration document France Telecom. Annual Financial Report* 2009).

According to the Act of 30 October 1935 on the standardization of forms of control, the Orange Board of Directors must include representatives of the French government. Their number must be proportional to the amount of shares in the company held by the state. In 2009, the French Treasury had three representatives from the total number of 15 board members (*Décret-loi du 30 octobre 1935 unifiant le droit en matière de chèques et relatif aux cartes de paiement* 1935).

Due to the small number of other shareholders usually taking part in the General Meeting, the Government of France, as the main shareholder (in agreement with the FSI) can make decisions concerning the company by a simple majority of votes (*2009 registration document France Telecom. Annual Financial Report* 2009).

Among the legal acts that ensure information security in France is also the Act of 10 July 1991 on correspondence sent by electronic means (Blocman 2000), which states that the French prime minister may authorize the interception of electronic communications for purposes of national security or to protect elements that are essential for the scientific or economic activities of France (Loi No. 91-646, 1991).

Legal restrictions also apply to investments in the sectors of telecommunications, media and technology, which in certain circumstances may be treated by the authorities as investments made in strategic sectors.

Thus, in accordance with Art. L151-1 and following of the Financial and Money Law, any investor from outside of France planning to invest in a strategic sector is required to apply for a formal permit from the Ministry of Economy of France. Transactions made before such a permit is issued have no legal force, and the deed is punishable by imprisonment for 5 years and a fine equivalent to twice the value of the transaction (*System kontroli strategicznych podmiotów sektora ICT we Francji* 2011).

In 2014, these provisions were tightened by a special decree of the French president, Francois Hollande. Besides telecommunications, the list of sectors requiring permission from the state now also includes energy, transport, healthcare and services related to water supply (Kublik 2014).

As the Minister of Finance Michel Sapin explained in an interview with French media, this decree plays a "fundamental role" in "protecting the strategic interests of France" (*Patriotisme économique: le décret Montebourg divise* 2014).

Among the state institutions that supervise French strategic entities in the telecommunications sector, the following deserve a mention:

(i) the General Directorate for Internal Security – Direction Centrale du Renseignement Intérieur (DCRI), a French counterintelligence agency,
(ii) the Regulatory Authority for Electronic Communications and Postal Services – Autorité de Régulation des Communications Électroniques et des Postes (ARCEP),
(iii) the French national competition regulator – Autorité de la concurrence (FCA).

Protection of telecommunications infrastructure in the United Kingdom

The British telecommunications market is composed almost solely of public entities. The privatization process in this country began on 19 July 1982, when the government officially informed about the intention to commercialize and privatize the national telecommunications operator, British Telecom. Thanks to the Telecommunications Act adopted in 1984, in November of that year over 50% of BT shares were sold in the public offering. However, the privatization process was not completed until July 1993 (Telecommunications Act 1984).

BT remains the largest telecommunications service provider in the UK, although it has lost monopoly and is now forced to operate under free market conditions. Henceforth, all entities that received the necessary operational license could operate within its framework[3] (*About Oftel* 2014).

Additionally, in 2001 BT was forced to split off the wireless operator O2, which was later purchased by the Spanish telecommunications company Telefónica (*British Telecom Group Annual Report & Form 20-F*, 2010, p. 150).

The ownership structure of the BT Group PLC is dispersed, and consists of 137 groups of the largest shareholders, including 98 institutions and 39 funds (data from the turn of 2012).

[3] Until 2003, these licenses were issued by Oftel, the government agency that supervised the telecommunications sector.

BT continues to control the largest telecommunications network in the UK. The owner of the fixed telephony network (based on copper links) is a spin-off company, Openreach. 50% of the shares in the British telecommunications market belong to Virgin Media[4].

As one of the largest operators in the country, BT provides services for government institutions. They are the largest and most important partners of the British Telecom Group in the United Kingdom (*British Telecom Group Annual Report & Form 20-F*, 2010, p. 48).

Although as a result of the privatization process the United Kingdom theoretically gave up the right of disposal of the assets of BT, in fact it still maintains informal control over the Group. It achieves this by using the shareholding structure of the company, which is deliberately dispersed and divided among a group of other entities, indirectly controlled by the UK government. Institutional investors who hold BT shares exercise authority in the company in a collective manner (during the General Meeting they form ad hoc coalitions and make decisions in line with British state interests). This method guarantees that London is able to maintain almost complete control over the operator (Kirchmaier 2004).

Another effective means for protecting the state against uncontrolled acquisition of BT is the so-called mandatory offer. In accordance with the provisions of the UK Code on Takeovers and Mergers, any shareholder in a given company who intends to acquire more than 30% of voting rights arising from shares held must make a mandatory offer to purchase the remaining shares of the company at the last trading price (Telecommunications Act 1984).

While the British government is not a formal owner of BT, it guarantees teleinformatic safety both for itself and for the citizens. This is achieved, in part, by skilfully steering the flow of money. Funds are channelled into BT and similar entities

[4] Virgin Media and BT are investing in the new generation of fiber-optic networks. Over the last decade, entities from the telecommunications market in the UK have made significant modernization investments, upgrading existing networks in order to adapt them to constantly evolving technologies. Funds were also invested in backbone networks. Data from the Infrastructure department of Her Majesty's Treasury, which deals specifically with the supervision of the level of technical advancement of the state's critical infrastructure in investments, coordinating investments made in order to expand and modernize that infrastructure and financing of these types of investments, just within 5 years (2005-2010) 150 billion pounds were invested in the UK into projects related to infrastructure expansion. 24% of these funds (35 billion pounds) was spent on investments in the telecommunications sector. It is expected that until 2030, investments into the UK's infrastructure will amount to 40-50 billion pounds per year. Of all the investments planned for the years 2010/11-2014/15 (total value – ca. 195 billion pounds), 17% – 34 billion pounds went to the telecommunications sector. (Strategy for National Infrastructure 2010; National Infrastructure Plan 2013).

e.g. in order to carry out investments inspired by the government or as payment for services provided by the operator to state institutions. The system is supplemented by legal regulations that impose various duties and restrictions on BT and other, similar entities. These duties and restrictions regulate, among other things, the functioning of strategic entities and the qualities of services which these entities provide to the state.

In the UK, the Telecommunications Act of 2003 remains the main legal act that contains regulations regarding the general framework for the functioning of a free telecommunications market, freedom of competition and equality of access to services. In accordance with the provisions of this Act and the Civil Contingencies Act of 2004, BT is designated by the state as the entity responsible for the provision and delivery of specified telecommunications services to government institutions. The BT group is also obliged to participate in the planning of telecommunication regulations, as well as in creating crisis management plans, e.g. for the purpose of disaster relief and restoring services suspended or interrupted as a result of disasters or catastrophes. UK authorities also put a similar legal obligation on other, smaller operators (Telecommunications Act 2003: sec. 51(1)(e) to 5.4; Civil Contingencies Act 2004).

These entities are obliged to cooperate with the relevant ministries and other state institutions. The above-mentioned operators are also on the list of entities belonging to the so-called Responsibility Category 2. Apart from BT, this category also includes: Affiniti, Cable & Wireless, COLT, Global Crossing, 3 Mobile, Kingston Communications, Level 3, NTL, O2, Orange, T-Mobile, Telewest, Thus, Vodafone Mobile, Verizon Business. These entities are legally required to cooperate with government institutions on the creation of the *National Emergency Plan for the UK Telecommunications Industry* (2011). They are additionally obliged to activities of this sort by bilateral agreements signed with the government. According to those agreements, telecommunications service providers have the right to exchange their human and material resources in emergency situations without the danger of losing sensitive data relating to the internal affairs of each entity.

Additionally, the Secretary of State acquired the right to give telecommunications operators specific directions pertaining to national security and international affairs related to the interests of the United Kingdom (or even relations with a "country outside the United Kingdom"). Normally the minister is required by law to lay a copy of every such direction before the Parliament, but in certain situations, for security reasons, he is allowed to refrain from this (Telecommunication Act 1984: sec. 94). The Secretary of State can also withhold the right of selected operators to provide services,

if it appears necessary to do so in the interests of public safety or national security of the UK (ibidem: sec 132).

Such action is in line with Art. 3 of Directive 2002/20/EC of the European Parliament and of the Council of 7 March 2002 on the authorisation of electronic communications networks and services and is associated with the possibility of exerting the rights of a Member State (Treaty on European Union 2007: art. 46 (1)).

Complying with the provisions of EU law, the UK authorities are responsible for supervising entities with a special market position known as "significant market power (SMP)". According to EU directives, this label applies to enterprises whose market share exceeds 25 percent. This control applies mainly to areas such as the availability of ICT infrastructure for emergency services (*Telecommunications Networks – a vital part of the Critical National Infrastructure* 2011).

Among the state institutions that oversee the telecommunications companies which are essential elements of CI, the following deserve a mention:

(i) Department of Infrastructure of Her Majesty's Treasury,
(ii) Ofcom – a government agency which implements the provisions of the Communications Act of 2003,
(iii) The Department for Business, Innovation and Skills (BIS) – a government department responsible for activity coordination between government agencies and private entities which manage critical infrastructure,
(iv) the Centre for the Protection of National Infrastructure (CPNI) – an interdepartmental centre for CI protection,
(V) the Government Communications Headquarters (GCHQ).

Summary

Leading EU member states clearly understand the role played by the teleinformatic sector of Critical Infrastructure in the system of national security. Thus, they protect and control strategic assets allocated in the economic entities that operate in this sector. They maintain a dominant position in the ownership structures of those enterprises (Germany, France) or, like the United Kingdom, they exert control in an indirect manner, through the votes of dispersed institutional shareholders. The activity of these entities is also regulated by numerous legal provisions which increase the state's control over them.

None of the states described above have opted to give up legal, institutional or ownership control over ICT sector entities. Some states, e.g. France, have actually increased their powers in this field in recent times, granting themselves the exclusive right to make decisions regarding mergers and acquisitions in strategic sectors.

Literature

2009 registration document France Telecom. Annual Financial Report (2009), France Telecom, http://www.orange.com/en/content/download/3111/36938/version/2/file/2009RegistrationdocumentFranceTelecomGroup.pdf

2012 registration document France Telecom-Orange (2013), France Telecom, http://www.orange.com/en/content/download/12506/259365/version/2/file/2012%20Registration%20Document.pdf

*About Oftel (*2014), http://www.ofcom.org.uk/static/archive/oftel/about/index.htm

Annual Report 2010, Deutsche Telekom AG, https://www.telekom.com/static/-/12172/2/110225-ar10-pdf-si

Blocman A. (2000), *E-mail Protected by Privacy of Correspondence*, IRIS Legal Observations of the European Audiovisual Observatory. IRIS 2000-10:9/17, http://merlin.obs.coe.int/iris/2000/10/article17.en.html

British Telecom Group Annual Report & Form 20-F (2010), https://www.btplc.com/Sharesandperformance/Annualreportandreview/pdf/BTGroupAnnualReport2010.pdf

Civil Contingencies Act (2004), Act of the Parliament of the United Kingdom, http://www.legislation.gov.uk/ukpga/2004/36/contents

Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, OJ L 345, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32008L0114

Décret-loi du 30 octobre 1935 unifiant le droit en matière de chèques et relatif aux cartes de paiement (1935), http://www.legifrance.gouv.fr/affichTexte.do;jsessionid=4E292DB84A7E82469050D450EF2F9416.tpdjo16v_2?cidTexte=LEGITEXT000006072897&idArticle=&dateTexte=20131210

Dekret Prezesa Rady Ministrów dot. technicznych zasad tworzenia, przekazywania, przechowywania, powielania i reprodukcji walidacji, nawet tymczasowo,

dokumentów elektronicznych [Decree of the President of the Council of Ministers concerning the technical principles of the production, transmission, storage, duplication and reproduction of validation, even temporarily, of electronic documents], 13.01.2004, http://www.altalex.com/index.php?idnot=7212 after: *System kontroli strategicznych podmiotów sektora ICT we Włoszech (Materiał poglądowy)* (2011), Instytut Strategii Polskiej, Warszawa

France – Fonds Stratégique d'Investissement (2009), Les Fonds Souverains, http://www.fondssouverains.com/pages/France_Fonds_Strategique_dInvestissement_FSI-994599.html

Heath D. (2009), *The electronic communication sector response to emergencies*, "UK Journal of the Institute of Telecommunications Professionals" Vol. 3, Part 4

KfW receives new shares in the course of Deutsche Telekom AG's scrip dividend (2013), https://www.kfw.de/KfW-Group/Newsroom/Aktuelles/News/News-Details_134528.html

Kirchmaier T. (2004), *Who governs? Corporate Ownership and Control Structures in Europe*, Jeremy Grant Graduate Institute of International Studies, Interdisciplinary Institute of Management LSE, Genova

Kublik A. (2014), *Rząd Francji broni swoje firmy przed cudzoziemcami*, http://wyborcza.biz/biznes/1,100896,15970541,Rzad_Francji_broni_swoje_firmy_przed_cudzoziemcami.html

Loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des communications électroniques, http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000006077780&dateTexte=20110915

Loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des communications électroniques, http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000006077780&dateTexte=20110915

Narodowy Program Ochrony Infrastruktury Krytycznej (2013), Rządowe Centrum Bezpieczeństwa, http://rcb.gov.pl/wp-content/uploads/NPOIK-dokument-główny.pdf

The National Emergency Plan for the UK Telecommunications Industry (2011), HM Government, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/61807/emergency-plan-telecomms-sector.pdf

The national infrastructure, Centre for the Protection of National Infrastructure, http://www.cpni.gov.uk/about/cni/

National Infrastructure Plan (2010), HM Treasury and Infrastructure UK, http://www.hm-treasury.gov.uk/ppp_national_infrastructure_plan.htm

National Infrastructure Plan 2013 (2013), HM Treasury, Infrastructure UK, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/263159/national_infrastructure_plan_2013.pdf

National Strategy for Critical Infrastructure Protection (2009), BSI, http://www.bsi.bund.de

Nationaler Plan zum Schutz der Informationsinfrastrukturen (2005), BMI, http://www.bmi.bund.de/cae/servlet/contentblob/121734/publicationFile/13577/Nationaler_Plan_Schutz_Informationsinfrastrukturen.pdf

Patriotisme économique: le décret Montebourg divise (2014), "Le Parisien", http://www.leparisien.fr/economie/investissements-etrangers-sapin-defend-un-decret-protecteur-pour-la-france-15-05-2014-3842759.php

Przygotowanie systemu ochrony ludności przed klęskami żywiołowymi oraz sytuacjami kryzysowymi (2013), Informacja o wynikach kontroli, KPB-4114-01-0/2012, Nr ewid. 148/2013/I/12/006/KPB, Najwyższa Izba Kontroli, Warszawa, https://www.nik.gov.pl/plik/id,5308,vp,6885.pdf

Recommendations for critical information infrastructure protection (2012), BSI, https://www.bsi.bund.de/EN/Topics/Criticalinfrastructures/criticalinfrastructures_node.html

Strategy for National Infrastructure (2010), HM Treasury, Infrastructure UK, http://www.direct.gov.uk/prod_consum_dg/groups/dg_digitalassets/@dg/@en/documents/digitalasset/dg_186451.pdf

A Strong Britain in an Age of Uncertainty: The National Security Strategy (2010), HM Government, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/61936/national-security-strategy.pdf

System kontroli strategicznych podmiotów sektora ICT we Francji (Materiał poglądowy) (2011), Instytut Strategii Polskiej, Warszawa

Telecommunication security, public interest, contingency planning – OECD Reviews of Regulatory Reform. Regulatory Reform in Germany (2004), OECD, https://www.oecd.org/regreform/32408088.pdf

Telecommunications Act (1984), Act of the Parliament of the United Kingdom, http://www.legislation.gov.uk/ukpga/1984/12/contents

Telecommunications Act (2003), Act of the Parliament of the United Kingdom, http://www.legislation.gov.uk/ukpga/2003/21/contents

Telecommunications Networks – a vital part of the Critical National Infrastructure (2011), Ofcom,

Treaty on European Union (2007), Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union, Official Journal C 326, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A12012M%2FTXT

Piotr Sieńko

Methods of securing and controlling critical infrastructure assets allocated in information and communications technology sector companies in leading European Union countries

Critical Infrastructure (CI) plays a significant role in maintaining public order and national security. The state may use many different methods to protect and control CI allocated to commercial companies. This article describes the three most important ones: legislation, ownership and government institutions and agencies. The data presented in this paper is the result of research done on the most developed countries in the EU (United Kingdom, France, Germany and Italy) and their strategic enterprises in the ICT sector, one of the most important sectors in any national security system.

Keywords – *information and communications technology, critical infrastructure, national security*

E-mail contact to the Author: sienko13@gmail.com