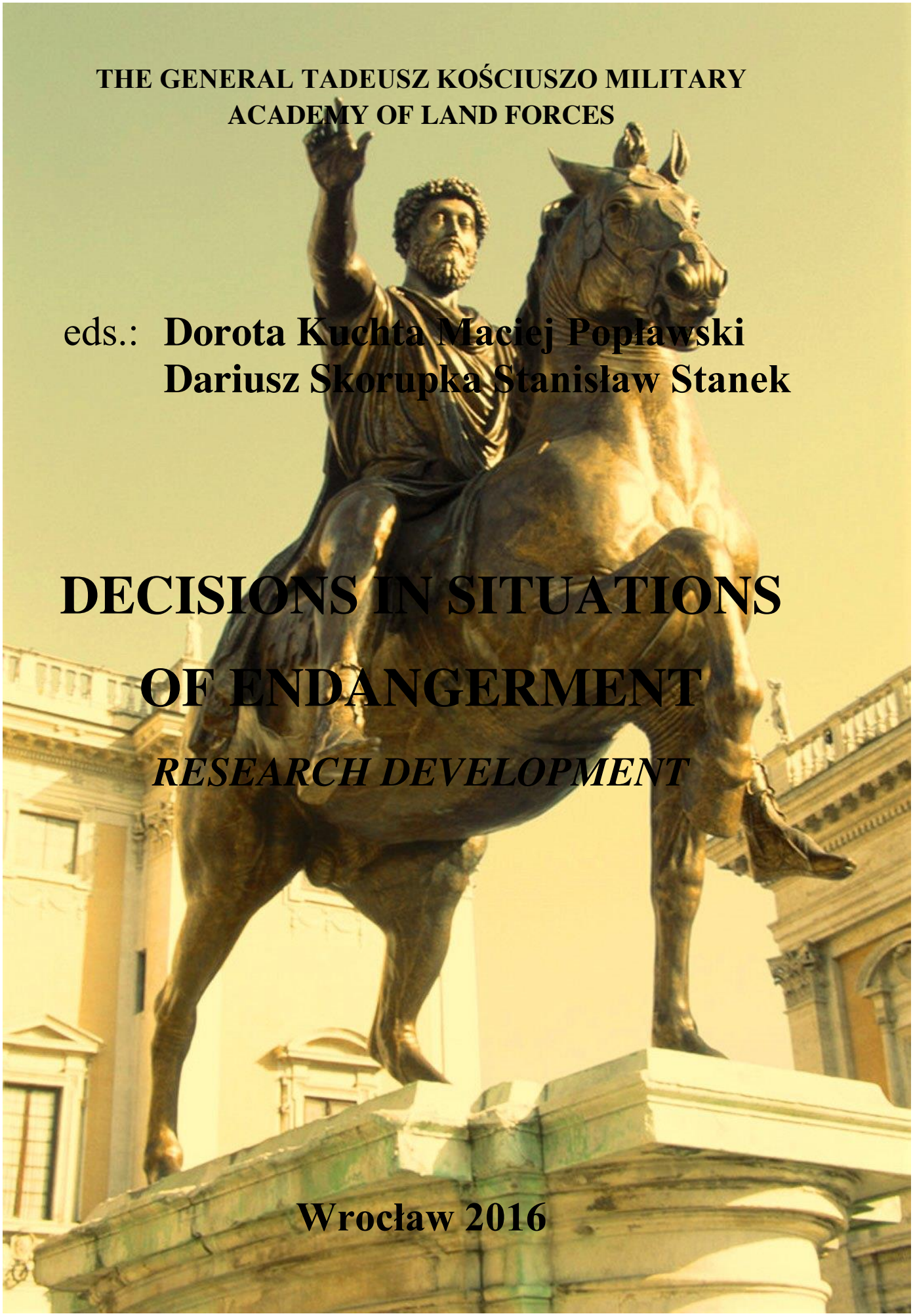
THE GENERAL TADEUSZ KOŚCIUSZO MILITARY
ACADEMY OF LAND FORCES



eds.: **Dorota Kuchta Maciej Popławski**
Dariusz Skorupka Stanisław Stanek

DECISIONS IN SITUATIONS OF ENDANGERMENT

RESEARCH DEVELOPMENT

Wrocław 2016

CRITICAL REVIEW
Tomasz SMAL
Marek WRÓBLEWSKI

CORRECTION
Maciej POPŁAWSKI

FRONT COVER PROJECT
Stanisław STANEK
Maciej POPŁAWSKI

TECHNICAL EDITION
Maciej POPŁAWSKI
Magdalena GOLONKA

The monograph has been published within the research and development work using the investment:
Decision suport in the situations of endangerment /ID: 230996/

ISBN 978 – 83 – 65422 – 30 - 9

The internal MALF signature: 196 /2016

Edition: 20 pieces
Affiliation: The Faculty of Management, MALF

Printing and binding: Copyright by Publishing House of the General Tadeusz Kościuszo Military Academy of Land Forces, order nr. 497/2016

3.2. Service continuity of critical energy systems in the light of present legal experience (by Grzegorz Blicharz, Tomasz Kisielewicz)

Grzegorz Blicharz [*], Tomasz Kisielewicz [**]

[*] *Jagiellonian University in Kraków, Faculty of Law and Administration*
e-mail: grzegorz.blicharz@uj.edu.pl

[**] *Warsaw University of Technology, Faculty of Electrical Engineering,*
e-mail: t.kisielewicz@ee.pw.edu.pl

Abstract

The paper represents an interdisciplinary approach on service continuity of critical infrastructure (CI). The legal and technological arguments are taken into account with aim to illustrate crucial points of this aspect. The need to protect critical systems infrastructure is quite natural when we accept state security standpoint. In the recent years world leaders saw the need to protect such structures as gas, power, water and tele-communications networks. Protection is based on two pillars, the first is law and the second is technology. In both areas the development depends on the cooperation on the international level and it is the effect of the technological and legal experience. Security of energy critical infrastructure however is a challenge not only for institutions but also for legal and technological concepts. Firstly, state interest has to deal with private owners of CI. In fact, legal solutions has to be analyzed with much broader perspective within European legal experience. The paper will analyze how far and why the state should be responsible for the maintenance and protection of CI. Thus, the legal strategies towards CI are compared with the ideas of Elinor Ostrom's governing the commons as way to find an effective solution. Secondly, on the technological level, the governing of CI is analyzed in the context of setting technical standards and recommendations. International and national standardization bodies are responsible for resolving safety and security problems. In that respect certain types of energy recommendations will be taken into account. The paper opens the discussion on the interconnectedness between technological and legal spheres and the importance of effective cooperation between them for CI security.

Keywords: law, critical infrastructure, governing the commons

1. Introduction

A line between what is public and what is private becomes less visible in crucial situations. Without doubt this reflection moves us directly to legal considerations. The origin of our understanding what belongs to private law and to public law lies in the Antiquity. Our Roman predecessors, namely Roman jurist Ulpian, taught us that private law deals with the benefit of individuals (*utilitas*), whereas public law with the matters of commonwealth[362]. Indeed, then and today, the division is not a clear one. What remains valid is the criterion of differentiation used by Ulpian – *utilitas* – utility. The inevitable tension between private interest and public demand can be easily noticed in the case of securing indispensable critical systems and services. Among them energy infrastructure is one of the most important one. The comparative and interdisciplinary perspective of legal

[362] Digesta, *Corpus Iuris Civilis*, vol. I, ed. Krüger P., Berolini 1954 (further: D.), D. 1,1,1,1

experience and energy engineering lead us to the common good and self-responsible community as driving concepts in the decision making process regarding critical infrastructure.

Nowadays „critical infrastructure" (CI) refers to a wide spectrum of systems, buildings, and services[363]. It is legislator who decides what will be covered by the legal definition of this term. What is to be a pure private enterprise today, tomorrow can be claimed critical infrastructure[364]. Thus, it immediately would start to be of great interest of the state and public law. In general critical infrastructure is defined as object, device, installation, service that is a part of a larger system and that is so vital for societal and economic life that any damage to it or lack of capacity can cause severe consequences for nation's economy, security, and health[365]. In the case of critical energy infrastructure the typical examples of CI are: power plants, energy, petrol or natural gas transmission systems, and distributors thereof. No matter when and where, energy supply and production was always treated as a crucial system for maintaining community and public order. In the case of critical energy systems we do now face problems and threats not only because of possible physical or cyber-attacks on the infrastructure but even due to natural conditions: extremely high temperatures, drought, and so on[366]. In the legal perspective no proper answer can be given to the question how to provide service continuity of critical energy systems without considering the state-citizen relations. From the technological point of view, the issue deals with the level of development of the elements of the infrastructure and with cooperation between many different entities located also outside one state extending to the interdependent international energy system[367]. The paper seeks to point out to the core problems of protecting critical energy infrastructure and to reveal ways of solving them. It applies both legal and technological point of view to present and analyze ways of dealing with the security of critical energy systems. We do believe that not only „who" but also „how" the CI will be protected remains an inevitable issue.

[363] Filiol E., Gallais C., *Critical Infrastructure: Where we Stand Today*, Proceedings of the International Conference on Information Warfare & Security; 2014, p. 47-57
[364] Vijayan J., *Obama executive order redefines critical infrastructure*, Computerworld | Feb 14, 2013
[365] Moteff J., Parfomak P., *Critical Infrastructure and Key Assets: Definition and Iden-tification*, CRS Report for Congress 2004
[366] Polskie Sieci Energetyczne, *Komunikat z dnia 10 sierpnia 2015 r. w sprawie wystąpienia zagrożenia bezpieczeństwa dostaw energii elektrycznej, podjętych działaniach i środkach w celu usunięcia zagrożenia i zapobieżenia jego negatywnym skutkom oraz o wprowadzeniu ograniczeń w dostarczaniu i poborze energii elektrycznej na polecenie OSP*.
[367] Luiff E., Klaver M., *Critical infrastructure awareness required by civil emergency planning*, IEEE Workshop on Critical Infrastructure Protection, IEEE, 2005

2. CI – types of ownership and models of governance

The idea of a state-governed security program contains the presumption that private owners of critical infrastructure either are not interested enough in investing too much in their protection systems, or they are not able to protect themselves enough against new types of threats like cyber-attacks. Thus, modern regulations are following the idea that nowadays critical energy infrastructure can be protected against any attack or any damage only thanks to a centralized decision making process which requires an ongoing sharing of information between all holders of critical infrastructure[368]. Opportunities to attack CI are so great that there is a need for centralized governing that will enable the state to have a broad picture of what is going on in the entire state. The idea is: the more information the state will gather the better protection there will be.

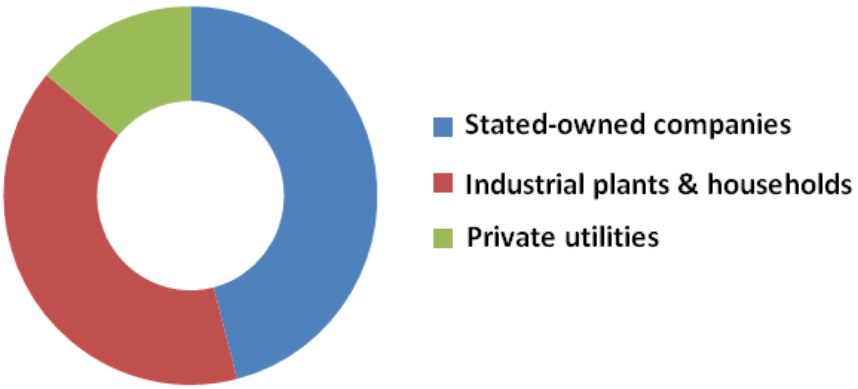
One shall consider how far and why the state should be responsible for the maintenance and protection of CI. Some conclusions can be obtained from the comparison of policy of three countries: USA, Poland, and Germany. If we talk about critical infrastructure the tension between private and public sphere is always to be considered. Not surprisingly, nowadays main part of the entire critical infrastructure belongs to private owners. In the USA they amounts to over 85% of the holders of CI – it is owned by them, operated or a combination thereof[369]. In Poland private owners are responsible for a significant part of CI. In Germany, however, CI is more broadly owned, operated and influenced by the state.

In the USA there are private companies that own power plants both coal-fired and nuclear ones. In Poland, like in the USA there are power plants that are in private hands. Power Plant in Pątnów, Adamów and Konin in which majority of shares belongs to a private owner. It produces 8,5% of national power capacity and it amounts to 2512 megawatts[370]. In Germany energy critical infrastructure is based on the unbundling policy of the European Union. Nevertheless, the division of energy market does not necessarily reveals the structure of ownership of CI. In fact the market is divided between four big companies which were divided by the state regulator: EnBW, E.ON, RWE, Vattenfall. However, they usually use under the special agreements utilities that are owned by municipalities[371]. Even in the EU policy towards vertical independence between participants of energy systems, remains valid the question about cooperation between private and public owners. The great influence of private and public ownership of energy and combination thereof is presented by the worldwide power capacity structure in the Figure 2. It

[368] Rządowe Centrum Bezpieczeństwa: *Program narodowy ochrony infrastruktury krytycznej*, Warszawa, 2013
[369] President Obama's *Executive Order 13636*, February 12, 2013
[370] http://zepak.com.pl/pl/, access: 11.05.2016
[371] Bayer E., *Report on the German power system*, Version 1.0. Study commissioned by Agora Energiewende., RAP 2015 NIPP 2013, *Partnering for Critical Infrastructure Security and Resilience*, US Homeland Security 2013

shows how inevitable is to ask about model of governing that will join the state structure with the private interest.

Figure 2. Ownership of Worldwide Capacity of Energy Power Plants



Source: own elaboration on the base of Energy Outlook Investment Report 2014: OECD/IEA 2014 London, 3 June 2014

The property regime of CI does influence the type of governance that should be conducted so as to provide service continuity of energy systems. On the example of the policy of those three countries one can distinguish two ways of providing the needed protection. In July 2015 Germany has promulgated the critical infrastructure cybersecurity regulation which deals also with the critical energy infrastructure. Energy companies are forced to introduce cyber security measures within two years, if not they must pay fines up to €100,000[372]. It is the first cybersecurity regulation in the world that is enforceable by economic penalty.

In the USA in 2013 has been introduced a set of new regulations dealing with CI[373]. There has been established a new definition of CI and has been approved ongoing model of cooperation between state and private energy companies. The national program of CI protection in Poland formulated two years ago is following the idea of cooperation while it avoids the reward-penalty model[374]. The crux of the matter is to encourage private owners to be up to date with the newest measures of security especially of cyber security. It is to be done by constant information sharing groups. Participation in them should be considered prestigious: they together should feel responsible for the nation security and nation prosperity. The similar regulations in the USA and in Poland oblige federal administration in the USA or governmental ministers in Poland to provide communication network, set up meetings and create the atmosphere of working together for the common good –

[372] IT-Sicherheitsgesetz Nr. 31 vom 24.07.2015, §14 (2)
[373] President Obama's *Executive Order 13636*, February 12, 2013
[374] Rządowe Centrum Bezpieczeństwa: *Program narodowy ochrony infrastruktury krytycznej*, Warszawa, 2013

public security. The approach is based on the assumption that any constraint or any flavor of duty will discourage private owners to willingly follow any security advises. Consequently, it will limit the protection to the necessary minimum and private owners will hide any possible lacunas in their security system[375]. Updating security of energy system is a costly burden. Prestige and social pressure could be not enough factors to encourage private owners to bear higher costs of conducting energy plant or an energy company. In Table 1 a comparison of governing the CI is shown.

Table 1. Comparison of Governing the CI

Region	Governing the Critical Infrastructure
United States of America	The Report of the President's Commission on Critical Infrastructure Protection (1997)
European Union	European Program of Critical Infrastructure Protection (2006)
Poland	National Program of Critical Infrastructure Protection (2013)

Source: own elaboration on the basis of official legal sources

On the other hand, no one has said that paying €100.000 fine will be enough to compel private owner to invest probably more in e.g. cyber security. In the end, the price for updating security would plausibly pay users within monthly invoices. Law aims „to make men good not only through fear of penalties but also indeed under allurement of rewards"[376]. Both ways of policing the legal order are well founded in our legal tradition thanks to Roman legal thought. Two lines which now appear before us: the German with economic penalty and all others including American and Polish solutions which favor soft cooperation, for now exhaust the possibilities that are used to enhance cyber security of the energy infrastructure.

3. CI – its way to the Polish regulation

In fact a starting point for any legal solution is the definition of CI. The first definition of CI was issued by President's Commission on Critical Infrastructure Protection in the United States of America in 1997. Since then, similar regulations have been introduced in many countries.

In the European Union (EU) the European Program of Critical Infrastructure Protection (EPCIP) was brought to life in 2006. The program sets a general framework for the countries affiliated in the EU in terms of improving the protection of European Critical Infrastructures (ECI). The EPCIP is supported by regular exchange of information between the member countries, and addresses a

[375] *Corpus Iuris Civilis*, vol. I, Krüger P. [ed.], Berolini 1954 (further: D.), D. 1,1,1,1
[376] ibidem

wide spectrum of threats including natural disasters, terrorism, criminal activities, and others[377]. The backbone of the EPCIP is the 2008 Directive on European Critical Infrastructures[13]. It establishes the procedure for identifying and assigning ECIs as well as a common approach for assessing the need to improve their protection. The directive has a sectorial scope, and applies only to energy and transport. As far as Poland is concerned, the CI regulations are founded on 26 April 2007 Decree on crisis management. As the following, the National Program of Critical Infrastructure Protection (NPOIK) emerged in 2013, and remains the state-of-the-art guide in this area.

The program defines the CIs and the measures of their protection. Since the CIs are often privately owned, the responsibilities of each side is also determined[378]. Critical infrastructure is defined as object, device, installation, service that is a part of a larger system. Then, one of the entities can be identified as CI based on 3-stage selection process. There are two types of criteria used for CI assessment[379]:

a) System Criteria – characterize the functions of an object quantitatively. They are defined for each type of infrastructure.

b) General Criteria – characterize the results of failure or damage of the particular object. They include: loss of human life; economic loss; evacuation; loss of the service; recovery time; international effects; uniqueness of the object.

Each object, in order to be considered CI, must undergo three-level selection process, which includes:

1. First stage – application of system criteria to recognize potential objects, installations, devices or services as CIs in a particular system.
2. Second stage – verification if the object, installation, device or service is crucial for the security of the country, allows functioning of public administration or other institutions and businesses
3. Third stage – the potential results of damage or breakdown of the potential CI are considered.

To the infrastructure that has undergone the first and the second stage, the general criteria are applied. So as to be recognized as CI, the infrastructure must at least fulfill two of them. The three-stage process of CI recognition is based on elimination and allows for selection of the most crucial infrastructure. After positive verification, the infrastructure is enrolled on the national list of CIs. The operation and protection of CIs is done on the basis of cooperation of the system operator (owner), who can be a private entity, scientific institution and the government administration. Each of these entities can take part in the protection of CIs. As far as the government side is concerned, the position of the host of the CI belongs to the

[377] www.ec.europa.eu, access: 15.04.2015
[378] Rządowe Centrum Bezpieczeństwa: *Program narodowy ochrony infrastruktury krytycznej*, Warszawa, 2013
[379] ibidem

minister responsible for the appropriate sector (each system type has an assigned ministry), who coordinates the management of the infrastructure at the country level. State marshals and city mayors have a different role to play. On the other hand, universities and other scientific institutions provide expertise for the improvement of the CI protection. Managing the CI is an ongoing process that involves cooperation of many parties, each of which has its own responsibilities. The involvement of the entities varies as well depends on the type of infrastructure e.g. province governor is responsible for a province hospital that is located in a particular commune.

4. Security of energy systems and governing the commons

Presumptions hidden at the back of modern governance of the critical infrastructure must be considered in the light of recent developments in governing the limited natural resources – commons[380]. In fact parts of critical energy infrastructure reveals to bear special characteristics that can make it a type of modern commons.

Elinor Ostrom's researches on management of common-pool resources (CPR) and institutional approach towards public policy (IAD) have revealed that one cannot overlook how important is process of rule-making in seeking for common good[381]. Common Pool Resources (CPR) 'refers to a natural or man-made resource system that is sufficiently large as to make it costly (but not impossible) to exclude potential beneficiaries from obtaining benefits from its use'. Originally it was used to describe natural resource systems like forests, rivers, or water basins[382]. In all dimensions it pertains to the problem of governing a crucial and limited amount of resource that is so important for a community that any abuse or damage caused to the resource will harm the whole community and will endanger its existence.

G. Hardin in 1968 said that: the problem lies in the number of users of limited resource. In 1993 E. Ostrom instead showed that the problem of managing commons does not rely on a number of users, but it relies firstly on the limited nature of good, which a community needs, and secondly on a reasonable administration of the resource. The problem boils down to the question, "how to use the resource" rather than "how many people have to use it" in order not to exhaust it.

As Elinor Ostrom has shown, the best way to govern, protect and provide the rules of usage of the resource which is endangered can be found by community itself. Community self-governance can bring better economical, cultural and legal

[380] Ostrom E., Governing the Commons. *The Evolution of Institutions for Collective Action*, Cambridge University Press 1990
[381] ibidem
[382] ibidem

results than one-subject management. Her idea has been empirically confirmed in all other the world – from limited water basins in California, in Spain, via limited grazing lands in Switzerland, via limited fisheries in Turkey to irrigation systems in Sri Lanka, Nepal and to limited forests in Japan. In effect, she became the first women who received the Nobel Prize in Economic Sciences in 2009.

Empirical experience made idea very powerful but in fact it confirmed that which was already present in the common good perspective. Human perfection and personal development is in the center of governing community. There are rules and institutional arrangements which can help every member become better than before.

We can cite Aristotle who considered *polis* as a natural environment for human. He praised with force the flourishing self-governance of the city with multiple communities and legislative bodies which enabled every individual to have influence on rules governing the whole society[383].

In social-economic thought it was Friedriech von Hayek who has shown that in order to adapt to economic surrounding there has to be community which teaches behavior and which create spontaneous order independently of state power – it is the idea of order which rises as a natural effect of human cooperation and could not be imposed by any power[384].

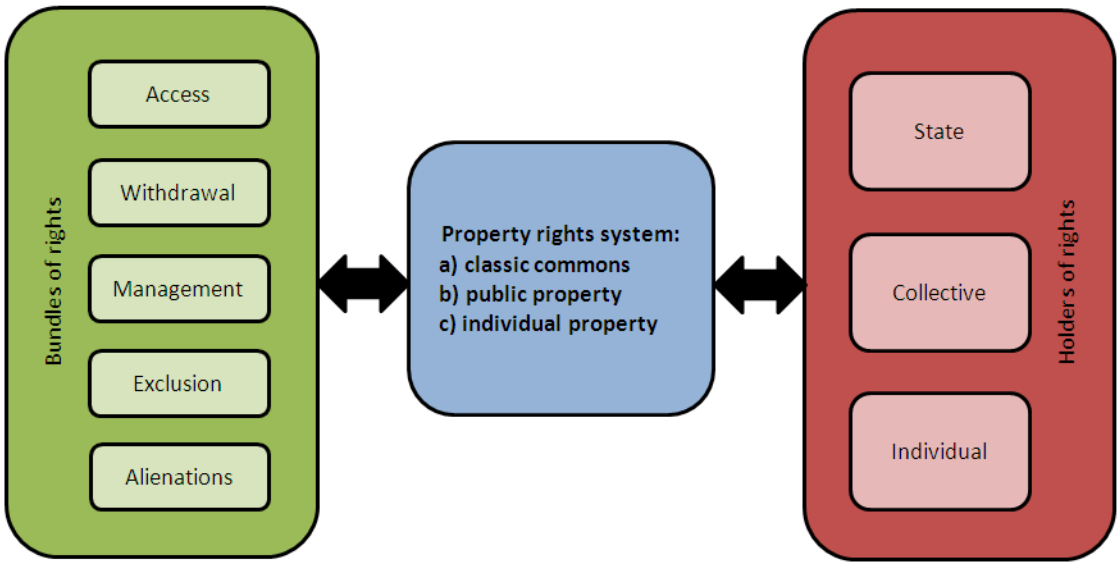
Finally, there is also religious perspective. For example we can take catholic social teaching and that which was presented by Benedict XVI in his official speech in Bundestag. He says that community to set up good institutional rules must always respect the ecological surrounding but not only environment – also the ecology of man. It shows that social and political thought go through the same paths and presents values which last unchanged in various contexts[385].

We have to keep in mind that ownership serves to protect users of special and important resources and goods. Finally it enables society to share peacefully a great variety of resources. However, there has to be return to the perspective in which every owner is also the member of society and possesses goods important for the whole society.

As it is presented by the Figure 3, the type of entity that holds the property of the crucial good is not separated completely from the nature of the protected good and from the know-how – the ways in which we can govern the commons. In fact, the evidence of Elinor Ostrom revealed that how we govern is far more important than who is holding the right: private entity or public one.

[383] Politics, 1276b; 1278b; 1280b
[384] von Hayek F., *The Constitution of Liberty*, Chicago: University of Chicago Press 1960, s. 59
[385] Benedict XVI, *The Listening Heart*. *Reflections on the Foundations of Law*, Reichstag Building, Berlin, 22 September 2011

Figure 3. Overview on property rights framework



Source: own elaboration

Critical infrastructure in fact has become a kind of commons – a limited amount of resource which is necessary for all community and which has to be protected against any form of destruction, so as to preserve the standard of living of the community[386]. Energy systems „fit major features of commons: they are a non-excludable resource system, there are appropriation problems related to rivalry in consumption of essential services, coordination needs deriving from system complementarities, diffuse property rights and decision rights with respect to the resource system, and multiple purpose services contributing to disperse and conflicting stakeholder interests" [387].

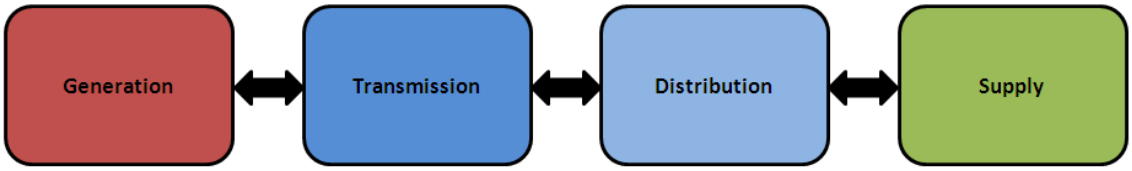
The inevitable tension between private interest and public demand of securing indispensable critical systems and services among which energy is one of the most important one, leads us to the concept of the common good and the self-responsible community.

Recent years have shown that states usually shape their energy policy moving from a governmental management of infrastructure to a liberal market model which is protected by a institution of a regulator[388]. Energy – critical source transmitted through critical infrastructure now usually is to be considered a mere commodity. The change has been made, along the line highlighted by Elinor Ostrom. The state seemed not to be effective and creative enough to ensure the level

[386] Rządowe Centrum Bezpieczeństwa: *Program narodowy ochrony infrastruktury krytycznej*, Warszawa, 2013
[387] Kunneke, RW & Finger, M ., *The governance of infrastructures as common pool resources*. [In:] Bauev J. [ed.], Workshop of the workshop, Bloomington (USA) Indiana 2009, pp.1-24
[388] Roelich K., Knoeri Ch., *Governing the infrastructure commons: lessons for community energy from common pool resource management*, SRI PAPERS 2015, pp.1-25

of investment and innovation and lower prices that can be achieved by the market rules[389]. In fact, the result is that energy sector is neither state governed nor the fruit of the free market operations. It is indeed a combination thereof which compels both sides to cooperate and adjust their demands with the good of the society.

Figure 4. Classical concept of power energy system



Source: own elaboration

To illustrate this, Figure 4 shows the structure of the classical electricity system. Electricity is generated, transmitted via the national grid and distributed to customers via regional distribution networks[390]. The formal structure of protecting CI is well founded. However, the problem lies in the practical effects of the prepared security structure. Generation and transmission of energy is usually considered to be in the public sphere. However, as it has been presented in the case of the USA and to some extent in Poland and in Germany private owners appear already in the process of generation and transmission. When it comes to the distribution and supply even in Germany private owners are invited to take care about the CI which is the closest to the users although in the EU under the control of a regulator. Step by step the chains of energy infrastructure become more open to network competition rather than to "one-body" management would it be a state or a private owner.

That structure of energy CI reveals the characteristics that are similar to the problems of commons: system management, capacity management, interconnectedness and interoperability. They are placed within the chain of energy process which is on the one hand now shifting from governmental control to the market governance and on the other hand which is becoming a globalized network of CI. All these compels to ask about involving local communities within these "blocks" of energy infrastructure[391].

The move from governmental to private governing in the case of distribution and supply has already created a simultaneous cooperation between public, private and the third sector – ie. self governance model[392]. The locally based action towards distribution and supply does not have to be dangerous for security and safety of CI.

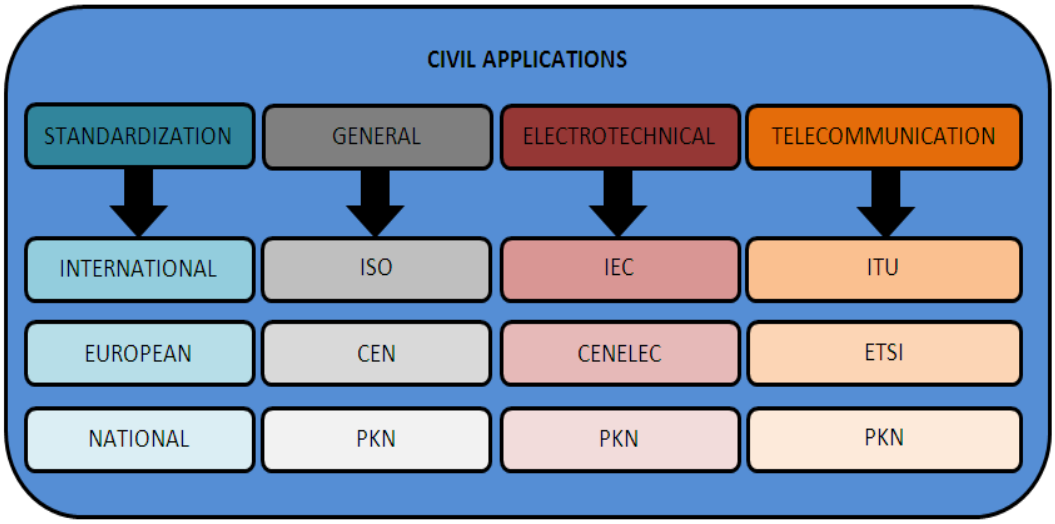
[389] ibidem
[390] ibidem
[391] Kunneke R.W., Finger M., *The governance of infrastructures as common pool resources*. [in:] Bauev J. [ed.], Workshop of the workshop, Bloomington (USA) Indiana2009, pp.1-24
[392] ibidem

What is more, it can be more flexible and adjust to the local needs and current security circumstances. Technical requirements of components of these „blocks" of energy process are vested in technical standards and recommendations that are open to anyone and which can help be up to date with the technological development and requirements of safe governing of CI.

5. Technical standards and recommendations

Legal experiences for service continuity of critical energy systems are strongly supported by technical standards and recommendations. These documents consist of a core of rules for regular operations of such systems. Some recommendations for emergency situations are also included and proposed. In practice different supporting standardization bodies appear. It is possible to characterized the standardization bodies taking into account the application field as well as the territory of influences. A brief summary of standardization bodies for civil applications is shown in Figure 5.

Figure 5. Overview on standardization bodies for civil applications

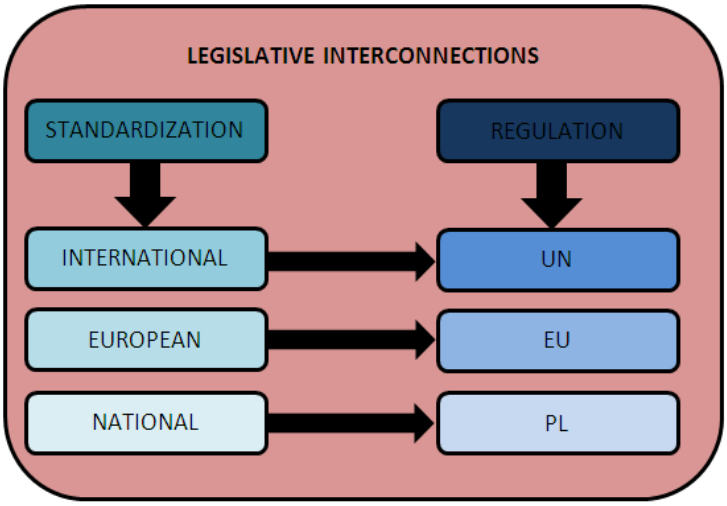


Source: own elaboration

It is well spotted that the output of standardization bodies is perfectly in line with needs of application for critical energy systems. The specific documents can be applied taking into account three basic pillars: general, electrotechnical and telecommunication. However in these documents some overlaps could also appear and furthermore the best practices of safety and security specialists shall be also applied. In some specific cases additional requirements should be applied taking into account another regulations e.g. in military field where the hierarchy should follow general schema NATO (NATO Standardization Office) → EDA (CEN, EDSTAR) → National MON (PKN TC 176) principles.

Schematic representation of legislative interconnections between standards and regulations is shown in Figure 6. Basically standards recommendations give an influence on specific territories. In addition some of them are called in specific decrees with aim to assure homogeneous and sustainable development continent, country or region.

Figure 6. Legislative interconnections between standardizations and regulations



Source: own elaboration

The service continuity of critical energy systems depends mainly on electrotechnical pillar which is well interconnected with another pillars. As it has been illustrated in Figure 6 the International Electrotechnical Commission (IEC) is the principal standardization organization interconnected with international level in the frame of United Nations (UN) as well as with other standardization organizations like European Committee for Electrotechnical Standardization (CENELEC) relevant to Europe and Polish Commit-tee for Standardization (PKN) relevant to Poland.

The IEC standards making process, similar to many other standards making processes, is handled by various technical committees (TC) or TC as they are called. The TCs are the key bodies that drive the standardization and comprise experts from the national committees. Each technical committee and its standardization efforts is vast and is carried out by various working groups within the technical committees.

Technical requirements for service continuity of critical energy systems are principally introduced by three IEC TCs namely:

- TC 8 – System aspects for electrical energy supply;
- TC 64 – Electrical installations and protection against electric shock;
- TC 81 – Lightning protection; and other relevant TCs and relative publications.

The TC 8 scope is to prepare and coordinate, in cooperation with other relevant TC/SCs, the development of international standards and other deliverables with emphasis on overall system aspects of electricity supply systems and acceptable balance between cost and quality for the users of electrical energy. Electricity supply system encompasses transmission and distribution networks and connected user installations (generators and loads) with their network interfaces. The following list contains a couple of examples on system related aspects and elements belonging to the overall process of electricity supply. The purpose of this non-exhaustive list is to illustrate, in which fields expertise is required within TC 8, in order to enable the committee to properly fulfil its given task. It is not meant to be a list of items to be standardised. Examples for main system aspects to be taken into account for service continuity of critical energy systems are the following: Electrical system reliability (planning, operating limits – capability, adequacy, system security), network responsibility (operational safety, security), communication (operational safety, security).

The TC 64 basic rules of work are similar to the TC 8. In principal this committee is focus on protection against electric shock arising from equipment, from installations and from systems without limit of voltage; and for the design, erection foreseeable correct use and verification of all kind of electrical installations at supply voltage up to 1 kV a.c. or 1,5 kV d.c., except those installations covered by the following IEC committees: TC 9, TC 18, TC 44, TC 97, TC 99. In addition it is important to stress that the standards of TC 8 will not cover individual items of electrical equipment other than their selection for use, taking into consideration the appropriate products characteristics and classifications. Moreover the TC64 has got the safety pilot function: protection against electric shock. Therefore the respective publications in this field have the status of basic safety publications. TC 64 understands itself as a system committee which sets the overall safety standards for protection against electric shock and, for installation, determines the characteristics for the selection of electrical equipment to enable the safe use of electricity and the proper functioning of the equipment in the installation environment.

The TC 81 basic rules of work are similar to the TC 8. It has been established to prepare international standards and guides for lightning protection for structures and buildings, as well for persons, installations, services and contents. The objective of these standards are focus on: requirements development for design and installation of lightning protection systems for civil structures; requirements development for protection against lightning of services entering the buildings; especially electrical and telecommunication lines; basic requirements development for protection against electromagnetic effects due to lightning; general guidance development to IEC member countries that may have need of such requirements; international exchanges that may be hampered by differences in national regulations.

These standards can be particular important taking into account needs of protection against transient surges appearing in the system.

In addition each TC has own specific action plan correlated to the market's needs. Principally the recommendations and standards prepared for service continuity of critical energy systems purposes should be carefully studied by safety and security specialists. The present state of art shows that a horizontal guide across all standards and recommendations could consist of an added value for safety and security problems.

6. Conclusions

The idea of the paper is to analyze the complicated structure both of legal aspect of governing the critical energy systems and the international network of cooperation between engineers who provide technological norms towards common way of dealing with CI. Interestingly enough, legal and technological issues were presented from the point of view of governing the commons which compels anyone to ask about rule-making and rule-following processes. Discussion with Elinor Ostrom's theory is usually methodologically limited to governing the natural commons. However, there is a place to make idea much broader, and extend it to the case of protecting safety and security of energy CI. The legal and technological processes in that respect are going twofold: one way is to move responsibilities from government level to private owners, the second way is a continuous globalization of rules and standards offered by the committees and international bodies. The aim was to examine the phenomenon of spontaneous cooperation between private and public sphere which breeds the question about the role of local communities and their influence for so a vital energy CI. The third way is focused on taking into account self-governance at the local level: in distribution, supply, transmission or generation. The aim was to examine the ways in which states shape the rules and conditions of governing CI in the perspective of governing the commons.

On the base of present paper following conclusions could be formulate:

- safety and security aspects consist of a multidisciplinary task which can be executed by experts only;
- service continuity of critical energy systems need to have low-organization procedures for regular and emergency cases;
- critical energy systems need to have an individual approach for the safety and security provision which engages local community
- documents produced by ISO, IEC, ITU consist of a good base to preparation an adequate safety level;
- legislator shall with due diligence define Critical Infrastructure so as to protect private and public needs

- two ways of promoting security of CI: through penalties and through cooperation can be analyzed through the idea of common good and governing the commons
- critical infrastructure security does not depend on the property regime of the systems, buildings, services, and so on, but it depends on the mode of governing the every single company, entity, etc.
- further investigation and analyses are needed with aim to well describe horizontal interaction of critical energy systems safety and security.

Acknowledgment

The paper has been prepared in the frame of national cooperation between Warsaw University of Technology and Jagiellonian University in Kraków.

This research was funded in part by a grant (No. 41/2015-25 - Effective protection of electronic and electrical apparatus against transient surges of natural origin) from the Warsaw University of Technology – Dean's grant of Electrical Department – prof. Lech Grzesiak.

The Authors wish to express their gratefulness to the Authorities of both Universities, especially to the Dean of Electrical Department of Warsaw University of Technology - prof. Lech Grzesiak for related support.

REFERENCES

1. Digesta. *Corpus Iuris Civilis*, vol. I, ed. Krüger P., Berolini 1954 (further: D.), D. 1,1,1,1;
2. Filiol E., Gallais C., *Critical Infrastructure: Where we Stand Today*, Proceedings of the International Conference on Information Warfare & Security; 2014;
3. Vijayan J., Obama executive order redefines critical infrastructure, Computerworld, Feb 14, 2013;
4. Moteff J., Parfomak P., *Critical Infrastructure and Key Assets: Definition and Identification*, CRS Report for Congress 2004;
5. Polskie Sieci Energetyczne, *Komunikat z dnia 10 sierpnia 2015 r. w sprawie wystąpienia zagrożenia bezpieczeństwa dostaw energii elektrycznej, podjętych działaniach i środkach w celu usunięcia zagrożenia i zapobieżenia jego negatywnym skutkom oraz o wprowadzeniu ograniczeń w dostarczaniu i poborze energii elektrycznej na polecenie OS*;
6. Luiff E., Klaver M., *Critical infrastructure awareness required by civil emergency planning*, IEEE Workshop on Critical Infrastructure Protection, IEEE, 2005;
7. Rządowe Centrum Bezpieczeństwa: *Program narodowy ochrony infrastruktury krytycznej*, Warszawa, 2013;
8. http://zepak.com.pl/pl/, access: 11.05.2016;
9. Bayer E., *Report on the German power system*, Version 1.0. Study commissioned by Agora Energiewende, RAP 2015 NIPP 2013, Partnering for Critical Infrastructure Security and Resilience, US Homeland Security 2013;
10. IT-Sicherheitsgesetz Nr. 31 vom 24.07.2015, §14 (2);
11. President Obama's Executive Order 13636, February 12, 2013;
12. www: ec.europa.eu, access: 15.04.2015;

13. The Council of the European Union: Council directive 2008/114/EC, Official Journal of European Union, 2008;
14. Ostrom E., *Governing the Commons*. The Evolution of Institutions for Collective Action, Cambridge University Press 1990;
15. Aristotle, Politics, 1276b; 1278b; 1280b;
16. von Hayek F., *The Constitution of Liberty*, University of Chicago Press, Chicago 1960;
17. Benedict XVI, *The Listening Heart*. *Reflections on the Foundations of Law*, Reichstag Building, Berlin, 22 September 2011;
18. Kunneke R.W., Finger M., *The governance of infrastructures as common pool resources*, [in:] Bauev J. [ed.], *Workshop of the workshop*, Bloomington (USA): Indiana 2009;
19. Roelich K., Knoeri Ch., *Governing the infrastructure commons: lessons for community energy from common pool resource management*, SRI PAPERS 2015.

BIOGRAPHICAL NOTES

Grzegorz Blicharz, PhD in Roman law and Comparative law, he received the Master of Law, Master of Philosophy, and PhD degrees from Jagiellonian University in Krakow. He completed Postgraduate Studies in Roman Law at University of Rome „La Sapienza", and he is the laureate of the „Diamond Grant" Program.

Dr Tomasz Kisielewicz, PhD in Electrical Engineering received the M.Sc. and Ph.D. degrees from Warsaw University of Technology, Poland and University of Rome „La Sapienza", Italy, respectively. His main field of scientific interest includes power systems safety and security, especially risk assessment and management, protection against transient surges.