UNDERSTANDING SECURITY POLICIES IN THE CYBER WARFARE DOMAIN THROUGH SYSTEM DYNAMICS

Stefano Armenia [(a)], Alessandro Cardazzone [(b)], Camillo Carlini [(c)]

[(a)] DIAG – Department of Computer, Control and Management Engineering "Antonio Ruberti" Sapienza University of Rome., Via Ariosto, 25 - 00185 Rome, Italy - President of the System Dynamics Italian Chapter (SYDIC) – www.systemdynamics.it
[(b)] DIAG – Department of Computer, Control and Management Engineering "Antonio Ruberti" Sapienza University of Rome., Via Ariosto, 25 - 00185 Rome, Italy

[(c)] DIAG – Department of Computer, Control and Management Engineering "Antonio Ruberti" Sapienza University of Rome., Via Ariosto, 25 - 00185 Rome, Italy

[(a)] armenia@dis.uniroma1.it, [(b)] *alessandro.cardazzone@gmail.com*, [(c)] *carlini@dis.uniroma1.it*

ABSTRACT

In this paper we deal with the analysis of the Italian Presidential Decree on CyberSecurity (January 2013). Reading it, we had the impression that, again, policy makers lack systemic skills and the ability to evaluate the impacts of their choices and assumptions before implementing their decisions. The Italian Cyber Security Act (DL.2013) establishes, in case of cyberthreat to national security, to activate the Inter-Ministerial Committee for the Security of the Republic (CISR), which should take decisions in a timely and effective manner. In this paper, we won't argue about the effectiveness of such board, which would have to be discussed by analysing both the specific competences brought to the Board by the various official stakeholders and by the processes put in place in order to favour the work carried out by such Board, rather we will discuss the inherent delays in the system ultimately made even worse by the need to activate such Board for certain critical decisions.

Keywords: Cyber Security, Cyber Warfare, Homeland Security, System Dynamics

1. INTRODUCTION

Every economy of an advanced nation relies on information systems and interconnected networks, thus in order to ensure the prosperity of a nation, making cyberspace a secure place becomes as crucial as securing society from the presence of criminal bands. Cyber security means ensuring the safety of this cyberspace from threats, which can take different forms. Stealing secret information from national companies and government institutions, attacking infrastructure vital for the functioning of the nation or attacking the privacy of the single citizen can all be seen as extreme examples of a large spectrum of threats. Additionally, perpetrators of attacks on cyberspace are now professionals working for governments, hacktivist organizations or criminal bands rather than teenagers looking for some short-term celebrity as it was in the old days. Intelligence operations are conducted through cyberspace in order to study the weaknesses of a nation and, to complete the picture, in the military domain cyberspace is now seen as one of the dimensions of the battlefield just like space, sea, ground and air. Understanding the complexity of the picture of making cyberspace a safe place turns out to be a problem, which is not only technical but rather a social, legal and economic one. Improving cyber security knowledge, skills and capability of a nation will be essential for supporting an open society and for protecting its vital infrastructures such as telecommunication networks, power grid networks, industries, financial infrastructures etc. (CIS Sapienza, 2013).

Each countries' critical infrastructures (from oil pipelines to the electricity grids, from gas to water, from transportation, to financial/banking systems, to public services) is becoming managed at an IT level in an increasing way. The massive and progressive introduction of network, monitoring and control systems has improved the performance level of such infrastructures, but has also introduced new ways (cyber) for criminals to carry out their misfits. Today, an effective infrastructures protection includes threat identification, vulnerability reduction and attack source identification, thus aiming at service downtime minimization and damage limitation.

The expression "cyber threat" denotes the set of behaviors that can be carried out in and through cyberspace. It mainly consists in cyber attacks, that are actions of individuals, states or organizations, aimed at destroying, damaging or interfering with the proper functioning of systems, networks and related processes, or at violating integrity and confidentiality of data/information (CIS Sapienza, 2013).

Depending on the actors and purposes, we can distinguish the following types:

- Cybercrime: all the activities with criminal purposes (such as, for example, fraud or wire fraud, identity theft, the misappropriation of information or of creative and intellectual property);
- Cyberespionage: unlawful acquisition of sensitive property or classified data or information;

- Cyberterrorism: the set of ideologically motivated actions, aimed at influencing a country or an international organization.

Typically, a cyber attack is launched:

1. to paralyze one or more critical infrastructures' activities;
2. to steal infrastructures information assets.
3. To cause a cyber war, a real conflict between nations that aims at paralyzing their respective vital sectors (when targets are critical infrastructures and warning systems, it is clear that the consequences for the entire society could be disastrous).

It is important to identify in advance which are likely to be possible targets of an attack so to assess the related risks and consequences, also in terms of time required to restore normal behaviour (resilience). Cyber threats are important challenges for the country, because they involve both the digital domain and because of their transnational nature. Cyber threats are not easy to counter: the actors, means, objectives and attack techniques vary continuously.

In light of the above and of the awareness that this is a continuously changing environment, it is urgent to intervene, at the national level and beyond, against all cyber crime forms, which represent a growing threat to critical infrastructure, society, business and citizens (CIS Sapienza, 2013).

2. LEGISLATIVE CONTEXT AND RESEARCH QUESTIION

In this paragraph we will briefly introduce the legislative context that ultimately brought us to consider posing our research questions.

Two main regulatory measures, adopted in Italy between 2012 and 2013, contribute to defining the organization and strategy for Italy's national cyber security. Law n.133/2012 and the DPCM (Decree from the President of the Ministries Council) dated 24 March 2013.

Law 133/2012 attributes new and more detailed responsibility in the field of national cyber defence and security to the Italian intelligence system. For instance this law gives the prime minister the power to issue directives to the Intelligence and Security Department (Dipartimento Informazioni per la Sicurezza - DIS), after prior consultations with the Inter Ministerial Committee for the Security of the Republic (CISR), and to the security intelligence services, in order to strengthen security intelligence activities for the protection of critical infrastructures, with particular reference to national cyber defence and security.

The DPCM 24 January 2013 defines the institutional architecture tasked with safeguarding national security in relation to critical infrastructures and intangible assets, with particular attention to the protection of cyber security and national security. It indicates the tasks assigned to each component and the mechanisms and procedures to follow in order to reduce vulnerability, to improve risk prevention, to provide timely response to attacks and to permit immediate restoration of the functionality of systems in the event of crisis.

It is worth mentioning the setting up of a so-called Nucleus for Cyber Security (Nucleo per la Sicurezza Cibernetica) within the Military Adviser's Office. It is a permanent body responsible for maintaining links and coordination between the different components of the institutional architecture involved in various capacities in the field of cyber security, in accordance with the powers conferred by law to each of them. Members of National Intelligence, Ministry of Internal Affairs and Foreign Affairs, Ministry of Defense, Ministry of Economic Development, Ministry of Economy and Finance, Civil Protection and the Digital Agency are part of the Nucleus for Cyber Security. The nucleus was established to support the prime minister in all activities concerning the prevention and/or preparation for a possible crisis and the activation of warning procedures. The nucleus, among other activities, will:

1. Promote the planning of the response to crisis situations by both government and private stakeholders and the development of all necessary procedures for inter-ministerial coordination, fitting in with the schedules of Civil Defense and Civil Protection;
2. assess and promote procedures for information sharing, including with private stakeholders, for the dissemination of alerts relating to cyber events and crisis handling;
3. promote and coordinate cybersecurity exercises, both Inter-Ministerial and at international level, involving the simulation of events.

In order to handle a crisis event in a coordinated manner, the decree assigns to the NISP the role of Inter Ministerial Cybernetics Crises Table. The inter-ministerial body is chaired by the prime minister's military advisor and will include representatives of all the institutions involved. It will ensure that the response and the appointment of the various departments' and agencies' responsibilities, in relation to cybernetic crisis, are performed in a coordinated manner. The decree, furthermore, establishes a strict collaboration between the Inter Ministerial Cybernetics Crisis Table and the national CERT (see next section) in order to deal with all technical aspects in elaborating emergency responses. (CIS Sapienza, 2013)

Thus, the rationale of this paper finds its roots in the analysis of the Italian Public Presidential Decree of Law on Cyber Security, dated January 2013 namely "Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale" (Dec. PCM, 2013).

By reading such D.L., we got the impression that, again, policy makers lack both systemic skills and nonetheless the ability of being able to evaluate the impacts of their choices and assumptions (ultimately turning into the application of a law and thus into money spent, choices done, people moved around, etc.) before implementing their decisions. The Italian D.L.

Sec. 2013 (DL.2013) basically focuses the attention on the possibility, in case of national security put under threat by a cyber menace, to recur to an inter-ministerial working group (Inter-Ministerial Committee for the Security of the Republic - CISR) which, in case of deep crises, should be able to take decisions in a timely and effective manner. In this paper, we won't argue about the effectiveness of such Board, which would have to be discussed by analysing on one hand the specific competences (if any) brought to the Board by the various official stakeholders and on the other by the processes put in place in order to favour the work to be carried out by such Board, rather we will argue about the inherent delays in the system ultimately even made worse by the need to activate such Board for certain critical decisions.

3. GENERAL A SYSTEM DYNAMICS MODEL TO GET INSIGHTS ON THE CYBER SECURITYAND CYBER WARFARE DOMAIN

A computer emergency response team (CERT) can be defined as an organization responsible for setting up a framework for responding to cyber security incidents. It provides the necessary services for handling incidents and supports its constituents in their recovery from breaches of computer security. In order to mitigate risks and to minimize the number of required responses, many CERTs also provide preventative and educational services for their constituents. More recently the term CSIRT, which stands for Computer Security Incident Response Team, is starting to replace CERT. It invokes a more holistic approach to security rather than relying only on reactive forces. CERTs worldwide are generally founded and financed by governments or academic institutions. The reason for this is that government agencies are interested in protecting national security and universities by their very nature try to find solutions to new problems. Historically, the name Computer Emergency Response Team is the designation for the first team at Carnegie Mellon University (CMU). CERTs existence is linked to malware, especially computer worms and viruses. After the Morris Worm paralyzed a good portion of the Internet in 1988, CERT/CC at Carnegie Mellon University was started under a US government contract.

To respect the indications of EU Directive 140/2009 and to achieve the target fixed by the European agenda, in several EU member states, governments have set up the so-called National CERTs. The main goal of a national CERT, from a cyber security perspective, is to protect national and economic security, the on-going operations of a government, and the ability of critical infrastructure to continue to function. Therefore a national CERT typically monitors incidents at a national level, identifies incidents that could affect critical infrastructure, warns critical stakeholders about computer security threats, and helps to build organizational CERTs in the public and private sectors (CIS Sapienza, 2013).

We will start our analysis by setting up a possible preliminary scenario (to be validated by eventually specializing the model to a real-case scenario in this area) where there are several generic attacks that are being carried out against a certain nation and where the national CERT acts in defence by monitoring incidents and trying to contrast them in order to mitigate the extent of the overall damages.

The purpose of the model is thus to analyze the impact of some cyber attacks on national defense system and the way the latter responds to such attacks.

The main process that will be modelled includes the arrival of some cyber attacks (Incoming Attacks) , according to a stochastic Poissonian distribution. All the attacks will be considered of equal weight in terms of damage caused. Once started (Started Attacks), they are discovered in time thanks to the allocation of specific resources for this task of detection (detection Rate), which is a function of the "Capability to Detect attacks". It is, in turn, the mathematical product between the number of "resources for detection" and the "detection Productivity". Attacks that are not detected (Undetected Attacks), a simplified function of an "average percentage of non detected", are still effective at the level of damage caused and may be rediscovered in time (re-discovery rate) or ending their life cycle (Max Attack Duration) having never been detected (Undetected non-mitigated), since, for example, the attack has completed his mission.

The rate "Undetected Attacks going unmitigated", as seen in Figure 1, depends on an average of time duration of the attack (Max attack duration AVG). In this sense, the greater the duration of the attack in time, the lower the number of attacks that pass in the state "non-mitigated".

The "detected attacks", in turn, will be contrasted (mitigation rate), by using some resources (Capability to Mitigate Attacks, in turn a function of the mathematical product between the resources dedicated to the mitigation and the resources productivity). In this way, Mitigation resources try to mitigate attacks and therefore to limit the attacks damage.

However, we have assumed that some of the detected attacks, cannot be mitigated (see Figure 1), so at the end of their life cycle (Max Duration of Attack) they finish their share of damage and disturbance (not mitigated).

Each "active" attack, in any state of the system (Started, Detected, Undetected, etc..), produces a certain amount of 'effective' damage (Max Damage for Attack) during its life cycle (Max Duration of Attack) (again, Figure 1).

Among the initial hypotheses of the model, we will assume as directly estimated the damages that the observer would expect as a cause of the detected attacks in progress (Expected Damages).

However, the discrepancy between the "Effective damages" to infrastructures (i.e., the amount of damage that can be observed) and the damage that the observer would expect is an information quite relevant to the job of threat contrast: in this way, if the damages that the structures received, are bigger (over a certain threshold) compared to those that would be expected from the detected attacks, then there must necessarily be some attacks that were not detected and that are producing damages unnoticed. The estimation of threat severity (threat of Effective severity ratio) calculated as the ratio of actual damages (Effective Damages), and estimated damage from attacks detected (Expected Damages) is a determining factor of acceleration in the process of acquisition of resources which can be allocated either to the detection or the contrast of the attacks. (see Figure 1).

Among the initial assumptions, we expected in normal circumstances that there is a certain amount of resources dedicated to the one side on detection process (Active resource for detection) and to the other side on mitigation process (Active resource for mitigation) of cyber attacks. As described above, the model provides a self-regulating mechanism whereby if detection or mitigation resources are not able to handle an unexpected peak in attacks, resources are acquired from outside (Resource Acquisition).

But the process of acquiring resources from the outside, obviously requires time (Acquisition process delay time) (Figure 1)

4. RESULTS, DISCUSSION& FUTURE WORK

We have simulated our model with the following assumptions and initialization values (unit: 1 hour):

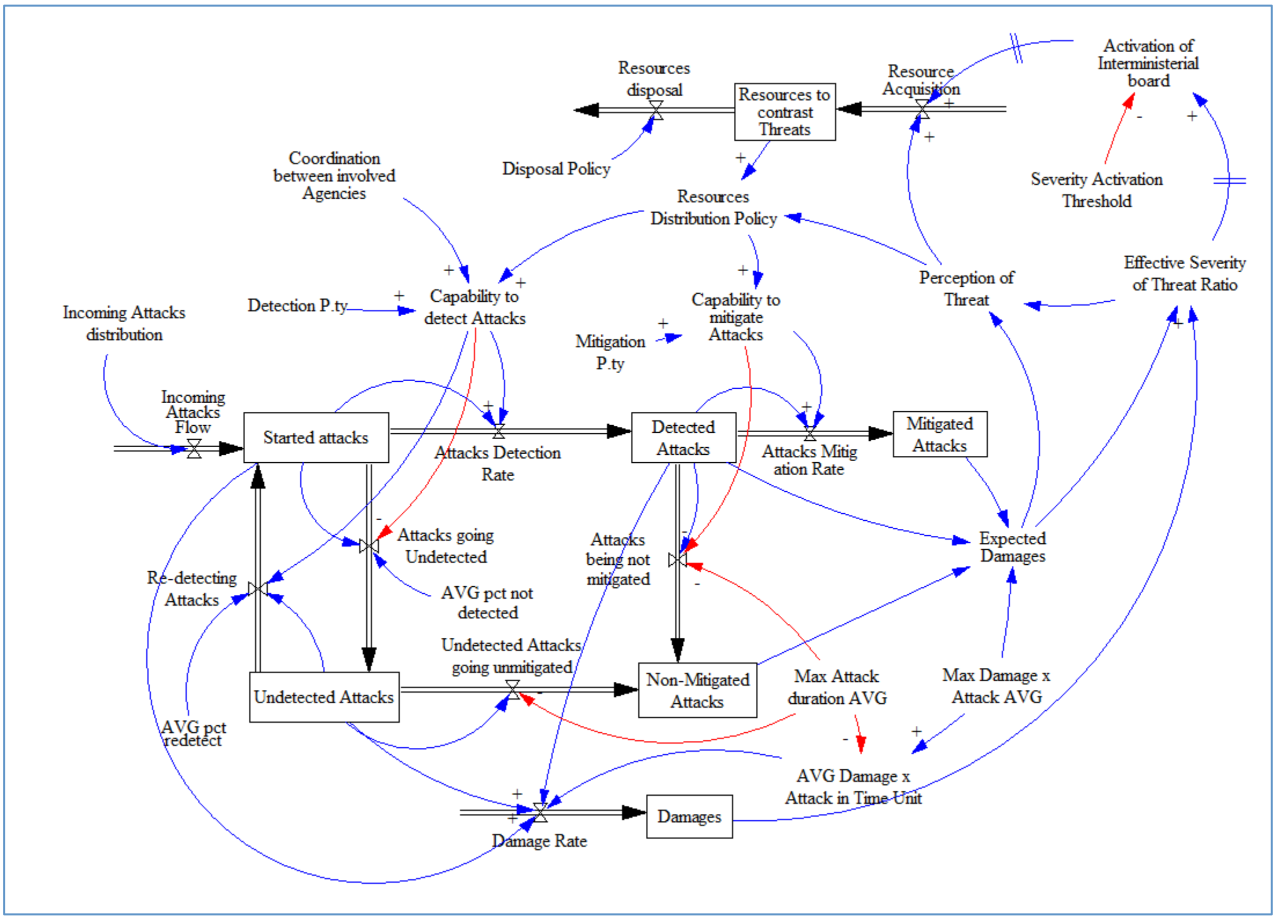

Figure 1: Resource Distribution Policy

- Attacks_Increase = STEP(Offensive,168) - STEP(Offensive,336)
- Acquisition_process_delay_time = 72+(Activation_of_Interministerial_board*96)
- AVG_pct_not__detected = 0.1
- Delay_in_Activating_the_board = 24
- Incoming__attacks_distribution = poisson (Mean_of_attacks+Attacks_Increase)
- Max_Attack_duration__AVG = 96
- Max_Damage_x__Attack_AVG = 10

- Mean_of_attacks = 20
- Offensive = RANDOM (100,150)
- Severity__Activation__Threshold = 2
- Std_Detection_Pty = 6
- Std_Mitigation_Pty = 3

From Figure 2, we notice that we have the desired increase in the number of average attacks after the first week of simulation, which structurally brings, due to the new desired values for resources in detection and mitigation, to a growth in the related rates.

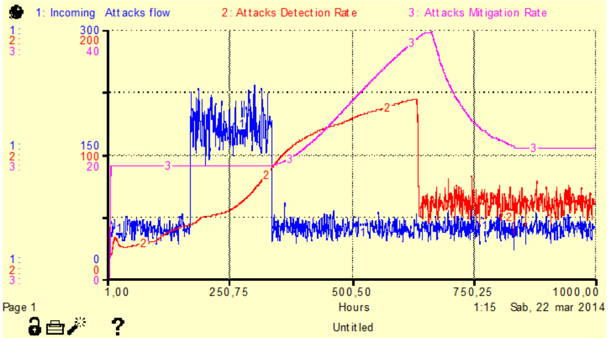

Figure 2: Attacks flow rates

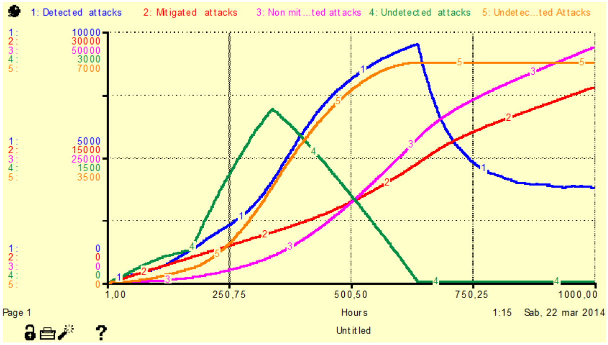

Figure 3: behaviors of “attacks” stocks over time

From Figure 3, we can notice that the backlogs are somehow managed over time thanks to the growth in resources contrasting (detecting and mitigating) the attacks.

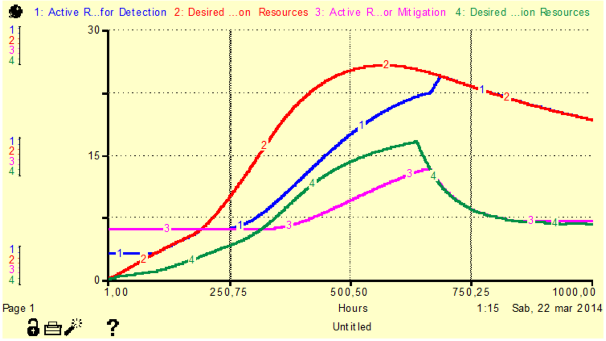

Figure 4: behaviors of resources dedicated to detection and mitigation

From Figure 4, we see that the model gives priority to detecting attacks as at a certain moment, there is a clear perception that the Nation is under attack but the CERT cannot correlate the damages they experience to a real threat that they recognize (so priority is given to detection so to be able to “empty” earlier the Started and Undetected Stocks, which contribute heavily to procure damages “unseen” in the first moments of the simulation.

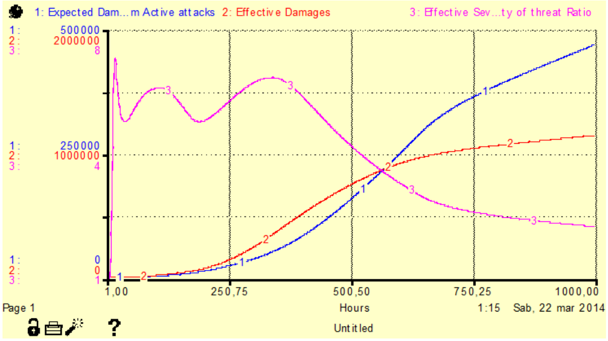

Figure 5: Effective damages vs. Expected Damages

We can see that the Effective Severity of Threat is quite high at the beginning but then decreases as the “unseen” stocks get emptied out over time (Figure 5)

As a final remark, we are obviously still in the tuning phase of our model but we can see the promised potential for understanding the structure of attacks and response to a cyber menace.

From the above results, we can only have a partial conclusion which tells us that the model seem to behave correctly but a more accurate tuning phase, a sensitivity analysis and more structured approach to experiments will be able to tell us more in the near future (possibly by the upcoming conference in summer).

In future developments, in order to provide a way to measure the effectiveness of the response of an organization (i.e.: a CERT) to a cyber threat, we will introduce in the some KPI’s that are interesting to consider (5), and namely what is called the cyber security readiness index, which is a composite measure of the capacity and willingness of an organization to face cyber threats.

It consists of the composition of the following KPIs:

- Awareness index: Assesses the situational awareness related to cyber risks of the organization;
- Defense index: Assesses the capacity of an organization to protect itself from a cyber attack. Notice that the defense index is somehow correlated with the awareness index, since the implementation of strong defence mechanisms shows cyber security awareness;
- Policy index: Assesses the implementation of security related policies. A high score in this index shows compliance to several security policies and their constant update. There is a strong correlation of the policy index with the awareness index since the adoption of updated security policies show an increased awareness;

- External independency index: Assesses the correlation between internal systems and external providers. A low score on this index shows the correlation of the organization mechanism to external providers since the fault of an external cloud provider could impact on its possibility to deliver the core product of its business. A high score on this index shows an organization that relies minimally on external services that could impact on its security. Note that such high scores imply larger operational costs as the organization has to insource software services without the involvement of third parties.

REFERENCES

DECRETO DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI 24 gennaio 2013 "Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale", 2013

Council Directive 2008/114/EC, 2008, On the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, Official Journal of the European Union.

Brunner, M., Suter, E. M., 2008, "International CIIP Handbook 2008/2009", Center for Security Studies, ETH Zurich.

Byres, E.J., Lowe, J., 2004, "The Myths and Facts behind Cyber Security Risks for Industrial Control Systems", VDE 2004 Congress, October 2004, Berlin.

CIS Sapienza, 2013, The 2013 Italian Cyber Security Report: the Critical Infrastructures and other sensitive sectors readiness, Università di Roma La Sapienza, Available from http://www.dis.uniroma1.it/~cis/media/CIS%20Resources/2013CIS-Report.pdf

ENISA (European Network and Information Security Agency), 2010, "Incentives and Challenges for Information Sharing in the Context of Network and Information Security".

European Commission, 2006, "Proposal for a Directive of the Council on the identification and designation of European Critical Infrastructure and the assessment of the need to improve their protection" .

European Commission, 2005 "Green Paper on a European programme for critical infrastructure protection", COM(2005)576, Bruxelles.

European Commission, European Communication from the Commission to the Council and the European Parliament of 20 October 2004, 2004, "Critical Infrastructure Protection in the fight against terrorism", COM (2004) 702.

European Union, 2013, "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace", JOIN/2013/0001.

ENISA, 2012, "National Cyber Security Strategy. Practical Guidebook", December 2012, p8.

European Union Directive, 2008, 2008/114/EC.

Franchina, L., 2008, "Dalla Direttiva UE alla 'governance' nazionale, Infrastrutture Critiche sotto protezione", [online], GNOSIS, italian journal of Intelligence

Franchina, L., 2007, "Come si proteggono le infrastrutture critiche", [online], GNOSIS, italian journal of Intelligence

Italian Information and Security Department, 2011, "Report on information policy for security in the year 2010", Presidency of the Council of Ministers, pp. 23-35, 2011, Rome.

Italian Ministry for the Interior Decree G.U. 30 aprile 2008, n. 101, "Individuazione delle infrastrutture critiche informatiche di interesse nazionale".

Italian Presidency of the Council of Ministers, 2012, Sistema di informazione per la sicurezza della repubblica, "Il linguaggio degli organismi informativi. Glossario intelligence", Quaderni di Intelligence Gnosis.

Italian Presidency of the Council of Ministers, 2004, "Protezione delle Infrastrutture Critiche Informatizzate".

Kern, R., Peltz, V., 2003, "Disaster Recovery Levels", IBM Systems Magazine.

Microsoft, 2012, "Microsoft Security Intelligence Report", Regional Threat Assessment: Italy", Volume 14, July through December.

Ponemon Institute, 2012, "2011 Cost of Data Breach Study, Italy", available from: http://www.ponemon.org.

Rinaldi, S.M., Peerenboom, J.P., Kelly, T.K., 2001 "Identifying, Understanding and Analyzing Critical Infrastructure Interdependencies", IEEE Control Systems Magazine, Vol. 21, No. 6, 11-25.

Shackelford, S.J., 2012, "In search of cyber peace" Stanford Law Review, available from: http://www. stanfordlawreview.org/online/cyber-peace.

US Information Technology Industry Council, 2011, "Steps to Facilitate More Effective Information Sharing to Improve Cybersecurity", available from www.itic.org.

US Presidential Decision Directive 63 (May22), 1998, "Critical Infrastructure Protection".

US Presidential Policy Directive 21 (February 12), 2013, "Critical Infrastructure Security and Resilience".

UK Cabinet Office, 2011, "The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world", United Kingdom, London, Cabinet Office.

United Nation, 2008, "Overview of cybersecurity", ITU Recommendation ITU-T X.1205", Geneva 2008, ITU-T, p.2,.

Westby, J. R., 2012, "Governance of Enterprise Security: CyLab 2012 Report", Carnegie Mellon University CyLab, available from: https://www.cylab.cmu.edu/outreach/governance.html.