ISSN 2421-4442

SICUREZZA TERRORISMO SOCIETÀ

Security Terrorism Society

INTERNATIONAL JOURNAL - Italian Team for Security, Terroristic Issues & Managing Emergencies

EDUCatt

SICUREZZA, TERRORISMO E SOCIETÀ

INTERNATIONAL JOURNAL
Italian Team for Security,
Terroristic Issues & Managing Emergencies

16

ISSUE 2/2022

Milano 2022

EDUCATT - UNIVERSITÀ CATTOLICA DEL SACRO CUORE

SICUREZZA, TERRORISMO E SOCIETÀ
INTERNATIONAL JOURNAL – Italian Team for Security, Terroristic Issues & Managing Emergencies

ISSUE 2 – 16/2022

Largo Gemelli 1, 20123 Milano - tel. 02.7234.22.35 - fax 02.80.53.215
e-mail: editoriale.dsu@educatt.it (produzione); librario.dsu@educatt.it (distribuzione)
web: www.educatt.it/libri

Associato all'AIE – Associazione Italiana Editori

ISSN: 2421-4442
ISSN DIGITALE: 2533-0659
ISBN: 978-88-9335-041-9

copertina: progetto grafico Studio Editoriale EDUCatt

Sommario

Crisis management vs. cyber threats

Mirosław Karpiuk

Mirosław Karpiuk, PhD., Prof. Dr. Habil., Full Professor, University of Warmia and Mazury in Olsztyn, Faculty of Law and Administration, Department of Administrative Law and Security Sciences, ORCID: 0000-0001-7012-8999, e-mail: miroslaw.karpiuk@uwm.edu.pl.

Abstract

An effective response to cyber crises is determined not only by having forces and resources adequate to such a threat, but having appropriate regulations in this regard are also important. The European Union has not yet developed common standards to deal with the threats that cause such crises, instead leaving crisis management in the event of such crises situations caused by cyber-attacks firmly to national legislation.
Commission Recommendation (EU) 2021/1086 of 23 June 2021 on the Establishment of a Common Cyberspace Unit (OJ EU L 237, p. 1) states that Member States and relevant EU institutions, bodies and agencies should ensure a coordinated EU response to, and recovery from, large-scale cyber incidents and crises. In this situation, it is necessary to swiftly and effectively mobilise operational resources for mutual assistance. In order to provide an effective coordinated response to cyber crises, relevant actors should be able to share best practices and ensure necessary preparedness. Their operation should take into account existing processes and the expertise of the different cybersecurity communities.
In turn, according to Commission Recommendation (EU) 2017/1584 of 13 September 2017 on the Coordinated Response to Large-Scale Cybersecurity Incidents and Crises (OJ EU L 239, p. 36), Member States and EU institutions should establish an EU Cybersecurity Crisis Response Framework integrating the objectives and modalities of cooperation. The EU Cybersecurity Crisis Response Framework should, in particular, identify the relevant actors, EU institutions and Member State authorities, at all necessary levels – technical, operational, strategic – and develop standard operating procedures that define the way in which these cooperate within the context of EU crisis management mechanisms. Emphasis should be placed on enabling the exchange of information without undue delay and coordinating the response during large-scale cybersecurity incidents and crises.

Keywords

Crisis management, cybersecurity, critical infrastructure, essential service

1. Introduction

Cyber threats can lead to all sorts of adverse phenomena, including crises, especially if cyber-attacks target communication and information systems designed to achieve the state's strategic objectives, including those related to ensuring the continuity of critical infrastructure. Threats in cyberspace can lead to crisis situations, especially since public institutions and private entities are largely digitised and the communication and information systems they use are not always properly secured.

The Polish legislators in Article 2 of the Act of 26 April 2007 on Crisis Management (consolidated text: Journal of Laws of 2022, item 261, as amended – hereinafter: the ACM) defines crisis management as the activities of public administration authorities which are part of State security management, and which consist in the prevention of crisis situations, the preparation to control such crisis situations as part of planned activities, response in the event of the occurrence of a crisis situation, the elimination of their consequences, and the restoration of resources and critical infrastructure. Based on the legal definition of crisis management, it is possible to distinguish four phases of crisis management: prevention, preparation, response and recovery (Czuryk, Dunaj, Karpiuk, Prokop 2016, p. 21). The term comprises the activities of public administration authorities that involve responding to a threat resulting in the emergence of a crisis situation (or the possibility thereof). The preventive aspects of such activities are extremely important, allowing the prevention of the emergence of such situations.

A crisis situation, as defined in Article 3(1) of the ACM, is a situation that has a negative impact on the level of security of the population, can cause significant damages to property or the natural environment, and results in substantial limitations of the activities performed by public administration authorities due to inadequate forces and resources. The legislators do not list the prerequisites that can lead to such a situation, so it should be assumed that it can be triggered by any threat that significantly affects the level of security. Such situations can therefore also emerge due to cyber threats. Accordingly, the role of the authorities responsible for crisis management is also to act to ensure cybersecurity, to the extent that threats in cyberspace may result in the emergence of a crisis situation.

As defined in Article 2(4) of the Act of 5 July 2018 on the National Cybersecurity System (Journal of Laws of 2020, item 1369, as amended – hereinafter: the NCSA) cybersecurity means the resilience of information systems to any action that compromises the confidentiality, integrity, availability and authenticity of the data processed or of the related services offered by those systems. And an information system is a communication and information sy-

stem and the electronic data processed in it. A communication and information system is defined in Article 3(3) of the Act of 17 February 2005 on the Computerisation of the Operations of the Entities Performing Public Tasks (Journal of Laws of 2021, item 2070 as amended) as a set of cooperating IT hardware and software, providing the possibility to process and store, as well as send and receive, data via ICT networks with the use of an end device suitable for a given network type. The concept of cybersecurity involves the protection of resources (data, information, i.e. digital content), the protection of communication and information systems and networks, devices, as well as the protection of content transmission over the network (Chałubinska-Jentkiewicz 2019, p. 20)

The managing authorities are also part of the National Cybersecurity System, the objective of which, pursuant to Article 3 of the NCSA, is to ensure cybersecurity at a national level, including the uninterrupted provision of essential services and digital services by achieving an appropriate level of security of the information systems used to provide these services and ensuring the handling of incidents.

According to Commission Recommendation (EU) 2021/1086 of 23 June 2021 on the Establishment of a Common Cyberspace Unit (OJ EU L 237, p. 1), faced with the cross-border nature of cybersecurity threats and the continuous surge of more complex, pervasive and targeted attacks, relevant cybersecurity institutions and actors should increase their ability to respond to such threats and attacks by harnessing existing resources and better coordinating efforts. All relevant actors in the EU need to be prepared to respond collectively and exchange information in such scope. The purpose of this Recommendation is to identify the actions necessary to coordinate EU efforts to prevent, detect, discourage, deter, mitigate and respond to large-scale cyber incidents and crises. Member States and relevant EU institutions, bodies and agencies should ensure that, in cases of large-scale cybersecurity incidents and crises, they coordinate their efforts through a Joint Cyber Unit which enables mutual assistance through expertise from Member State authorities and relevant EU institutions, bodies and agencies.

2. Critical infrastructure protection against cybersecurity threats

The objective of the crisis management system is to protect critical infrastructures from the threats that have an impact on their operation. The operation of critical infrastructures can be disrupted by threats occurring in cyberspace, so the protection must take into account the principles of cybersecurity allowing them to operate properly, and so not only the anticipation

and elimination of obstacles, but also the elimination of any damage caused by unwanted incidents.

(National) critical infrastructure should be construed as systems and their functionally related facilities, including civil structures, equipment, installations, services essential to the security of the state and its citizens required to ensure the smooth functioning of public administration authorities, as well as institutions and entrepreneurs. This definition is given in Article 3(2) of the ACM, also indicating that it includes the following systems: 1) the supply of energy, energy-producing raw materials and fuels; 2) communications systems; 3) ICT networks; 4) financial systems; 5) food supply; 6) water supply; 7) health care systems; 8) transport systems; 9) rescue systems; 10) systems ensuring the continuity of public administration; 11) manufacturing, warehousing, storage and the use of chemical and radioactive substances, including pipelines for dangerous substances. A critical infrastructure will have a European dimension if its disruption or destruction would have a significant impact on at least two European Union member states.

In Article 3(3) of the ACM the legislators also defined critical infrastructure protection, defined as all activities aimed at ensuring the functionality, continuity and integrity of critical infrastructures in order to deter threats, risks or vulnerabilities, as well as to limit and neutralise their effects and to ensure their rapid restoration in case of breakdowns, attacks or other events which disrupt their proper functioning. Therefore, critical infrastructure protection comprises a preventive aspect (anticipating threats and providing protection against them), a current aspect (combating threats), and a follow-up aspect (removing the effects of threats). All these stages of critical infrastructure protection are very important from the perspective of effective crisis management, including cases of threats occurring in cyberspace.

An important planning document covering critical infrastructure protection is the National Critical Infrastructure Protection Programme established by the Council of Ministers in the form of a resolution. It clearly provides that the critical infrastructure protection system should apply to all types of identified threats – natural, intentional or technical – and be prepared to restore the functions performed by the infrastructure as quickly as possible. In addition, the system should be comprehensive and flexible, as well as easy for those responsible for protecting critical infrastructure to apply and to understand its mechanisms. Critical infrastructure protection is carried out, among other things, through the provision of ICT security, which is seen as a set of organisational and technical measures aimed at minimising the risk of disrupting the functioning of this infrastructure following any unauthorised impact on communication and information systems. Pursuant to § 7 of the Regulation of the Council of Ministers of 30 April 2010 on the National Critical In-

frastructure Protection Programme (Journal of Laws of 2010 No. 83, item 541), the conditions for improving critical infrastructure security are created through: 1) the implementation of the designated priorities and objectives of the programme; 2) ensuring conditions for improving the protection and continuity of critical infrastructure; 3) preparation for crisis situations that may result from or adversely affect the disruption of critical infrastructure; 4) the preparation for responding in situations of the destruction or disruption of critical infrastructure; 5) ensuring conditions for critical infrastructure reconstruction; 6) compliance with the standards and requirements of the programme; 7) cooperation in implementing the programme.

The National Critical Infrastructure Protection Programme is an element of planned activities performed by public administration in the area of security, which also involves cyber threats. Public administration authorities are required to draw up various types of plans, strategies, or programmes. Furthermore, in their planning documents they sometimes have to take into account cybersecurity as an important element to ensure efficient performance of the public tasks that need to be protected against cyber threats. Planning, including planning for cyberspace, makes it possible to take coordinated action allowing for the proper, timely and harmonious implementation of the objectives set for public administration in an organised and continuous manner, especially with the involvement of many entities (Karpiuk 2021, p. 47).

In Article 6(1) of the ACM, the legislators generally define critical infrastructure protection tasks, indicating that they include: 1) the collection and processing of information concerning threats to critical infrastructure; 2) the development and implementation of procedures in the event of threats to critical infrastructure; 4) the reconstruction of critical infrastructure; 5) collaboration between public administration and owners, owner-like possessors and lessees of critical infrastructure facilities, installations or devices in respect of their protection. Threats to critical infrastructure can vary in nature and affect it in different ways. Particularly dangerous are attacks on communication and information systems, including those used for fundamental tasks, whether in terms of the stability of the economy or the normal operation of the state, especially since the critical infrastructure serving these purposes is largely automated and thus vulnerable to cyber-attacks.

Owners, autonomous possessors and dependent possessors of critical infrastructure facilities, installations or equipment are obliged to protect them, in particular by preparing and implementing, adequately to the foreseen threats, critical infrastructure protection plans and by maintaining their own backup systems ensuring security and sustaining the functioning of this infrastructure until its complete restoration. If at the same time they are operators of essential services, they include in their critical infrastructure protection plans

documentation concerning cybersecurity of the information systems used to provide essential services. This obligation is imposed by Article 6 (5-5a) of the ACM. Therefore, in this instance, the cybersecurity elements must be mandatorily taken into account when drawing up critical infrastructure protection plans.

A critical infrastructure protection plan drawn up by its operator, pursuant to § 2 of the Regulation of the Council of Ministers of 30 April 2010 on Critical Infrastructure Protection Plans (Journal of Laws of 2010 No. 83, item 542), should include: 1) general data: a) including the name and location of any critical infrastructure, b) allowing the identification of the operators of critical infrastructure, including names, addresses and registered offices, c) allowing the identification of the entities that manage the company on behalf of the operator of critical infrastructures, including names, addresses and registered offices, d) including, to the extent necessary for the implementation of crisis management tasks, the business data of the owners, autonomous possessors and dependent possessors of facilities, installations or equipment of critical infrastructure responsible for maintaining contacts with entities competent for the protection of critical infrastructure, e) including the name of the person drawing up the plan; 2) critical infrastructure data including: (a) characteristics and basic technical parameters, (b) a plan (map) showing the location of facilities, installations or the system, (c) functional connections to other facilities, installations, equipment or services; 3) characteristics of: (a) threats to critical infrastructure and an assessment of the risk of their occurrence, together with anticipated scenarios for the development of events, (b) the dependence of critical infrastructure on other critical infrastructure systems and the possibility of disruption as a result of disruptions in other critical infrastructure systems, (c) their own resources that can be used to protect critical infrastructure, (d) resources of territorially competent authorities that can be used to protect critical infrastructure; 4) essential options: (a) to act in a situation of threat or disruption to the operation of critical infrastructure, (b) to ensure continued operation of critical infrastructure, (c) to reconstruct critical infrastructure; 5) principles of cooperation with locally competent: (a) crisis management centres, (b) public administration authorities.

3. Essential services vs. cyber threats

Essential services are of major importance for crisis management. The NCSA imposes a number of cybersecurity protection obligations on owners, autonomous possessors and dependent possessors of critical infrastructure facilities, installations or equipment that are operators of essential services.

They are provided in the energy, transportation, banking, health care, water supply, or digital infrastructure sectors.

An essential service is defined in Article 2(16) of the NCSA as a service that is essential for the maintenance of critical societal and/or economic activities, as included in the list of essential services.

The authority competent for cybersecurity shall issue a decision recognising the entity as an operator of essential services if: 1) the entity provides an essential service; 2) the provision of this service depends on information systems; 3) an incident would have significant disruptive effects on the provision of essential services by that operator. The above-mentioned prerequisites, which make it possible to decide whether a given entity should be recognised as an operator of essential services, are set forth in Article 5(2) of the NCSA. The above-mentioned prerequisites must be met together, which means that the absence of any one of them prevents a public administration authority from issuing an identification decision. The legislators do not specify whether the authority initiates the procedure for recognising an entity as an operator of essential service ex officio or upon the request of the party, so it should be assumed that both forms are permissible.

For the entity that no longer meets the requirements for recognising it as an operator of an essential service, the competent authority for cybersecurity, pursuant to Article 5(6) of the NCSA, shall issue a decision declaring an expiration of the decision under which it was recognised as an operator of essential services. Derogation from legal circulation of such a defective decision is the duty of the relevant authority.

The legislators impose on operators of essential services additional obligations connected with ensuring cybersecurity. They are required, under Article 8 of the NCSA, to implement a security management system in the information system used in the provision of essential services. The system aims to ensure: 1) regular incident-risk assessment and risk management, 2) the implementation of the appropriate technical and organisational measures proportionate to the assessed risk, taking into account the latest state of the art measures, including (a) the maintenance and safe operation of the information system, (b) security and the continued provision of the services on which the provision of the essential service is dependent, (c) the deployment, record-keeping, and maintenance of action plans which allow the continuous and uninterrupted provision of the essential service, and ensure the confidentiality, integrity, availability, and authenticity of information, (d) the implementation of a continuous monitoring system to supervise the information system used to provide the essential service, 3) the collecting of information on cybersecurity threats and the vulnerabilities of the information system used to provide the essential service, 4) incident management, 5) the

applying of measures to minimise the impact of incidents on the security of the information system used to provide the essential service. In this regard it is necessary to keep the software up to date, apply security measures against unauthorised modification in the information system and take immediate action upon identifying a vulnerability or a cybersecurity threat, 6) using the means of communication which facilitate accurate and safe communication within the national cybersecurity system. Security of the information systems used to provide essential services is an important aspect of crisis management, the purpose of which is to neutralise phenomena that adversely affects the level of security, causes significant restrictions in the operation of specific public administration authorities or events that have, or may have, an adverse impact on cybersecurity.

Article 9 of the NCSA imposes an obligation to: 1) designate a person responsible for communicating with entities in the National Cybersecurity System, 2) provides essential-service users with access to knowledge which allows them to understand cybersecurity threats and to employ effective precautions against such threats as required in relation to the essential services provided, in particular by publishing relevant information on an operator's website, 3) inform the authority competent for cybersecurity about which EU member states the entity has been recognised as an operator of essential services in, and the date of termination of the provision of the essential service, no later than within three months of changing the data. This obligation is imposed on operators of essential services.

If an operator of essential services is at the same time the owner, autonomous possessor or dependent possessor of facilities, installation, equipment or services being part of a critical infrastructure, which has an approved critical infrastructure protection plan that includes cybersecurity documentation of the information system used to provide the essential service, he is not required to develop it once again. He is released from this obligation under Article 10(4) of the NCSA. However, he is required to apply it and keep it up to date, as well as establish supervision over it.

As provided for in Article 11 of the NCSA, operators of essential services are also obliged to: 1) ensure incident handling, 2) provide access to information on recorded incidents to the relevant Computer Security Incident Response Team CSIRT MON, CSIRT NASK, or CSIRT GOV, insofar as necessary for the performance of its tasks, 3) classify a given incident as serious based on the thresholds for considering a given incident as serious (these thresholds are set out in the Regulation of the Council of Ministers of 31 October 2018 on Serious Incidents Thresholds, Journal of Laws of 2018, item 2180), 4) promptly report any serious incident, not later than within 24 hours from its detection, to the relevant CSIRT MON, CSIRT NASK, or

CSIRT GOV, 5) cooperate with the relevant CSIRT MON, CSIRT NASK, or CSIRT GOV during the handling of a serious and critical incident by providing the required data, including personal data, 6) remedy vulnerabilities that have led, or could have led, to a serious incident, a significant incident or a critical incident, and inform the authority competent for cybersecurity of their remediation.

Operators of essential services are required to ensure that a security audit of the information system used for the purpose of the provision of essential services is conducted at least once every two years. This obligation is provided for in Article 15(1) of the NCSA. The role of the audit is to evaluate the examined areas and inform about the effectiveness of the processes taking place, which were designed to help a specific entity achieve its planned strategic goals (Romaniuk 2022, p. 200). Neither the entire activity of operators of essential services, nor the facilities, installations, or equipment of critical infrastructure, but the information system used to provide essential services, are subject to auditing.

4. Conclusions

Cybersecurity is a specialised security department that aims to protect information systems against threats (Czuryk 2019, p. 42). Information systems are widely used not only by private actors (including entrepreneurs), but also by public authorities, and serve not only for faster communication (including over long distances), but also for the performance of tasks, including those of fundamental importance to the state and its institutions. They are therefore important to the normal operation of the state, and consequently must be protected to eliminate cyber-attacks that disrupt their functioning. This normal operation of the state also ensures the proper operation of critical infrastructures which are vulnerable to cyber-attacks.

Cybersecurity threats may lead to a crisis situation, so it will be necessary to initiate actions appropriate to crisis management, which may, among others, result in restrictions on civil liberties.

Disruptions to information and communications systems and networks are highlighted in the National Crisis Management Plan, by indicating that they are caused by, among others, cyber threats that includes both intentional actions (attacks, sabotage) with the use of and against information systems, as well as unintentional actions (failures, errors). They are among the most disruptive (in terms of damage) incidents hitting modern society, critical infrastructures and essential services. Cybersecurity incidents are becoming more common because: 1) generally available tools and devices are sufficient enough to carry out an attack in cyberspace; 2) cyberspace does not have spe-

cific control barriers; 3) the probability of finding vulnerabilities is relatively high; the targets of intentional actions are very diverse – computer networks are at risk, as well as government computers, banking and private enterprise systems, and home users; 4) due to the widespread use of information systems and their diversity, failures and errors become more and more likely. According to the National Crisis Management Plan, communication and information systems and networks are disrupted due to: 1) human factors, where we are dealing with ignorance or the disregard of regulations and procedures; 2) computer sabotage, organisational error, human error, a lack of supervision; 3) the modification of systems and data; 4) technical or programming errors (application vulnerability); 5) failure, sabotage, damage or the theft of transmission elements; 6) a lack of control of the hardware and software supply chain; 7) a lack of developed, implemented and applied security policies and procedures; 8) a lack of implemented and tested safeguards adequate to identify threats; 9) a lack of regularity in updating security systems; 10) a lack of regularly conducted security tests of IT infrastructure; 11) IT staff shortages; 12) a lack of, or a low level of, training on cyber threats and information security. These disruptions can occur in government institutions and offices, in government administration, or in local government. Disruptions to communication and information systems and networks also occurs amongst entrepreneurs, including those that are operators of critical infrastructure or essential services.

Ensuring cybersecurity requires international cooperation for the protection of cyberspace. Developing a unified security system should guarantee a high level of protection in all cooperating states (Chałubinska-Jentkiewicz, Karpiuk, Kostrubiec 2021, p. 72). This international cooperation should also take into account the protection of critical infrastructure, when this infrastructure also serves for the provision of essential services that depend on information systems.

According to Commission Recommendation (EU) 2017/1584 of 13 September 2017 on the Coordinated Response to Large-Scale Cyber Incidents and Crises (OJEU L 239, p. 36), the use of, and dependence on, information and communication technologies have become fundamental aspects in all sectors of economic activity as companies and citizens are more interconnected and interdependent across more sectors and borders than ever before. A cybersecurity incident affecting organisations in more than one Member State, or even the entire Union, with potential serious disruptions to the internal market or more broadly to the network and information systems on which the Union economy, democracy and society rely is a scenario that Member States and EU institutions have to be well-prepared for. A cybersecurity incident may be considered a crisis at Union level when the disruption

caused by the incident is too extensive for a concerned Member State to handle on its own or when it affects two or more Member States with such a wide-ranging impact of technical or political significance that it requires timely coordination and response at the Union political level. Cybersecurity incidents can trigger a broader crisis, impacting sectors of activity beyond network and information systems and communication networks. Any appropriate response must rely upon both cyber and non-cyber mitigation activities.

Bibliography

Chałubińska-Jentkiewicz, K. (2019) Cyberbezpieczeństwo – zagadnienia definicyjne, *Cybersecurity and Law*, 2, pp. 7-23.

Chałubińska-Jentkiewicz, K., Karpiuk, M., Kostrubiec, J. (2021) *The Legal Status of Public Entities in the Field of Cybersecurity in Poland* Maribor.

Czuryk M. (2019) Supporting the development of telecommunications services and networks through local and regional government bodies, and cybersecurity *Cybersecurity and Law* no. 2, pp. 39-50.

Czuryk, M., Dunaj, K., Karpiuk, M., Prokop, K. (2016) *Prawo zarządzania kryzysowego. Zarys systemu* Olsztyn.

Karpiuk, M. (2021) Cybersecurity as an element in the planning activities of public administration *Cybersecurity and Law* no. 1, pp. 45-52.

Romaniuk, P. (2022) Administrative and legal obligations of the auditee in connection with the performance of an audit task in local government units *Cybersecurity and Law* no. 1, pp. 191-201.

Questo volume è stato stampato
nel mese di dicembre 2022
su materiali e con tecnologie ecocompatibili
presso la LITOGRAFIA SOLARI
Peschiera Borromeo (MI)

La Rivista semestrale *Sicurezza, Terrorismo e Società* intende la *Sicurezza* come una condizione che risulta dallo stabilizzarsi e dal mantenersi di misure proattive capaci di promuovere il benessere e la qualità della vita dei cittadini e la vitalità democratica delle istituzioni; affronta il fenomeno del *Terrorismo* come un processo complesso, di lungo periodo, che affonda le sue radici nelle dimensioni culturale, religiosa, politica ed economica che caratterizzano i sistemi sociali; propone alla *Società* – quella degli studiosi e degli operatori e quella ampia di cittadini e istituzioni – strumenti di comprensione, analisi e scenari di tali fenomeni e indirizzi di gestione delle crisi.

Sicurezza, Terrorismo e Società si avvale dei contributi di studiosi, policy maker, analisti, operatori della sicurezza e dei media interessati all'ambito della sicurezza, del terrorismo e del crisis management. Essa si rivolge a tutti coloro che operano in tali settori, volendo rappresentare un momento di confronto partecipativo e aperto al dibattito.

La rivista ospita contributi in più lingue, preferendo l'italiano e l'inglese, per ciascuno dei quali è pubblicato un Executive Summary in entrambe le lingue. La redazione sollecita particolarmente contributi interdisciplinari, commenti, analisi e ricerche attenti alle principali tendenze provenienti dal mondo delle pratiche.

Sicurezza, Terrorismo e Società è un semestrale che pubblica 2 numeri all'anno. Oltre ai due numeri programmati possono essere previsti e pubblicati numeri speciali.

EDUCatt - Ente per il Diritto allo Studio Universitario dell'Università Cattolica
Largo Gemelli 1, 20123 Milano - tel. 02.72342235 - fax 02.80.53.215
e-mail: editoriale.dsu@educatt.it (produzione) - librario.dsu@educatt.it (distribuzione)
redazione: redazione@itstime.it
web: www.sicurezzaterrorismosocieta.it
ISBN: 978-88-9335-041-9

Euro 20,00