ISSN 2421-4442

Sicurezza Terrorismo Società

Security Terrorism Society

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

6
2017

EDUCatt

SICUREZZA, TERRORISMO E SOCIETÀ

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

6

ISSUE 2/2017

Milano 2017

EDUCATT - UNIVERSITÀ CATTOLICA DEL SACRO CUORE

SICUREZZA, TERRORISMO E SOCIETÀ

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

ISSUE 2 – 6/2017

Direttore Responsabile:

Matteo Vergani	(Università Cattolica del Sacro Cuore – Milano e Global Terrorism Research Centre – Melbourne)

Co-Direttore e Direttore Scientifico:

Marco Lombardi	(Università Cattolica del Sacro Cuore – Milano)

Comitato Scientifico:

Maria Alvanou	(Lecturer at National Security School – Atene)
Cristian Barna	("Mihai Viteazul" National Intelligence Academy– Bucharest, Romania)
Claudio Bertolotti	(senior strategic Analyst at CeMiSS, Military Centre for Strategic Studies – Roma)
Valerio de Divitiis	(Expert on Security, Dedicated to Human Security – DEDIHS)
Chiara Fonio	(Università Cattolica del Sacro Cuore – Milano)
Sajjan Gohel	(London School of Economics – London)
Rovshan Ibrahimov	(Azerbaijan Diplomatic Academy University – Baku, Azerbaijan)
Daniel Köhler	(German Institute on Radicalization and De-radicalization Studies – Berlin)
Miroslav Mareš	(Masaryk University – Brno, Czech Republic)
Vittorio Emanuele Parsi	(Università Cattolica del Sacro Cuore – Milano)
Anita Perešin	(University of Zagreb – Croatia)
Giovanni Pisapia	(Senior Security Manager, BEGOC – Baku – Azerbaijan)
Iztok Prezelj	(University of Ljubljana)
Eman Ragab	(Al-Ahram Center for Political and Strategic Studies (ACPSS) – Cairo)
Riccardo Redaelli	(Università Cattolica del Sacro Cuore – Milano)
Mark Sedgwick	(University of Aarhus – Denmark)
Arturo Varvelli	(Istituto per gli Studi di Politica Internazionale – ISPI – Milano)
Kamil Yilmaz	(Independent Researcher – Turkish National Police)
Munir Zamir	(Fida Management&C7 – London)
Sabina Zgaga	(University of Maribor – Slovenia)
Ivo Veenkamp	(Hedayah – Abu Dhabi)

Comitato Editoriale:

Gabriele Barni	(Università Cattolica del Sacro Cuore – Milano)
Alessia Ceresa	(Università Cattolica del Sacro Cuore – Milano)
Barbara Lucini	(Università Cattolica del Sacro Cuore – Milano)
Marco Maiolino	(Università Cattolica del Sacro Cuore – Milano)
Davide Scotti	(Università Cattolica del Sacro Cuore – Milano)

© 2017 **EDUCatt** - Ente per il Diritto allo Studio Universitario dell'Università Cattolica
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: 978-88-9335-249-9

copertina: progetto grafico Studio Editoriale EDUCatt

Table of contents

Essays

Analysis and Commentaries

Critical infrastructures and cyber security: a fundamental economic intelligence issue

Laris Gaiser

Nota Autore

Laris Gaiser: Dr. Lais Gaiser is assistant professor in security studies at Faculty of Government and European Studies of Nova Univerza in Slovenia, member of ITSTIME at Università Cattolica del Sacro Cuore in Milan and Senior Fellow at GLOBIS Center - University of Georgia (US). From 2012 until 2014 he served as president of Euro Mediterranean University - EMUNI and strategic advisor of the Minister of Foreign Affairs of Republic of Slovenia. As visiting lecturer he teaches geopolicy and geoeconomy at Diplomatic Academy of Vienna.

Abstract Italiano

La competizione globale basata sull'intelligence economica deve prendere atto del fatto che le infrastrutture critiche rappresentano il presupposto della stabilità e della competitività di uno Stato. In Italia, nonostante le aperture della Legge 124/2007, non si è ancora giunti all'implementazione di una politica d'intelligence economica che possa aiutare il Paese a divenire nuovamente competitivo a livello internazionale, tuttavia – nonostante la mancanza di un approccio sistemico – il Legislatore ha mostrato una certa attenzione per il settore della sicurezza cibernetica. In questo articolo si vuole sottolineare come la difesa delle infrastrutture critiche sia connessa alla sicurezza cibernetica e come questa debba sempre essere disegnata sulle priorità nazionali non esistendo definizioni univoche di infrastrutture critiche a livello internazionale. Le minacce cibernetiche sono multiformi ed ogni Stato deve gestirle secondo le proprie priorità ovvero secondo il proprio schema istituzionale. Con il decreto Gentiloni del Febbraio 2017 il governo ha affidato al DIS il compito di gestire le vulnerabilità nonché instaurare le dovute collaborazioni per una maggiore resilienza del sistema-Paese.

Abstract English

Global competition based on economic intelligence must be aware that critical infrastructures are the prerequisite for a state's stability and competitiveness. In Italy, in spite of the openings of Law 124/2007, the implementation of an economic intelligence policy that can help the country to regain international competitiveness, has not yet been implemented. However – despite the lack of a systemic approach – the decision makers have shown interest for cyber security sector. This article seeks to emphasize how the defence of critical

infrastructures is connected to cyber security and how it should always be drawn on national priorities given the lack of a standard definitions of critical infrastructures at international level. Cyber threats are multifaceted and each state must handle it according to its own priorities and according to its own institutional framework. With the Gentiloni Decree dated February 2017, the government has entrusted Security Intelligence Department (DIS) with the task of managing vulnerabilities and establishing the necessary collaboration for greater country-system resilience.

1. Introduction

The gathering and strategic management of information is a complex art with economic relevance. Economic intelligence consists of gathering and processing information relevant to the economic sector with the aim of making operational choices. It consists of activities aimed at obtaining information, surveillance of competitors, protection of strategic information, and capitalising on this knowledge in order to influence, determine and control the global economic environment.[1] Economic intelligence, however, is also the most refined and up-to-date version of the economic warfare and it also requires the protection of strategic infrastructure, i.e. the backbone of any economic system. The terrain of the economic struggle does not have the stability of the old political alliances. Economic challenges have minimised the room of manoeuvrability of military warfare, although the final objective of accumulating power and wealth, has remained unchanged. The fluidity of today's international relations has forced countries to tackle global competition in such a way as to achieve the best possible outcome in terms of profits, development and wealth. Within such a framework, the countries return to be active co-protagonists of the economy, destined to catalyse and implement strategies of reform that allow the country-systems to remain, or return to be, competitive. The structures of economic intelligence are nothing other than the means, by which the public and private sectors can collaborate efficiently for the common wellbeing, in an historical period in which, if they remain separate, they are destined to perish. In this way, the entrepreneurial sector maintains its vitality while the state rediscovers a new *legitimizing* mission.[2] In the Nineteen-Eighties, Edward Luttwak announced the onset of a new world order, in which military warfare was to be replaced by economic weapons. Economic means are used by countries to increase their own clout and to have an impact on the balances of power. Military alliances and threats of

[1] Gaiser Laris, *Economic Intelligence and World Governance – Reinventing States for a New World Order*, Il Cerchio, RSM, 2016, p.24; cfr. Jean Carlo, Savona Paolo, Intelligence Economica, Il Rubbettino, Soveria Mannelli, 2011.
[2] Gaiser Laris, *Intelligence Economica*, Aracne, Ariccia, 2015, p.23.

war have lost some of their former strength.[3] Although Luttwak is right about the fact that countries tend to prefer power based on economic influence to territorial ambitions, which is considerably more sensible from a cost-benefit perspective, waged wars remain the *ultima ratio regis* of international politics. Economic warfare has given countries more options then waging into armed conflicts. This has – to some extent – loosened the interdependence between economy and war. This diverges from the 20th century, where the former was at service to the latter. As these borders expand over time, countries need to put in place their own economic intelligence units, because it is the tool they are forced to resort to, if they are to play on the new chessboard.

2. Critical infrastructure and the cyber domain

The context of economic activities in the past ten years has been radically transformed by an intense combination of technological innovations and geo-political confusion that have led to intense competition, greater interconnection, and unrestrained technological development.

Living every day in a complex world, we realize that traditional wars have been substituted by commercial wars, by *infowars* and by *cyberwars*. These end up characteristically being much less costly from the human point of view – meaning, more acceptable – but are often also more profitable. Economic wars are a reality in which information, knowledge and innovation are the raw materials, the international markets the frontline, while the failures of companies, unemployment, lack of public resources and the drop in the power of acquisition represent defeat.

In the post-Clausewitzian logic, conflict does not require the destruction of the enemy: the goal of economic war becomes submitting the adversary with the least amount of expenditure of energies possible. Unlike military conflicts, which sooner or later face a time limit, economic conflicts have a permanent character. In addition, unlike codified military rules, the rules of economic competition and enterprise protection must be regularly updated and adapted to ongoing technological change. The economic intelligence is a tool aimed to cope with global competition, to create governance and to shape national security with a clear final goal: producing added value.

In an economy that is every day more connected and technologically dependent, the cyber domain is one of the most important frameworks of international competition. A framework of vital importance but, ironically, at the same time a framework of greatest vulnerability.

[3] Luttwak Edward, *The Endangered American Dream*, Simon&Schuster, NY, 1993.

Shortly after his nomination to Secretary of Defence of the United States in 2012, Leon Panetta described today's situation in the field of *cyber* competition between nations, as a potential "Pearl Harbor" for US infrastructure.

We have witnessed, ever since, a series of damaging actions caused by cyberwarfare, a major security issue, a full-scale problem for the national security of various countries, especially when directed against critical infrastructure. At an international level, there are at least two generally accepted definitions. The first was given by NIST – the US *National Institute of Standards and Technology* – where critical infrastructure is defined as the "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." Conversely, the second definition comes from the European Commission and describes CI as "physical structures of information technology, networks, services and goods that, if subjected to destruction or damage, would have a serious impact on the health, wellbeing, security or economic stability of the citizens, or on the function of the governments of the European Union." The generic definition is supplemented by the one in Communication 702/2004 with the following more detailed list:

a) Energy installations and networks (e.g. electrical power, oil and gas production, storage facilities and refineries, transmission and distribution system)
b) Communications and Information Technology (e.g. telecommunications, broadcasting systems, software, hardware and networks including the Internet)
c) Finance (e.g. banking, securities and investment)
d) Health Care (e.g. hospitals, health care and blood supply facilities, laboratories and pharmaceuticals, search and rescue, emergency services)
e) Food (e.g. safety, production means, wholesale distribution and food industry)
f) Water (e.g. dams, storage, treatment and networks)
g) Transport (e.g. airports, ports, intermodal facilities, railway and mass transit networks, traffic control systems)
h) Production, storage and transport of dangerous goods (e.g. chemical, biological, radiological and nuclear materials)
i) Government (e.g. critical services, facilities, information networks, assets and key national sites and monuments)

Regardless of these two definitions, it should be noted that almost every country has its own mode of conceiving CI and that such a large number of perceptions does not facilitate a comparative analysis of strategies or a holistic approach in addressing issues regarding critical infrastructure's security.

Almost every CI today is directly or indirectly connected to the cyber world. Such connection exponentially raises the system's vulnerability.

The diffusion of Internet and of information systems shortens the distances around the world, facilitates work, making everything faster, but at the same time leads to a paradoxical consequence, where the most informed and developed countries are also the most vulnerable ones. The knowledge of these vulnerabilities is the assumption of an effective strategy of cyber protection and information security. Cyberspace is the space that includes every form of digital activity that is carried out online, a space where critical infrastructure itself is at the service of several other pieces of infrastructure.

Cyberspace threats are multiform. The original sin of the insecurity of the information infrastructure can be recognized in the fact that the web – on which everything is based – was moulded in the beginning on the simplicity of open TCP/IP protocols, without system-protection measures or auto-encryption, since simplicity and speed had to be guaranteed for the sake of efficiency and cost-effectiveness of the new tools. The digital economy was therefore born with a huge loophole. The logic of effectiveness has prevailed over that of national security. Information technology helped economies to develop, boosted their productivity, promoted innovation, facilitated international exchange and shaped new social balances. Internet has penetrated every area of our lives, including the vital services of our countries. However, the security researches have failed to keep pace with the fast development of cyberspace. Today's inadequate level of protection of digital technologies poses a strong challenge for economic development and a heavy burden to social stability. The same technological innovations that have brought many benefits to our society can now be exploited by enemy countries to carry out cyber-attacks with disastrous consequences. Information technology networks act as multipliers and generators of economic and military power. According to Prof. Umberto Gori almost one third of SCADA systems has already been infiltrated.[4] Attacks to critical infrastructure (CI) are constantly growing and represent the greatest challenge to our *cognitive bias*, since the nature of future attacks is just anyone's guess. In 2016 Clusit reported that in 2015 cyber-attacks against CI increased by 153% compared with 2014.

Contrary to the general opinion, individual hackers cannot bring serious harm to national critical infrastructure and therefore policy makers and com-

[4] Gori Umberto, *Dall'intelligence economica alla cyber intelligence: sfide e promesse per le imprese*, in *Cyberwarfare 2014*, ed.by Gori Umberto, Lisi Serena, Franco Angeli, Milano, 2015.

mon citizens must understand that such projects are the domain of lone wolves. Hacking websites, overtaking social media accounts and stealing confidential data are very showy operations, which however, usually do not have consequences for national safety. Low level cyber-attacks cannot affect the general economic and social stability of a country. In order to seriously destabilize a national system, the enemy must target critical infrastructure. To destabilize highly qualified resources, hackers need access to state-of-the-art technology. In most cases, only state-players can afford such levels of coordination and if only states can compete on this cyber level, then we are talking about cyberwar. Clarke defines cyberwar as a state's coordinated actions designed to penetrate computers and networks of another state with the purpose of causing damage or malfunction.[5] Cyber weapons exploit software and hardware vulnerabilities to gain access to critical targets. The vulnerabilities could be either due to coding or designing errors or to backdoors inserted on purpose in software or hardware. Considerable levels of intelligence and coordination skills are needed to discover these vulnerabilities, and the development of such weaponry requires substantial funding.[6] Cyberwar is highly unpredictable, fast and dynamic, since it annihilates the strategic values of distance, time and borders. In the cyber domain it is practically impossible to send notifications in time, mostly because the "warriors" wage attacks, whose origin, load and possible effects are hard to pinpoint. In 1999, Chinese Colonels Liang and Xiangsui argued that wars are about to become perennial and unlimited.[7] The international system is moving from a *time of war* to an *era of war*. Cyberwar shares many characteristics with aerial war, as defined in the 1930s by the theories of aerial supremacy and as actually implemented on the battle fields. From a tactical point of view, the goal of aerial warfare is to destroy the vital infrastructure of an enemy country, making it difficult to maintain the war effort and threating the livelihood of the civil population. Strategic bombardments of industrial structures, production plants, pathways of communication and supply, or aerial recognitions, are all activities that are easily assimilated to the extreme goals of modern cybernetic warfare to the CI with which the adversaries seek to seize secrets or hinder the normal functioning of a country. Depending on the operative means chosen, cyberwar may

[5] Clark Richard, Knake Robert, *Cyberwar: The Next Threat to National Security and What to Do About It*, Ecco, New York, 2010.

[6] Zanasi Alessandro, *Cyber Defense, Cyber Intelligence e relative armi: casi di collaborazione tra pubblica amministrazione, industria e ricerca finanziata dalla Commissione Europea*, in *Cyberwarfare 2014*, ed.by Gori Umberto, Lisi Serena, Franco Angeli, Milano 2015, p.40.

[7] See: Liang Qiao, Xiangsui Wang, *Unrestricted Warfare,* PLA Literature and Arts Publishing House, Beijing, 1999.

have both tactical and strategic goals. Nevertheless, aerial war and cyberwar are also similar for another reason: just as Alexander de Seversky noted in his fundamental work on the theory of aerial power, *Victory Through Air Power*, in 1942, in which he underlines how the preferred objectives for this type of war are the countries with a developed economy, the same can be said today for cybernetic war: The countries with underdeveloped systems of communication, transport or production are more immune than the more developed ones, which are consequently more vulnerable to air attacks or, today, to *cyber* infiltrations.

3. Security dilemmas and the Italian cyber-security approach

Given the dual nature of the cyber domain, which is physical and virtual, offense has always an advantage over defence. Every potential player is inclined to act in an offensive way. The dilemma of security – which we could define as the *offensive non-equilibrium* of the cybernetic system – is a problem of non-secondary importance for the future economic stability of the more developed countries, but most of all, it is a problem of pure balance of powers given how difficult it is to determine the place of origin of the attacks, which consequently diminishes the possibilities of reprisal. The Internet was born as a multiplier of power, in which the activities of defence are highly vulnerable also because the CI, for lack of pressure in the past, was often created without paying attention to redundancy systems or even duplicating or triplicating the control apparatus and procedures which could ensure the system remains operational even in the case of aggression.

Infrastructure resilience is the ability to reduce the magnitude and/or duration of disruptive events. The effectiveness of a resilient infrastructure or enterprise depends upon its ability to anticipate, absorb, adapt to, and/or rapidly recover from a potentially disruptive event. Resilience is a multifaceted issue involving security, risk management, business continuity and crisis management. One of the aspects that makes infrastructure (security) administration particularly complicated is the fact that, while the security of citizens relies on law enforcement structures, many pieces of critical infrastructure are owned or managed by the private sector. When speaking of security and resilience of CI, it is necessary to keep in mind that a public-private partnership is strongly needed here: an adequate level of cyber security can only be pursued through a broad collaboration among all the stakeholders. Resilience is a function: the awareness of a present or a foreseeable situation. It is the fundamental management of any type of vulnerability and the adaptability of a structure, namely the ability to mutate the factors that define equilibriums such as strategy, operating systems, decision-making and command structures.

There is no need to emphasize that the strategies and resilience techniques must adapt to the various infrastructure sectors. Specialized literature offers us as many definitions of resilience as there are infrastructure systems in order to create quantitative models for measuring the resilience to disruptive events, to assess the impacts on system performance and to calculate the recovery costs.

A complete and successful resilience strategy should always consider that CI is composed not only by technology but by people, processes and organizations, as well. Specific cultural backgrounds make each system unique.

The economic intelligence systems around the world should adapt their national economic frameworks to tackle the challenges of hybrid warfare. Resilience, more than the sum of all the processes needed, becomes a cultural approach that must involve the entire society. Critical infrastructure is almost synonymous to national economy and national security. Since governments are generally responsible for both, they are also responsible for delivering cyber strategies to protect infrastructure. It is a question of national governance, whose aim shall be to establish strong security tools for the national economy.

If governments really wanted to survive and maintain their historical roles, they should turn into business-friendly service platforms guaranteeing legal and infrastructural support to companies. Internationally competitive companies represent internationally competitive countries. Efficient information sharing between state-managed intelligence agencies and private business-intelligence units is absolutely needed to shape a new security culture as well as to guarantee a sound economy. Without private-public partnerships there is no efficient resilience. What is needed is a "mental reset" strategy, that does no longer rely only on reacting to attacks. We should change the rules of the game and thus identify the threats and vulnerabilities before any attack, while also adhering to national doctrines supporting the development of a less anarchic system.

In 2007, Italy reformed its intelligence sector. By Law 124/2007, the Security Intelligence Department (DIS) became the pivotal body coordinating the internal and the external intelligence agencies. In 2012, the Parliament updated Law 124 and thus entrusted the intelligence system with activities aimed at protecting critical infrastructure and strengthening the national cyber defence and security. In January 2013, Mario Monti signed the "National Strategy for Cybernetic Security" decree, by which the notions of security and cybernetic threat have been redefined for the very first time.

Security was thus redefined as: *The condition, in which cyberspace is protected by means of adopting appropriate measures of physical, logical and procedural security in the event of a voluntary or accidental acquisition and* *consequent transfer of data, their modification or illegitimate distribution, damaging, destruction or blocking of the regular functioning of the web and information systems or of their constitutive elements.*

Cybernetic threat has similarly been redefined as: *The complex of activities, carried out within the cyberspace or by using its means, aimed at damaging the cyberspace itself or its constitutive elements, achieved by the actions of individuals or either private or public organizations, with the aim of acquiring and transferring data, modifying or illegitimately destroying it, and thus to damage, destruct or block the regular functioning of the web and information systems or of their constitutive elements.*

An institutional architecture was therefore set out on three separate levels. The first level consists of political and strategic coordination - with the task of identifying goals - given to the Interministerial Committee for the Security of the Republic (CISR). The second level, named Nucleus for Cybernetic Security (NSC), shall ensure the coordination between the various administrations and the CISR. It was entrusted with activating possible actions of alert in the case of a crisis and was located into Military Adviser's Office at Prime Minister's Cabinet, composed of representatives from the intelligence agencies (DIS, AISE and AISI), the Ministry of Internal Affairs, the Ministry of External Affairs, the Ministry of Defence, the Ministry of Economic Development, the Ministry of Economy, the Department of Civil Protection, and the Agency for Digital Italy. The third level, Interministerial Situation and Planning Nucleus (NISP), received the task of managing possible crises.

In February 2017, the Italian government modified the described system. Replacing the Monti Decree with a new one. Premier Gentiloni, clearly followed the suggestions gathered since 2013 form the intelligence world, while trying to comply with the European Directive on Security of Network and Information Systems (NIS). The new Decree strengthened the coordination duties of the Interministerial Committee for the Security of the Republic within the cyber field and transferred the Nucleus for Cybernetic Security (NSC) to the Security Information Department (DIS) directly under the umbrella of the operational intelligence structure. The General Director of DIS has now the responsibility to define lines of action that will ensure the necessary security levels of strategic public and private systems and networks by checking and eliminating vulnerabilities. Such a shared-participation approach has been the main trait of the new Italian intelligence approach since 2007, by which the system has been opened to a broader collaboration with the "outside world", the academia and private companies, which are invited to collaborate with DIS to reach mutual benefits and improve the country's resilience.

The new Italian cyber security decree has therefore established the role of control of the cyber domain as an issue of national sovereignty, emphasizing that the goal cannot be reached without leadership by the government. The slightest fault in preparedness in any field, could – on a long-term basis – represent a serious threat to national security and economic stability.

Each country should find its own path in coping with this kind of issues to safeguard its future and to shape deterrence policies toward any potential – internal or external – sources of threat. National doctrines are the first step toward a more generally accepted international doctrine enhancing the establishment of a joint governance. The cyber security of CI must be resistant to attacks to such an extent that it simply makes sense for hackers to spend time and resources on taking it down.

4. Conclusions

There are no doubts about today's existence of multinational economic groups or small, ungoverned organisations that – if properly coordinated among themselves – can detain a highly penetrating and therefore undeniable power. The importance of territory for the fate of countries has changed dramatically over the years. Nevertheless, the 'sovereigns' have shown the ability to adapt and revise the concept of 'State', which is currently better described by the term 'country-system', in which the economic and social ties represent the fundamental adhesive for redefining the boundaries and the equilibriums of a nation.

Countries that are unable to be competitive – having no solid, safe and critical infrastructure – are doomed to succumb to others or become non-influential on a world scale. International competition has grown strongly and therefore country-systems need more sophisticated, precise and organized means to preserve their credibility, attract investments, remain structurally stable and make sound economic choices. If we consider these aspects, we could divide nations into three categories: the ones with an economic-intelligence system, the ones intending to adopt one, and the ones that will probably never have a similar system for an array of different reasons. While the first ones are in a position of overwhelming advantage, those in the second category still have a chance of not being completely subdued. Both will, however, exploit the weaknesses of ill-prepared nations, which are therefore doomed in global competition.[8]

[8] Gaiser Laris, *Intelligence Economica*, op.cit., p.24.

References

Clark Richard, Knake Robert, *Cyberwar: The Next Threat to National Security and What to Do About It*, Ecco, New York, 2010

CEPS. (2010), Protecting Critical Infrastructures in the EU, CEPS, Belgium

Gaiser Laris, *Intelligence Economica*, Aracne, Ariccia, 2015

Gaiser Laris, *Economic Intelligence and World Governance – Reinventing States for a New World Order*, Il Cerchio, RSM, 2016

Gori Umberto, *Dall'intelligence economica alla cyber intelligence: sfide e promesse per le imprese*, in *Cyberwarfare 2014*, ed. by Gori Umberto, Lisi Serena, Franco Angeli, Milano, 2015

Gori Umberto, Lisi Serena (ed.), *Cyberwarfare 2013*, Franco Angeli, Milano 2014

Gori Umberto. Lisi Serena (ed.), *Cyberwarfare 2014*, Franco Angeli, Milano 2015

Jean Carlo, Savona Paolo, *Intelligence Economica*, Il Rubbettino, Soveria Mannelli, 2011

Liang Qiao, Xiangsui Wang, *Unrestricted Warfare*, PLA Literature and Arts Publishing House, Beijing, 1999

Luttwak Edward, *The Endangered American Dream*, Simon&Schuster, NY, 1993

Zanasi Alessandro, *Cyber Defense, Cyber Intelligence e relative armi: casi di collaborazione tra pubblica amministrazione, industria e ricerca finanziata dalla Commissione Europea*, in *Cyberwarfare 2014*, ed.by Gori Umberto, Lisi Serena, Franco Angeli, Milano 2015

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: 978-88-9335-249-9

9 788893 352499

Euro 20,00