RESILIENT CRITICAL INFRASTRUCTURE AND ECONOMIC INTELLIGENCE IN THE CYBER DOMAIN

Dr. Laris Gaiser[1]

Introduction

In the academia, as among the specialized public it is quite impossible to find a single, commonly accepted definition of economic intelligence. According to Jean and Savona, economic intelligence is the discipline that study information needed by companies and states to take the right development decisions with the aim of fine-tuning their cognitive and decision-making capacities in the complex context of global competition (2011). The gathering and strategic management of information is a complex art with economic relevance and therefore businesses are forced to establish

1 Dr. Laris Gaiser is Assistant Professor at Università Cattolica del Sacro Cuore – Milano

their own business intelligence units. The efficiency of such units could be improved by appropriate cooperation at the state level, where national security agencies must adopt a decisive role both in terms of protecting and gathering information. 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 (Gaiser, 2016). 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 catalyze and implement strategies of reform that allow the country-systems to remain 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 (Gaiser, 2015). 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 war have lost some of their former strength (1993). 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.

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 cyber wars. 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. 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. We have witnessed, ever since, a series of damaging actions caused by cyber warfare, 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:

(1) Energy installations and networks (e.g. electrical power, oil and gas production, storage facilities and refineries, transmission and distribution system)

(2) Communications and Information Technology (e.g. telecommunications, broadcasting systems, software, hardware and networks including the Internet)

(3) Finance (e.g. banking, securities and investment)

(4) Health Care (e.g. hospitals, health care and blood supply facilities, laboratories and pharmaceuticals, search and rescue, emergency services)

(5) Food (e.g. safety, production means, wholesale distribution and food industry)

(6) Water (e.g. dams, storage, treatment and networks)

(7) Transport (e.g. airports, ports, intermodal facilities, railway and mass transit networks, traffic control systems)

(8) Production, storage and transport of dangerous goods (e.g. chemical, biological, radiological and nuclear materials)

(9) 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 (see table below) and that such a large number of perceptions does not facilitate a comparative analysis of strategies or a holistic approach in addressing issues regarding the resilience of critical infrastructure.

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 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. 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 (2015). 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. Last year Clusit reported that in 2015 cyber-attacks against CI increased by 153% compared with 2014.

Contrary to the general opinion, individual hackers do not bring serious threats to national critical infrastructure and therefore policy makers and common citizens must understand that such projects cannot be the domain of lone wolves.

Cyberwars are state's coordinated actions designed to penetrate computers and networks

of another state with the purpose of causing damage or malfunction (Clark 2010). Cyber weapons exploit software and hardware vulnerabilities to gain access to critical targets. 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. 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 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.

Table 1: Examples of taxonomies[2]

	EU	G8	USA	RUS	UK	NL	FR	GER	SWE
ICT and MEDIA	✓	✓	✓	✓	✓	✓	✓	✓	✓
WATER, DAMS, SURFACE WATER MNGT	✓		✓	✓	✓	✓	✓		
ENERGY	✓	✓	✓	✓	✓	✓	✓	✓	✓
NUCLEAR (radiological hazard), HAZARDOUS MATERIALS	✓		✓			✓	✓	✓	
FOOD	✓		✓		✓	✓			
AGRICULTURE			✓	✓					
HEALTH, MEDICAL SERVICES	✓	✓	✓	✓	✓	✓	✓		✓
FINANCE	✓	✓	✓	✓	✓	✓	✓	✓	✓
TRANSPORT, POSTAL, PIPELINES and LOGISTIC	✓	✓	✓	✓	✓	✓	✓		✓
CHEMICHAL INDUSTRY and BIOTECH	✓		✓			✓	✓		
SPACE	✓								
MONUMENTS ICONS			✓						
GOVERNMENT ADM		✓	✓	✓	✓	✓		✓	
DEFENSE INDUSTRY BASE, DEFENSE			✓	✓					
COMMERCIAL FACILITIES			✓						
EMERGENCY SERVICES		✓	✓		✓				
CRITICAL MANUFACTURING			✓						
VERY LARGE INFORMATION SYS				✓					
UTILITY INCLUDING WARMING SYSTEMS				✓					
INDUSTRY				✓					
MUNICIPAL SERVICES				✓					✓
CIVIL DEFENSE				✓					
LEGAL ORDER, PUBLIC SAFETY						✓	✓		
HAZARDOUS MATERIALS								✓	
SERVICES, OTHER								✓	
RETAIL, PROVISIONS									✓
PROTECTION & SAFETY									✓

Security dilemmas and IC resilience

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. According to Libicki, a dollar spent in offense equals far more than a single dollar spent in defence, if we are to restore the previous levels of security (2009). The dilemma

2 (author: Luisa Franchina, 2012)

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 English term intelligence derives from the Latin word intelligere, composed of the preposition inter, between, and legere, to read. Intelligere therefore signifies to read between the lines, to understand beyond the surface, to stabilize the relationship between the elements. The current definition of intelligence is thus the reasoning, planning, learning, and coming up with solutions to problems. Moreover, it should be recalled that for the German philosopher and psychologist William L. Stern, intelligence was none other than “the general capacity to adapt one’s own thought and behaviour in the face of new conditions and situations.” (Gaiser, 2015)

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.

Resilience has a series of technical, personal, organizational and co-operational aspects and consequently a series of capacities: predictive, absorptive, reactive and restorative, which imply the required tools of resilience: redundancy, robustness and segregation. Resilience is a complex issue tightly linked with prevention, since it must be based on the mental presumption that we cannot foresee the exact nature of future cyber-attacks and we can never exclude a black swan event. If prevention is—by its very definition— composed of active and passive moments and if only the governments have all the tools needed to successfully organize public-private partnerships, it would be sensible for intelligence agencies to act within the logic of economic intelligence, i.e. to act as national hubs coordinating active and passive policies. The seven mitigating mechanisms still valid today consist of creating awareness, reducing dependency, increasing redundancy, developing back-up alternatives, increasing flexibility, transferring risk and sharing information. 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.

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 (Gaiser, 2015).

References

1. *Andrew, C. (1985). Secret Service: The Making of the British Intelligence Community. London: Sceptre.*
2. *Clark, R., Knake R. (2010). Cyberwar: The Next Threat to National Security and What to Do About It. New York: Ecco.*
3. *CLUSIT. (2016). Rapporto Clusit 2016 sulla sicurezza ICT dell'Italia. Milano: Astrea.*
4. *De Seversky, A. (1942). Victory Through Air Power. New York: Simon&Shuster.*
5. *Franchina, L. (2012). La protezione delle Infrastrutture Critiche e la sicurezza adattiva: l'uso delle tecniche di analisi previsionale. GNOSIS, 2012/2.*
6. *Gaiser, L. (2016). Economic Intelligence and World Governance – Reshaping States for a New World Order. RSM: Il Cerchio.*
7. *Gaiser, L. (2015). Intelligence Economica. Ariccia: Aracne.*
8. *Gori, U. (2015). Dall'intelligence economica alla cyber intelligence: sfide e promesse per le imprese. In U. Gori, S. Lisi (ed.). Cyberwarfare 2014. Milano: Franco Angeli.*

9. *Jean, C., Savona, P. (2011). Intelligence Economica – Il Ciclo dell'Informazione nell'era Globale. Soveria Manelli: Il Rubettino.*
10. *Liang, Q., Xiangsui, W. (1999). Unrestricted Warfare. Bejing: PLA Literature and Arts Publishing House.*
11. *Libicki, M. (2009). Cyber deterrence and Cyberwar. Santa Monica: RAND*
12. *Luttwak, E. (1993). The Endangered American Dream. New York: Simon&Schuster.*