InDret
REVISTA PARA EL
ANÁLISIS DEL DERECHO

WWW. INDRET.COM

Cyber Risks: Liability and Insurance

The extraordinary risks in a hyperconnectivity world

Jesús Jimeno Muñoz

Lawyer and Doctor of Law

BARCELONA, ABRIL DE 2019

Abstract

The aim of this article is to provide a current and broad analysis of cyber risks, through its civil liability and insurance. In this order, the article firstly explains briefly the concept and scope of cyber risks. Secondly, it addresses the concept and scope of cybersecurity as consequence of the existence of cyber risks, taking into account as an essential element the IT development. Thirdly, the relationship between cyber risks and cybersecurity requires a digital environment called cyberspace. Cyberspace (with physical and un-physical implications) is affected not only by the IT development but also by the connectivity and hyper connectivity; so the paper analyse how those circumstances defined the developed of extraordinary and catastrophic IT threats. Fourthly, the article analyses the insurance coverage and the compensation systems of these cyber risk categories.

Keywords: Cybersecurity, Cyber Terrorism, Insurance, Reinsurance, Extraordinary and Catastrophic Risks, Civil Liability and Tort Law

Sumario

1. Introduction

Cyber risk has been defined as the risk associated with the IT use, property, operatively, influence, participation and the implementation of IT systems. For this reason, it is possible to consider that the progressive development of IT systems has caused the increase and evolution of cyber risk. Actually, since the creation of the first computers to the actual Internet of Things (hereafter IoT) IT has been applied for a huge number of socioeconomic actions and daily routines. Therefore, the cyber risks have extend the traditional technology threats to the every single good and right protect by either public or national interest.

In a group of cases the IT systems represents just a new way to produce damages into the referred interests, with the same motivation (cyber terrorism) **and prejudicial consequences** (physiological and physical damages) **to the traditional threats used to have**. In those cases, **the threats could be covered by the traditional insurance policies and catastrophic reinsurances** (whenever there will not be a new object or damage specifically excluded), so it will be relevant to study the impact of the IT threats into the traditional catastrophic events and its coverage.

Otherwise, the IT systems have created a hyper-connectivity world so there are an uncountable number of goods and rights possibly affected by the cyber events. Indeed, they could affect to the Critical Infrastructures or they could also produce a unlike reaction in millions of devices -IoT- around the world. Probably, those situations would cause a particularly kind of catastrophic effect that we could classify as an extraordinary risk, and it is going to entail certainly consequences for the liability and the insurance industry.

2. The cyber risk

The first point of the analysis provided by this paper consists of explaining the concept and the scope of cyber risks. In a broader sense, cyber risk or IT risk has been defined as the risk associated with the IT use, property, operatively, influence, participation and the implementation of IT systems (ISACA IT Risk Framework)[1]. This means that every technology system connected one to another underlies under this category. Aware of the extensive concept of cyber risks and its own limitation, the he National Institute of Standards and Technology (hereafter, NIST)[2] understands that risks affecting IT are characterized by the level of impact on the organization's operations (mission, functions, image and reputation), the assets of the organization and the information systems.

Therefore, in a strict sense, the concept of cyber risk is the probability of an accidental or intentional threat as a consequence of an IT's vulnerability. This tendency has been consolidated by the

[1] COBIT 5 for Risk, ISACA (2013) http://www.isaca.org/COBIT/Documents/COBIT-5-for-Risk-Preview_res_eng_0913.pdf

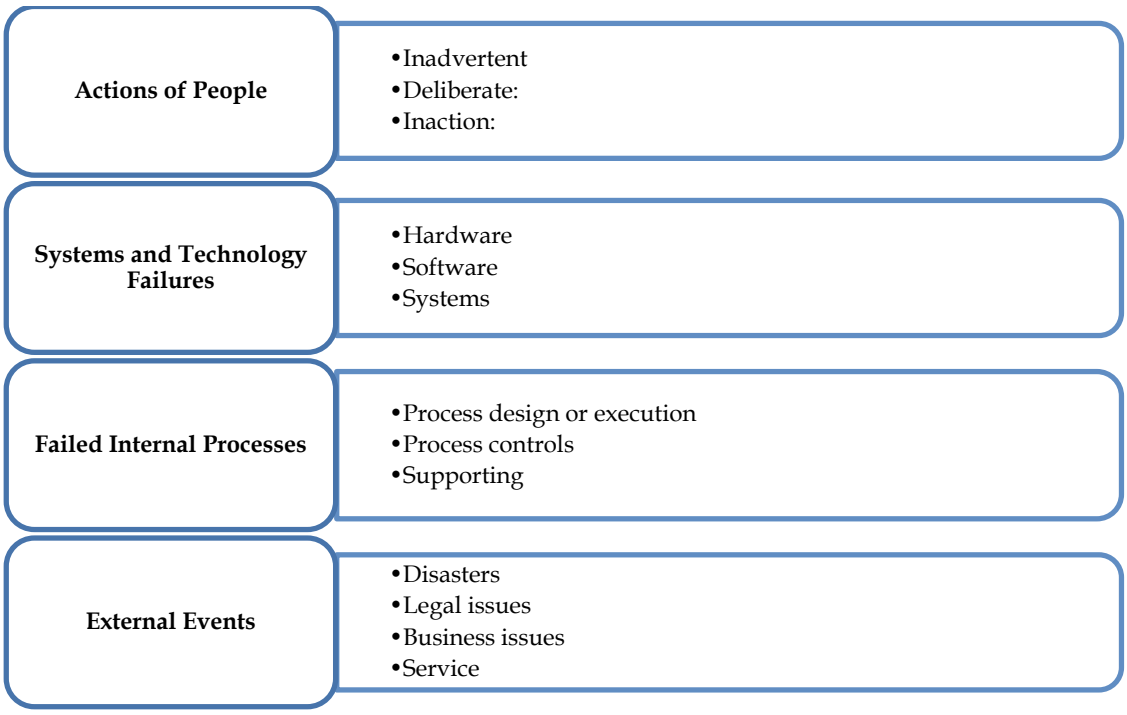
[2] Gary STONEBURNER, Alice GOGUEN y Alexis Feringa RISK, (2002), *Management Guide for Information Technology Systems*, National Institute of Standards and Technology NIST SP 800-30 http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

International Organization for Standardization (hereafter, ISO), which points out IT risk as the potential threat caused by a technology vulnerability of any asset which would produce damage in an organization[1].

Another definition may be provided following the guidelines establishes by the report called A Taxonomy of Operational Cyber Security Risks (CEBULA, 2010)[2] understanding cyber risks as the human actions or omissions may, or may not be, the voluntary cause of a failure in the technological systems and internal processes of safety, which causes external damage or effect. This definition introduces a nuance between cyber risks and IT risks highlighting the damage action area.

2.1. The Scope and effects of cyber risk

The cyber risks, damages are caused on the cyberspace extending their effects on the IT systems, while IT risks damages directly arise on the IT systems. On one hand, cyberspace is undefined concept, which may affect material, social, personal, corporate, political, institutional or economic framework. On the other hand, IT risks may be classified in four basic elements: the human action, the failures of IT systems and internal security process cause by it, and the consequently occurrence of external effects. These elements may be represented by the following figure:



[1] ISO/IEC 27005:2011, Terms and definitions, ISO, Online Browsing Platform (OBP), https://www.iso.org/obp/ui/#iso:std:56742:en

[2] James J. CEBULA y Lisa R. YOUNG, (2010), *A Taxonomy of Operational Cyber Security Risks*, Carnegie Mellon University, Software Engineering Institute, Pittsburgh, PA, http://bit.ly/1NEBcTU

Figure 1: The Characteristics of Operative IT Risks Taxonomy of Operational Risk[1].

The second issue to analyse is the scope of cyber risks, and as a condition to delimitate the above-mentioned scope, it is necessary to examine the different circumstances and causes -related to IT- which arises cyber-risks.

Cyber risks may come from cyber events or cyber threats which are based on four different groups of elements taking into account the current IT development:

a. **General interest and national security** have raised doubts about how the insurance industry and the government should cooperate against cyber threat. In fact, that relationship between general interest and national security represents a significant discussion concerning who must assure the cyberspace. Even though, from a current and practical point of view, some risks produced by cybercrime and cyber terrorism may be considered as extraordinary risks, which have ensured by systems such as cyber pool and funds.

b. **The data** has been considering as the main pillar for the development of cybersecurity. In fact, the first tendency for developing cyber insurances was guided by the evolution of indicatory data protection. Traditionally, some of these circumstances and causes used to be linked to Personal Data.

   Indeed, Personal Data was the first aspect of cyber risks regulated by the US legal system. However, evolution has clarified that possible damages caused by cyber risks are countless and they overcome the breaches of Data Protection rights or the mere violation of the right to privacy. Actually, cyber insurances are essential for the cyber policies focusing on the claims relating to the personal data rights issues (e.g loss, theft). It is remarkable to point out that data protection is also based in other different goods and rights. Especially, the Intellectual and Industrial property rights (IP´s rights) which are regulated by other legal instruments. Therefore, cyber policies through cyber insurances must address damages caused by cyber events, including data protection issues as well as infringement of IP rights´.

c. **The IT structures and systems**, part of the physical infrastructure of cyberspace, may be exposed to suffer damage or impairment. Thus, the development of IT through IT systems (i.e.IoT) is likely to cause, through cyber events, physical and material damages. As an example, the developing IT structures and systems of self-driving cars shall be adapted to the insurance industry for correctly implementing and applying a new form of liability.

d. **The non-physical damages** come from the particular effects of hyper-connectivity and the dependence of each socioeconomic aspect related to the cyberspace, this relation could produce serious consequences for the users and third parties in the case of the wrong or

[1] CEBULA y YOUNG (2010).

the paralysation of systems. In some of these cases, the cyber events produced reputation and professional prestige losses which are essential damages for the future of cyber risks policies.

As a result of the awareness of the existence of cyber risks, IT and cyber security has been developed in order to address the issues arisen by the constant progress of the IT systems. In fact, a deeper analysis of the scope of cyber risks must be focused on the physical damage caused as a result of cyber risks to third parties, not only in breaches of Personal Data or other circumstances. **For all of these reasons, there is an uncountable number of goods and rights possibly affected by the cyber events because of the connectivity between systems as common characteristic.**

However, in basis of the damages caused by cyber events, cyber risk may be classified by two spheres. The private sphere which comprises the damage suffered by individual subjects, and the public one formed by the socio-economic threats posed by cyber risks –the public sphere of them-. These two spheres may arise liability, through the following elements: the action or the event generator of risks, the cyber-attack works and the cyber event effects.

2.2. The cyber risk management and cybersecurity

Afterwards the analysis of the concept and the scope of cyber risks, these cyber risks should be addressed by cybersecurity, as the main concern of the management of the IT threats. The cybersecurity should be issued in this paper as the systems focus on control and mitigate the effects of any kind of IT threats, so it undertakes the positive perspective of the cyber risks control.

Nevertheless, cybersecurity requires a further explanation of the IT systems and its development; the term "information technology" (afterwards "IT") was introduced by Harold J. LEAVITT and Thomas L. WHISLER (1958)[1]. These authors considered that this concept contains three categories: processing techniques; the application of statistical and mathematical methods for decision making; and the simulation of higher thinking through computer programs. These IT characteristics have been affected by different changes since their beginning (BUTLER)[2]. Currently, IT characteristics are associated with tools which allow to sharing information through networks and connections; that is, the so-called cyberspace.

In this manner, the concept of IT and its main characteristics lead us to delimitate the definition and scope of cybersecurity. In fact, "cybersecurity actions" or "cybersecurity" may be defined as the situation of absence of threats cause by, or related to IT and their networks (SÁNCHEZ ROJAS, 2010)[3]. Furthermore, cybersecurity has been considered as an amorphous system (VACCA, 2012)[4],

[1] Harold J. LEAVITT y Thomas L. WHISTLER (1958), *Management in the 1980s*, Harvard Business Review, p. 11.

[2] Jeremy G. BUTLER, "A History of Information Technology and Systems", University of Arizona.

[3] Emilio SÁNCHEZ ROJAS (2010), "¿Ciber…qué? La ciberseguridad", Ejército, vol. 837, p 138.

[4] Alexander W. VACCA (2012), "Military Culture and Cyber Security", Survival, vol. 53, nº6, p. 159.

because initially, it used to not pay attention to systemic and global risks. Indeed, "cybersecurity actions" are created by individual contingencies plans, which represent isolated solutions which may arise in particular technological systems. Nevertheless, cyber risks are continuously evolving through a dynamic environment. Likewise, with the aim of avoiding cyber risks, "*cybersecurity actions*" or "*cybersecurity*" *are* implemented building a safe digital environment. However, the international essence of cyber risks requires cooperation and the development of a global IT security for tackling the main issues.

The increasing relevance and extension of cyberspace have extended these global threats. Currently, cyber risks could affect all kinds of systems and subjects which participate in the digital environment so-called cyberspace. Thus, terrorist or military actions which take place on the cyber space could be considered as a National Security issue[1]. Furthermore, it is possible to classify as a National Security issue, these actions which affect public order, civil population or strategic systems and/or structures. This is due to the fact that they are essential for socioeconomic stability. In this case, the Critical Infrastructures (CI) threats may be considered by National Security (TIKK, 2011)[2].

The global cyber threats and the presence of hostile actors (whether governments, organizations or common criminals) has been increasing on the network, having forced some of the worldwide governments to analyse potential vulnerabilities of illegal activities which are taking place on the cyberspace. Nevertheless, it is a controversial topic, the control of cyberspace and the limits of regulation and activities which may be carried out by the State for guaranteeing cyber security. Thus, the lack of clear limits of the cyberspace complicates to figure out a global solution for delimitating differences between Public and Private interests of this environment[3].

The discussion between freedom and intervention has been defining as cyber-dilemma, it tries to understand in which situations the individual freedom/liberty should be favoured, and when the State should intervene to ensure the security of cyberspace and the integrity of the subjects operating in it (MOLINA MATEOS, 2013)[4]. Finally, this consideration will determine the regulatory perspective of cyber risks management and the compensation systems applicable to the cyber breach effects.

---

[1] SÁNCHEZ ROJAS (2010, p. 140).

[2] Eneken TIKK (2011), "Ten Rules for Cyber Security", Survival, vol. 53, nº3, p 119.

[3] Eguskiñe LEJARZA ILLARO (2014), "Ciber guerra los escenarios de confrontación", Instituto Español de Estudios Estratégicos, nº 14, p. 2-4 http://www.ieee.es/Galerias/fichero/docs_opinion/2014/DIEEEO18-2014_Ciberguerra_EscenariosConfrontacion_EguskineLejarza.pdf

[4] José María MOLINA MATEOS (2013), "Ciberdilema", Instituto español de estudios estratégicos nº 115, p.1 http://www.ieee.es/Galerias/fichero/docs_opinion/2013/DIEEEO115-2013_Cyberdilemma_JM.MolinaMateos.pdf

3. The IT in the connectivity world: Cyber space and Digital ecosystems

The general perspective of the digital development, its nature and elements will be necessary to comprehend the effects of cyber risks. The future effects of IT threats will depends on the cyber environment limits and the digitalization of traditional process, so It is possible to consider that the progressive development of IT systems has caused the increase and evolution of cyber risk. Indeed, since the creation of the first computers to the actual IoT (Internet of Things), IT has been applying for more number of basic socioeconomic actions and daily routines. Therefore, cyber risk could affect the private lives of each citizen for either Public or National interest.

The connection between different kinds of systems has expedited the creation of cyber space where interactions of every type of subjects (e.g. individual, corporative, institutional- take place. Therefore, the public and private interests are connected to cyber space suffering cyber damages jointly. These characteristics of cyber events have been spreading out through every kind of system, and it is the reason why they are considered at the category of global risk, and in some cases they should be taken as an extraordinary risk. Therefore, cyberspace has two different areas:

- Physical: the cyberspace is comprised by IT systems such as IT infrastructures and the elements and systems connected to these.
- Non-physical: the cyberspace is a real area where the users interact and develop diverse activities through the information and data transference.

This digital ecosystem makes a new place where every kind of goods and rights could be under risk or they could also be damaged, impaired or deteriorated. Therefore, the security of both parts (physical and non-physical) is vital to avoid the effects of cyber events which certainly jeopardize the integrity of entire cyberspace. In that case, limits of the collective and individual interests shall be delimitated to attribute the cyber security duties for each subject.

3.1. The cyberspace

Digital ecosystems, like any other ecosystem, have their own habitat where there are some particular conditions which are suitable for life. Life may be understood as the activity developed by a person or a community of an organism[1]. In fact, cyberspace is an environment built or arose by digital communications taking place through the IT systems[2].

This concept became popular after BARLOW speech "A Declaration of the Independence of Cyberspace" (February 8th, 1996 in Davos, Switzerland)[3]. In this declaration, he also claimed to the

[1] Vida, Diccionario de la lengua española, Edición del Tricentenario, RAE, http://dle.rae.es/?id=blw7uSa

[2] Cyberspace, Oxford living Diccionaries, Oxford University, http://www.oxforddictionaries.com/us/definition/american_english/cyberspace

[3] Jhon Perry BARLOW (1996), A Declaration of the Independence of Cyberspace, Electronic Frontier Fundatio EFF, https://www.eff.org/es/cyberspace-independence

freedom of cyberspace so he considers it as an environment where the citizens live in absolute freedom without the control of governments and public institutions. The Oxford dictionary defines the term cyberspace as *"the notional environment in which communication over computer networks occurs"*. Nonetheless, the main element of this concept has to be linked with the social relations –which take in place in this ecosystem- than with the IT systems –which make the material part of it-[1]. Even so, there is not a global definition of this concept[2] , the approach should follow the terms proposed by International Telecommunication Union (ITU)[3] and ISO/IEC 27032:2012. Thus, the cyberspace is the environmental complex caused by the interaction between people, software and Internet services and crated by the network and IT device –the material part- which connect all of them[4].

Looking back to the above-mentioned concept of IT systems, cyberspace comprises the networks and connections aimed to transfer and share information. In this order, cyberspace is an essential element for the personal, the organizational and the administrative sphere with a large scope in the global socioeconomic affairs. That is the framework where public and private activities (which may have some digital component) are carried out. In fact, this new environment has provided an opportunity to governments, companies and civil society to share and participate in mutual information, with an unlimited capacity for development. In this way, cyberspace could be understood as a "new virtual world" formed by individual connections where the governments and public institutions operate as an individual subject and their control over the global system is really limited. All these interactive actors of this specific environment are exposed to its inherent risks that are cyber risks or IT risks (vid 1 "The cyber risk: concept and scope").

Summing up, the cyberspace is a "dual reality" made by physical and un-physical reality where it is difficult to distinguish between some elements and limits as the open and the closed reality, or individual and common interest[5]. These two spheres, on one hand, arise a digital ecosystem, and on the other hand, may be affected by cyber threats as well as different goods and rights, either material or immaterial.

3.2. Connectivity, Hyper-connectivity and Cyberspace

The IT development may reduce the traditional accidental events and cyber events (i.e. hood) using the modern systems of management and risk prevention. Nonetheless, technology development

---

[1] Chip MORNINGSTAR and F. Randall FARMER (2003), *The Lessons of Lucasfilm's Habitat. The New Media Reader*. Ed. Wardrip-Fruin and Nick Montfort: The MIT Press.

[2] CYBERPOWER AND NATIONAL SECURITY (2009), "Policy Recomendations for a Strategic Framework" in Cyberpower and National Security, FD KRAMER, S. STARR, L.K. WENTZ (ed.), National Defense University Press, Washington (DC).

[3] Frederick WAMALA (2011), *The ITU National Cybersecurity Strategy Guide*, CISSP.

[4] ISO/IEC 27032:2012 Information Technology Security Techniques, Guidelines for Cybersecurity, ISO, http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=44375

[5] Sebastián Koch MERINO, (2015), "Libertad en el ciberespacio", Revista de Ensayos Militares vol. 1 nº2, p. 92.

aspects not only prevent but also cause important risks for global socioeconomic stability[1]:

e. **The connectivity is the modern society distinctive element** (CASTELLS, 1996)[2]. The development of IT systems in some areas, such as the transport, commerce and the information systems, has produced the dependence based on the deferments subjects in the cyberspace. This dependence implies two perspectives. The positive one is appropriate for calculating risks in the light of the collecting and processing data. The negative approach allows extending risks through the entire cyber environment.

f. **The speed of technological development and the IT systems dependence**. The speed of technology market development and the success acceptation of the new IT products -which rapidly replaced the previous ones-, could make us to forget all the future implications. Especially when the scenarios or possible situations are unlimited and the effects are often unpredictable. An example of this lack of foresight was the widespread fear of the millennium bug effects. Surely, this situation was unpredictable concerning the date showed in computers.

For this reason, possible system failures (e.g. the cyber-attacks and the cybercrimes) require Critical Infrastructure security. In particular, certain industries may affect public and common interests (i.e. Energy, telecommunication or transport), whose breaches may produce catastrophic damages. The IT omnipresence and the increasing importance of technology are likely to cause any breach or failure with possible damages to global socioeconomic areas. Historically, many sources may cause devastating global consequences for the economy and political status-. However, currently, some qualified individuals are able to cause, such devastating consequences, remotely and anonymously through the IT systems. This possibility implies **the transfer of power to the technological world** and the paradigm of healthy cyberspace. In addition to this perspective, systemic cyber risks may be considered as part of global policies and governmental strategies.

Indeed, the development of IT and the connectivity has created a **global system** with firm socioeconomic capabilities, which has **streamlined the globalization process**. At the same time, that process has leaded to an increasing interdependence as main characteristic of the 21st century damage events. IT development has granted to risks with the **potentiality** to cause significant **damage to systems and infrastructures** on which our society as well as the global economy depends under the name of ***"mega-risks"***. This situation may produce serious **difficulties for traditional risk management and the insurance industry[3].**

[1] Emerging Risks in the 21st Century AN AGENDA FOR ACTION, OECD (2003), p. 12. https://www.oecd.org/futures/globalprospects/37944611.pdf

[2] M. CASTELLS (1996), The Rise of the Network Society. Oxford: Blackwell.

[3] Emerging Risks in the 21st Century, the Secretary-General Emerging Risks, OECD, https://www.oecd.org/futures/globalprospects/37944611.pdf

4. The extraordinary risks and catastrophic threats

The cyber risks are not only isolated problems related to the IT systems, but also they are part of broader context compromised with a really large range of currently socioeconomic matters. Indeed, the referenced hyper-connectivity produces the exponential increase of subjects, processes and goods connected through the cyberspace[1]. Precisely, the "Risk and Responsibility in a Hyper-connected World" report published in 2014 by The World Economic Forum had established three possible scenarios based on the study of the future hyper-connectivity effects[2]. In the best scenario **based on** *Mudding into the Future***,** the hyper-connectivity is able to create 3,72 trillions of USD in 2020, and in the worst one -*Backlash Decelerates Digitization*- the cyber threats would reduce the potential economic growth in 1,3 trillions of USD[3]. The Global Risk Report 2012 (published by The World Economic Forum), regarding the subject "*The Dark Side of Connectivity*", advices to the increasing IT dependence on our daily life. So on, **the report links up the risk of the physical world with the cyber threats. These links allow the cyber events to produce relevant damages**[4].

On one other hand, critical infrastructure failures are the main example of potential cyber threat. Critical infrastructure failures may be caused by some a widely group of potential triggered technological threats, in relation with the physical and non-physical elements of cyberspace. These types of threats can be considered as a ***"Centre of Gravity"*** **because they are the most influential cyber risk** maintaining a direct links with the economics, environmental and geopolitical threats[5]. On the other hand, **the removal of limits and barriers of hyper-connectivity and its causes may extent damages through the entire system**. For these reasons, the security of each individual systems of the digital ecosystem contributes to create a "*healthy*" digital space favoured for all subjects. At that case, experts accept the fact that there are not completely secure systems but systems whose vulnerabilities have not yet been discovered[6].

In the natural environment, there are numerous and unpredictable systemic and extraordinary risks which would be exposed the social stability, now that concept can also be applied to the cyber risk as it have been apply to the traditional financial and economic risks. This consideration comes from the potential systemic impact of cyber events on national security and economy[7]. In the same

---

[1] Risk and Responsibility in a Hyperconnected World, World Economic Forum (February 2014), p. 5, http://www3.weforum.org/docs/WEF_IT_PathwaysToGlobalCyberResilience_Report_2012.pdf

[2] Risk and Responsibility in a Hyperconnected World, World Economic Forum (February 2014), p. 26, http://www3.weforum.org/docs/WEF_IT_PathwaysToGlobalCyberResilience_Report_2012.pdf

[3] Risk and Responsibility in a Hyperconnected World, World Economic Forum (February 2014), p. 30, http://www3.weforum.org/docs/WEF_IT_PathwaysToGlobalCyberResilience_Report_2012.pdf

[4] Global Risks 2012, World Economic Forum (2012), pp. 24-25.

[5] Global Risks 2012, World Economic Forum (2012), p. 44.

[6] Global Risks 2012, World Economic Forum (2012), p. 27.

[7] Cyber Risk– a Global Systemic Threat, a White Paper to the Industry on Systemic Risk , DTCC (October 2014), Prologue, https://www.google.es/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad =rja&uact=8& ve d=0ahUKEwjG7Ibqw-bPAhXCQBQKHUveB5UQFggcMAA&url=h ttp%3A%2F%2Fwww.dtcc.com%2F~%

way, the reports published by the Depositary Trust & Clearing Corporation (hereafter, DTCC) (Systemic Risk White Paper 2013) consider that the critical nature and effect of the interconnection caused by cyber risks make them the biggest systemic threat which affects the financial markets, the industry, and governmental and military stability[1].

This perspective was confirmed by the DTCC's Systemic Risk Barometer survey (October 2014) where the 84% of the experts considered that the cyber threat as one of the top 5 systemic damage[2], and respectively, the International Organization of Securities Commissions 2013 survey pointed out that the 89% of the experts considered the cybercrime as the main systemic.

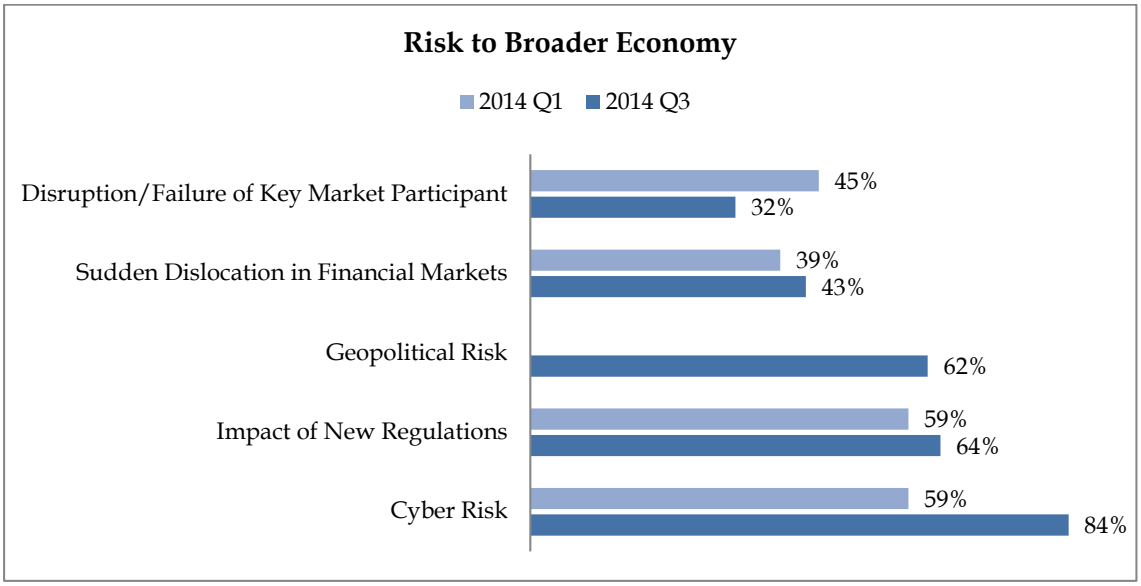


Figure 2: Risk to Broader Economy Top 5 Risk Identified, Risk to Broader Economy[3].,

The hyper-connectivity not only allows the damage would be spread out through the system and produce indirect damage; but also allows hackers to use a large number of systems to cause huge damages. Indeed, the new generation of cyber-attacks are also systemic tools, which are identified by the use of malware designed to infect systems massively through multiple media (web, mail, applications ...)[4]. These systemic attacks allow to obtain a large amount of data and information from the entire ecosystem, and they also permit to establish a network of infected systems (Boths) which could be used to provide other attacks triggering the damages. **In that case, cyber**

2Fmedia%2FFiles%2FDownloads%2Fissues%2Frisk%2Fcyber-risk.pdf&usg=A FQjCNHaLHeWuZLVBLjiw_2JwBAUCh4xPA&sig2=QE0u1kerPcAwi_6NYsv-_w&bvm=bv.136499718,d.d24

[1] A White Paper to the Industry on Systemic Risk, DTCC (October 2014), p. 1.

[2] Systemic Risk Barometer, DTCC (2014), http://www.dtcc.com/~/m edia/Files/Downloads/issues/ risk/Systemic_Risk_Summary_Report.ashx

[3] Top 5 Risk Identified, Risk to Broader Economy, Systemic Risk Barometer, DTCC (2014), p. 3 http://www.dtcc.com/~/media/Files/Downloads/issues/risk/Systemic_Risk_Summary_Report.ashx

[4] Advanced Targeted Attacks: How to Protect Against the New Generation of Cyber Attacks, FireEye, (2015), p. 4, http://www2.fireeye.com/rs/fireye/images/fireeye-advanced-targeted-attacks.pdf

extraordinary events represent the most catastrophic situation caused by the potential damages of hyper-connectivity. As a result of these threats, the fear of uncertainty damages and of potential effects of cyber threats are based on the above mentioned facts and on the particular circumstance that the main critical infrastructures (e.g. energy, water, transportation) are controlled by systems connected to the Internet (e.g. the global financial system)[1].

4.1. The Traditional Catastrophic Risks: a path to "cybergaeddon"

Some cyber events may be considered as potential key elements to arise a ***"Global Catastrophic Risk"***. In that case, the Global Catastrophic Foundation sets out cyber events as the *"events or processes that would lead to the deaths of approximately a tenth of the world's population, or have a comparable impact"*. Any case, the Global Catastrophic Risks include as a possible catastrophic risk the digital violence, so this report remind that this violence could come from either political violence or cyber-attacks. Under these considerations, the report classifies the technological risks as unknown risks, so the "speed" and "suddenness" of technological breakthroughs may also be a risk factor out of the governments control mechanisms[2].

The Global Catastrophic Risks could also be catalogue as catastrophic risks with local implications, when cyber events produce the same impact on a specific environment or affect the regional socioeconomic stability. It is the extraordinary risks case, which are not able to produce a global catastrophe but they have a large range of unlike consequences for human beings. **Those extraordinary risks are unpredictable, unknown and very unusual as the traditional extraordinary risks are**.

As there was mentioned above, the digital violence may cause catastrophic damages through cyber-attacks, classifying catastrophic damages under an extraordinary risk category in the cases they are regarding to, or come from the terrorist attacks or acts of war. Those are usually excluded by the insurance policies and they are mostly covered by the compensation organizations (e.g. public funds or pools of insurances). Nevertheless, it is convenient to emphasize the concrete **differences between the traditional catastrophic damage produced or derivated to some cyber events** (classify as cyber war, cyber terrorist, hacktivist…) **and the cyber extraordinary events which are a new different kind of catastrophe regarding to the hyper connectivity, the IoT and the called cybergaeddon** –as the most extreme case-.

The Spanish case is a particular example, and it is probably useful to explain **how the catastrophic risks –regarding to the IT systems- can be coverage by compensation fund**. That coverage was ruled by December 16th, 1954 ACT whose Article 1 assigned it to the Insurance Compensation

[1] Derek O'Halloran, (2013), Tech utopia or cybergeddon?, https://www.weforum.org/agenda/2013/01/tech-utopia-or-cybergeddon/

[2] Owen Cotton-Barratt, Sebastian Farquhar, John Halstead, Stefan Schubert, Andrew Snyder-Beattie, (2016), Global Catastrophic Risks, Global Catastrophic Foundation, http://globalprioritiesproject.org/wp-content/uploads/2016/04/Global-Catastrophic-Risk-Annual-Report-2016-FINAL.pdf

Board [1](*"Consorcio de Compensación de Seguros"- afterwards CCS)*, and during all these years the regulation related to the catastrophic and extraordinary risks have been developed close to this organization.

This Institution is supported by public funds and its main object consists of compensating the losses arising from extraordinary events in Spain and those which were occurring abroad while the policyholder has his habitual residence in Spain (article 6 of the CCS Act -"*Estatuto Legal del Consorcio de Compensación de Seguros*"-).

The Article 1.b of the Extraordinary Risk Insurance Regulation - "*Reglamento del seguro de riesgos extraordinarios*", approved by the "*Real Decreto 300/2004, de 20 de febrero*" (afterwards ERIR)- recognizes to the purposes of the *CCS* coverage such as Extraordinary Risks "*those violently caused, as consequence of terrorism, rebellion, sedition, mutiny and popular tumult*". And at that case the mentioned article defines as losses the "*direct damages caused for those to the people and the goods, as well as the loss of benefits that was consequence of those*".

Consequently, the Article 2 defines each of the mentioned actions by the creation of the next list:

a. Terrorism: *any violent action carried out with the purpose of destabilizing the political system, or causing fear and insecurity in the social environment.*

b. Sedition: *actions referred to in articles 544 to 549, both inclusive, of the Penal Code.*

c. Mutiny: *any movement accompanied by violence directed against the authority with the purpose of obtaining a satisfaction of certain political, economic or social claims* (which have to be provided by an act that neither was being terrorist, nor it was not being considered a riot).

d. Popular riot: *any action in a group and with the purpose of attempting against public peace that causes an alteration of order, causing injuries to persons or damage to property* (which have to be provided by an act that neither was being terrorist, nor it was not being considered a mutiny).

The cyber terrorism and hacktivism acts could be considered under some of the above definitions, because **the referred rule does not limit its effects to a particular place or environment**. Therefore, **cyber terrorism and hacktivism have the characteristics mentioned by those definitions without any doubt**; and the losses produced as a consequence of them **will be coverage** by the CCS, whether the good or the right affected by the damage it had been insured under once of the policies ruled by the Article 4 of the ERIR –first party coverage policies of vehicles, fire and natural catastrophes, thefts, and electronic and computer assets and third party vehicles policies-.

Particularly, the first party policies of vehicles, electronic and computer assets, and the third party vehicles policies may be affected by the cyber risks. Moreover, in those cases, **the cyber events**

[1] Translated by the author in light of achieving legibility.

could affect either the material components of the IT systems, and the software and data stored into them.

Beside the traditional first party policies which used to cover the material and physical damages of the IT systems (hardware), currently it has been increased the number of policies included in their wordings concepts such as the data thefts and losses. At any case, the IT systems are formed by some elements - physical elements (hardware), software and storage data which are necessary linked- , which are an essential part of the IT nature. **Therefore, all of these elements may be covered by first party electronic and IT devices policies if they were not expressly excluded or limited.**

For those reasons, the first party cyber policies would have the elements required by the ERIR, so the **traditional extraordinary risks – Terrorism, Mutiny and Riot- associated to the cyber events could be covered by the** CCS.

a. Loss of profits

The loss profit cases are comprehended as a part of the CCS coverage stipulated by the Article 3 of ERIR:

> "*It is understood that there is a loss of profits whether the result of any of the extraordinary events provided for in this regulation, there is an alteration of the normal results of the economic activity of the insured subject, resulting from the suspension, suspension or reduction of the productive or business processes of the said activity* ".

Therefore, it is important to highlight the work stoppage (as a consequence of Distributed Denial of Service Attack (hereafter, DDoS)? attacks or any standstill of the IT Systems) is one of the main losses caused by the cyber events. Thus, as the hyper-connectivity consequences grow up continuously those damages could be huge in the immediate future.

b. CCS mandatory coverage

As it was said, some of the new cyber policies have the characteristics required by the mentioned Article 4 –section 1.a- in whose consideration it is recognized which policies have to be affected by the *CCS mandatory recharge"*. Therefore, according with the DGSFP[1] Resolution of May 28th, 2004 the cyber policies should set out the mandatory recharge stipulated by the *CCS Act*, thereby:

- The Article 7 established that *"it is mandatory the surcharge in favour to the CCS" for the fulfilment of its functions in the matter of compensation for losses arising from extraordinary events".*

[1] Directorate-General for Insurance and Pension Funds (Spanish: Dirección General de Seguros y Fondos de Pensiones) The Spanish regulatory department that supervises and controls insurance and pension fund sector.

– The Article 8.3 established that *"all the policies included in the prior article have to set out the CCS provision"*

Otherwise, the first party cyber policies and **the coverage of the cybernetic assets** complete the first party policies of *"electronic assets and computers"*, so there are not substantial changes in the covered objects. Indeed, those are one of the **currently IT development effects in the insurance industry**, and they have just **extended to the definitions** setting out policies in order to adapt policies **to the new technological assets**.

4.2. The cyber terrorism: an example of the traditional catastrophic risks

The cyber terrorism is briefly considered as the use of the IT systems to attack critical infrastructures or any systems belongs to the governments and public institutions. Furthermore, these actions could try to produce the coercion and intimidation in the civil society and the government[1]. The **1937 Convention for the Prevention and Punish of Terrorism** introduce into the definition of terrorist acts *"the criminal acts against the Estate"* or those whose main objective was to produce terror into the individual citizen, group of people or the entire civil society[2]. As consequence, **the main element to classify an act (committed by or through the IT systems) as cyber-terrorism shall be their consequences**. Indeed, it is required a violent act against people or a relevant threat which actually can produce the extraordinary real fear to be damaged. One of the examples of cyber terrorism are attacks, either effective or threat, targeted to critical infrastructure due to the fact to the impact and the potential consequences of such attacks[3]..

On the other hand, even so the cyber terrorism is a common concept; there is not an accepted general methodology to determine it, so currently it is still difficult to difference between cyber terrorism and the common cyber-attacks. The term was firstly created by Barry Collin in the 1980s (COLLIN, 1997)[4] and its use became common in the 1990s as it is said for some studies such as *"Protect yourself from the cyberterrorist"*; *"Insure yourself against cyberterrorism"*; *"Funding forthcoming to fight cyberterrorism"* (HAMBLEN, 1999[5]; LUENING, 2000[6]).

---

[1] James LEWIS (2002), United States. Center for Strategic and International Studies. Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats. Washington, D.C.

[2] Convention pour la prévention et de la répression du terrorisme/ Convention for the Prevention and Punishment of Terrorism (16 de noviembre de 1937), https://www.wdl.org/es/item/11579/view/1/1/

[3] D. DENNING, "Cyberterrorism", Testimony before the Special Oversight Panel of Terrorism Committee on Armed Services, US House of Representatives, (23 de mayo de 2000), http://www.cs.georgetown.edu/~denning/infosec/cyberter ror.html

[4] B. COLLIN (1997), *The Future of Cyberterrorism, Crime and Justice International*, pp. 15-18.

[5] M. HAMBLEN, Clinton commit $1.46B to fight cyberterrorism http://www.cnn.com/TECH/computing/9901/26/clinton.idg , (26 de enero de 1999).

[6] E. LUENING, Clinton launches plan to protect IT infrastructure. CNET, (7 de enero de 2000).

Otherwise, **the particular element of the cyber terrorism is the motivation. In fact,** hackers are not motivated by the same goals as the cyber terrorists are (Gabriel WEIMANN, 2004[1]). Indeed, **the unique distinctive element of cyber terrorism is to commit acts of terrorism with such motivation using IT systems**. Therefore, **cyber terrorism may be considered as a new technological tool use for the traditional terrorists,** and for these reasons, the direct or consequent damages caused by cyber terrorists **shall be covered by the terrorist insurance pools or funds**.

Notwithstanding these aspects, cyber terrorism shall be analysed jointly with terrorism regulation and measures as an international issue. Due to this fact, it is necessary to examine the EU and the international perspective as well as the US and the UK regulation for offering a Comparative Law approach.

a. Moving on to the **European Union** approach, the EU has taken significant actions against terrorist attacks, through diverse measures, among them some rules have been approved with the intention to mitigate the adverse effects of terrorism acts (e.g. the Asylum, Migration and Integration Fund[2] and the Internal Security Fund[3]). It is necessary to highlight some EU actions in the framework of terrorism attacks:

a) the European Union Solidarity Fund was created in 2002 focusing on the practical effects of the solidarity clause introduced by Article 222 of the Treaty on the Functioning of the European Union[4]. Particularly, this solidarity clause has established a range of common actions against terrorist attacks and catastrophic events (produced by natural or human acts). The 24th June, 2014 Council Decision at its Article 2 determined that referred clause was applicable to terrorist attacks understanding such as an event caused by a terrorist act define for the 13th June, 2002 Council Decision. Indeed, the Article 1 of the referred Council Decision has set out a list of actions which may be understood as terrorist acts, and all of them could be committed through the IT systems and the cyber space, especially:

- The Article 1.1d: causing extensive destruction to a Government or public facility, a transport system, an infrastructure facility, including an information system, a fixed platform located on the Continental Shelf, a public place or private property likely to endanger human lifes or, to result in major economic loss;

[1] Gabriel WEIMANN (2004), *Cyberterrorism How Real Is the Threat?*, Special Report 119, United States Institute of Peace, https://www.usip.org/sites/default/files/sr119.pdf

[2] Regulation (EU) No 513/2014 of the European Parliament and of the Council of 16 April 2014 establishing, as part of the Internal Security Fund, the instrument for financial support for police cooperation, preventing and combating crime, and crisis management and repealing Council Decision 2007/125/JHA

[3] Regulation (EU) No 514/2014 of the European Parliament and of the Council laying down general provisions on the Asylum, Migration and Integration Fund and on the instrument for financial support for police cooperation, preventing and combating crime, and crisis management.

[4] Cláusula de solidaridad, EUR-LEX, http://eur lex.europa.eu/summary/glossary/solidarity_clause.html?locale=es

– The Article 3.c: drawing up false administrative documents with the view of committing one of the acts listed in Article 1(1)(a) to (h) and Article 2(2)(b).

The referred solidarity clause has been applied for mitigating the consequences of 2004 Madrid attacks[1]. In the same sense, the Proposal amending Council Regulation (EC) No 2012/2002, establishing the European Union Solidarity Fund COM(2005) 108 final 2005/0033 (COD) disposed in the Context of the Proposal (existing provisions in the area of the proposal): *"As at present, total direct damage in excess of an absolute or a regarding threshold, whichever is lower, is applied to the physical damage caused by disasters including the intervention costs to which these give rise. In practice, this will cover not only natural disasters but also public health emergencies, industrial accidents and physical damage resulting from acts of terrorism"*.[2] Moreover, this proposal added to the cited Regulation (Article 1) the mention to terrorist acts, so at this case Article 4 will recognise the terrorism victims assistance[3].

– The Regulation (EU) No 661/2014 of the European Parliament and of the Council of May 15th, 2014 has amended the Council Regulation (EC) No 2012/2002 which it was written to establishing the European Union Solidarity Fund. Further some amending aspects it has limited their effects to the "*natural catastrophes*". For this reason, the extraordinary risks and catastrophes created by the terrorist acts are already not including into the EU Solidarity Fund.

– The Regulation (EU) No 513/2014 has recognised as a priority term "*to raise levels of security for citizens and businesses in cyberspace*" and "*to increase Europe's resilience in the face of crises and disasters*". Thus, as a response to the effects of terrorist attacks and other disasters the article 10 maintain that "*The Instrument shall provide financial assistance to address urgent and specific needs in the event of an emergency situation*" in accordance with Articles 6 and 7 of the Regulation (EU) No 514/2014. This article 7 sets out the assistance and financing for emergency cases, even it has recognised that emergency assistance could be provided in the form of grants "*directly granted*" by the Union agencies.

From a global perspective, the Financial Stability Report (European Insurance and Occupational Pensions Authority -hereafter EIOPA- June de 2017)[4] has warned to the insurance industry the urgency to adapt themselves to the emerging risks stemming from terrorism and cyberspace. According to the terrorism acts, this report maintains that the recent attacks are more unpredictable

[1] Op. cit, , EUR-LEX, http://eur-lex.europa.eu/summary/glossary/solidarity_clause.html?locale=es

[2] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL establishing the European Union Solidarity Fund, Brussels, 6.4.2005 COM(2005) 108 final 2005/0033 (COD), http://ec.europa.eu/regional_policy/archive/funds/solidar/doc/com(2005)108%20final_en.pdf

[3] Patricia PAZOS DURÁN (2016), *Política de lucha contra el terrorismo de la UE: una prioridad en la agenda internacional*, Universidad Complutense de Madrid, Madrid, http://eprints.ucm.es/35585/1/T36825.pdf

[4] Financial Stability Report, EIOPA, (June 2017), p. 4, https://eiopa.europa.eu/Publications/Reports/Financial_Stability_Report_June_2017.pdf

and even so, more difficult to determine their basics characteristics such as who provoked the attack and why it was provoked. Furthermore, these new circumstances would make difficult the insurance coverage decision or the pool coverage determination[1]. In those cases, **the lack of data about the offender and his motivation could force to cover of genuine terrorist acts by the insurance industry –although, it was not officially recognized-**. Therefore, this risk may be especially highlighted within cyber terrorism cases which are harder to identify than official terrorism actions. In the same sense, the article *"Careful how you code: Cyberterrorism coverage under TRIA and stand-alone cyber policies"* (WILLIS, 2017)[2] warns about the importance of the underwriting appropriate insurance policies, because of the **unlikely possibility to cover damages caused by non-official acts of terrorism**.

b. **The US regulation and its global impact on global insurance policies.**

In the US, the Terrorism Risk Insurance Act - November 26th, 2002 – (afterwards TRIA) was approved, This rule established an insurance compensation system formed by public and private funds with the particular aim of coverage of losses of terrorist damages in the US[3]. Recently, the mentioned rule has been amended by the Terrorism Risk Insurance Program Reauthorization Act of 2015 - January 7th, 2015- (afterwards TRIPRA) for extending its force to 2020.

On one hand, the TRIA aims are to cover and absorb losses caused by terrorist attacks which affect property covered under the damage or liability insurance policies. In June of 2016, the National Association of Insurance Commissioners (hereafter NAIC) introduced the *"Cyber Liability"* policies into the *"Other Liability"* category. Afterwards at at 27th December of 2016, the US Department of the Treasury recognized that cyber-policies under the form of *"Cyber Liability NAIC"* and code 17.0028 shall be included within the *"property and casualty insurance"* category and covered under TRIA[4]. On the other hand, the TRIA defines the "act of terrorism" as the result of these elements:

- A violent act or an act that is dangerous to: human life; property; or infrastructure;
- These have resulted in damage within the United States.
- These have been committed by an individual or individuals acting on behalf of any foreign person or foreign interest, as part of an effort to coerce the civilian population of the United

[1] Financial Stability Report, EIOPA, (June 2017), p. 19, https://eiopa.europa.eu/Publications/Reports/Financial_Stability_Report_June_2017.pdf

[2] Careful how you code: Cyberterrorism coverage under TRIA and stand-alone cyber policies, Willis Towers Watson, (July 26th 2017), https://www.willistowerswatson.com/en-GB/insights/2017/07/decode-cyber-brief-careful-how-you-code

[3] "Terrorism Risk Insurance Program". U.S. Treasury Department Website. U.S. Treasury Department. (March 20th 2013).

[4] Careful how you code: Cyberterrorism coverage under TRIA and stand-alone cyber policies, Willis Towers Watson, (July 26th 2017), Willis Towers Watson, (26 de July de 2017), https://www.willistowerswatson.com/en-GB/insights/2017/07/decode-cyber-brief-careful-how-you-code

States or to influence the policy or affect the conduct of the United States Government by coercion.

– Any case, these have to be certified by the Secretary, in concurrence with the Secretary of State, and the Attorney General of the United States

Indeed, the 2016 Terrorism Risk Insurance Report (MARSH, 2016)[1] has already anticipated the possibility that certain cyber-attacks were covered by the TRIPRA. In the case, the characteristics aforementioned taking place (specially the official recognition of a terrorist act). Father to this consideration, on July 15th, 2016, the US Federal Court sentenced a Kosovo hacker for committing a terrorist offense by accessing and publishing the personal data of 1,000 employees of the US federal government.

This judgment constitutes a precedent and it may facilitate to recognize the cyber-attacks as official acts of cyber terrorism in future cases[2]. Consequently, it would lead to declare the losses coverage by the compensation funds which attend the risk derived to the terrorism acts -such as TRIA- (KRAUSS)[3]. However, this official recognition is still an isolated case, although the media have linked much of the major cyber-attacks with terrorist groups. For this reason, the insurance industry may cover losses caused by terrorist groups which have not been officially declared (or sentenced by a court) as a *"terrorist act"*. In those cases, the policy exclusions should be underwriting clearly because the cyber terrorism could be broadly understood. Further, there are certain cases which might be excluded by defining themselves as an *"act of war"* so the US[4] judicial precedents and the main insurance global policies do not require an official declaration of warfare to exclude its damages.

Concerning the impact on global insurances policies of the US actions mentioned, during the last years some governments have been creating pools and funds able to cover the consequences of terrorism, which assume this risk and allow the insurance industry to extend the property policies to this coverage, as the next cases:

	TERRORISM POOL OR REINSURANCE MECHANISM
Australia	Australian Reinsurance Pool Corporation (ARPC)

[1] 2016 Terrorism Risk Insurance Report, Marsh, (July 2016) P, 7. https://www.marsh.com/content/dam/marsh/Documents/PDF/USen/2016%20Terrorism%20Risk%20Insurance%20Report.pdf

[2] 2016 Terrorism Risk Insurance Report, Marsh, (July 2016) P, 7. https://www.marsh.com/content/dam/marsh/Documents/PDF/USen/2016%20Terrorism%20Risk%20Insurance%20Report.pdf

[3] Jason KRAUSS, Carefull How you Code…, Willis Towers Watson, https://www.willistowerswatson.com/api/sitecore/Article/Download?itemId=07ca0cd8-23b3-479d-96e1-3f17c23da863&lang=en-GB

[4] Pan American World Airways, Inc. V. Aetna Casualty & Surety Co. en Jason Krauss, op. cit., Willis Towers Watson, https://www.willistowerswatson.com/api/sitecore/Article/Download?itemId=07ca0cd8-23b3-479d-96e1-3f17c23da863&lang=en-GB

Austria	Österreichischer Versicherungspool zur Deckung von Terrorrisiken
Bahrain	Arab War Risks Insurance Syndicate (AWRIS)
Belgium	Terrorism Reinsurance & Insurance Pool (TRIP)
Denmark	Danish Terrorism Insurance Scheme
Finland	Finnish Terrorism Pool
France	Gestion de l'Assurance et de la Réassurance des risques Attentats et actes de Terrorisme (GAREAT)
Germany	Extremus Versicherungs-AG
Hong Kong-China	The Motor Insurance Bureau (MIB)
India	Indian Market Terrorism Risk Insurance Pool (IMTRIP)
Indonesia	Indonesian Terrorism Insurance Pool (MARIEN)
Israel	The Victims of Hostile Actions (Pensions) Law and The Property Tax and Compensation Fund Law
Namibia	Namibia Special Risk Insurance Association (NASRIA)
Nederland	Nederlandse Herverzekeringsmaatschappij voor Terrorismeschaden (NHT)
North Ireland	Criminal Damage Compensation Scheme Northern Ireland
Russia	Russian Anti-Terrorism Insurance Pool (RATIP)
South Africa	South African Special Risk Insurance Association (SASRIA)
Spain	Consorcio de Compensación de Seguros (CCS)
Sri Lanka	Strike, Riot Civil Commotion and Terrorism Fund – Government
Switzerland	Terrorism Reinsurance Facility
Taiwan	Taiwan Terrorism Insurance Pool
UK	Pool Reinsurance Company Limited (POOL RE)
US	Terrorism Risk Insurance Program Reauthorization Act of 2015 (TRIPRA)

Figure 3: 2016 Terrorism Risk Insurance Report, Marsh, (July 2016)[1]

c. **In the UK**, losses caused as a result of terrorist attacks have been covered by Pool RE since its foundation in1993 by the insurance industry and the UK Government, which has been maintained jointly with HM Treasury funds. Following the example of TRIA, the Pool RE covers damages caused as long as the HM Treasury certified the act as terrorism[2].

Currently, the damages caused by cyber-events expressly excludes the Pool RE coverage. However, in 2016[3] the institution announced the creation of a commission at the Judge Business School (University of Cambridge) focused on the cyber terrorism coverage, so the institution is currently studying the appropriate means and measures to include cyber events coverage and losses. Indeed, Pool RE has included cyber terrorism risk coverage into its objectives and initiatives of modernization. In order to achieve this goal, the collaboration of public and private institutions

[1] Terrorism pool or Reinsurance Mechanism, 2016 Terrorism Risk Insurance Report, Marsh, (July 2016) P, 8. https://www.marsh.com/content/dam/marsh/Documents/PDF/USen/2016%20Terrorism%20Risk%20Insurance%20Report.pdf

[2] POOL RE TERRORISM ENDORSEMENT, http://www.lmalloyds.com/CMDownlo ad.aspx?ContentKey=e1df14f4-f0 66-41b7-a635-23298fc580d4&ContentItemKey=d3219f2e-9772-4e92-a9c1-c28dbfea3fb0

[3] Julian Enoizi, Message from the Chief Executive, Pool RE, (2016), https://www.poolre.co.uk/newsletters/PoolRe-Newsletter-0416-for-web.pdf

and the application of prevention tools (Cyber Essentials, ISO 27001) have been considering necessary[1].

The Pool RE wording has excluded "*any loss directly or indirectly arising out of, contributed to by, or resulting from: Cyber Terrorism*", in that case this institution defines as a cyber-terrorism[2]:

- "*the alteration, modification, distortion, corruption of or damage to any computer or other equipment or component or system or item which processes, stores transmits or receives data or any part thereof whether tangible or intangible (including but without limitation any information or programs or software); or*
- *any alteration, modification, distortion, erasure, corruption of data processed by any such computer or other equipment or component or system or item,*

whether the property of the Insured or not, where such loss is directly or indirectly caused by or contributed to or arising from or occasioned by or resulting from Virus or Similar Mechanism or Hacking or Phishing or Denial of Service Attack."

This broad definition of cyber terrorism has been completed with a closed list of specific terms which are particularly considering as a cyber-attack (Virus or Similar Mechanism or Denial of Service Attack). Actually, those cases complete the major range of events able to produce a cyber-event, but **they suppose a closed list of cases so they could be exceeded by the development of new techniques of cyber-attack**. Particularly, there is no reference to social engineering techniques which combine cybernetic elements with other techniques or tools (aside to cyberspace) and they caused effects similar to the cyber-attacks expressly excluded.

Analysing the UK judicial decisions concerning cyber terrorism, it is necessary to highlight that the first case of cyber terrorism recognized by a UK judgment was the terrorist Samata Ullah sentenced in May, 2017. The judgment expressly acknowledges that the accused "*deployed his not inconsiderable self-taught computer skills to further the cause of terrorism and in particular Islamic State*". Particularly, he stored and shared tools and instructions to commit various forms of terrorist attacks using the IT systems[3]. This case of obtaining and publishing data for terrorist purposes was also recognized to declare it as a cyber-terrorism action in the judgment issued by the "Virginia federal court" on June 17th, 2016 in the US[4].

---

[1] The role of Pool Reinsurance Company Ltd, Pool RE, (June 9th, 2017) https://www.treasury.gov/initiatives/fio/acrsm/Documents/ACRSM_Presentation_By_Pool_Re.pdf

[2] Pool RE Terrorism Endorsement, LMA5225 (October 1st, 2015) www.lmalloyds.com%2FCMDownload.aspx%3FContentKey%3De1df14f4-f066-41b7-a635-23298fc580d4%26ContentItemKey%3Dd3219f2e-9772-4e92-a9c1-c28dbfea3fb0&usg=AFQjCNGNBkly-aVlqHSG75uF66kFtg9rjQ

[3] Alistair Smout, (2017), Briton who promoted Islamic State with special cufflinks jailed for eight years, Reuters, http://www.reuters.com/article/us-britain-security-library/briton-who-promoted-islamic-state-with-special-cufflinks-jailed-for-eight-years-idUSKBN17Y17S?il=0

[4] Daniel Wilson, ISIS-Linked Hacker Pleads Guilty In Cyberterror Case, Law360, https://www.law360.com/articles/808220/isis-linked-hacker-pleads-guilty-in-cyberterror-case

Therefore, in that case it has been considering than the TRIPRA could cover the losses, if the data would be used to produce any damage out of the cyberspace (MCCABE, 2016)[1].In this sense, it is important to note the **cybernetic element could take place either during the preparation or the perpetration of a terrorist attack**, even though it could be an essential element to the terrorist attack commission; and in all of these cases, **it could not be the direct cause of the damage**; particularly, we could highlight two examples:

- Considerate the damages as a result of any attack committed by traditional tools (out of cyberspace) when information about the target was obtained by a cyber-attack.
- Damage caused by an explosive device –or any other physical device- controlled by the IT systems.

In the second case, if the attack is perpetrated by a terrorist using a regular van to cause injures in the pedestrian who are walking on the street the losses will be covered by the Pool RE; but, if the terrorist has hacked the GPS and he accessed to the control of the autonomous van the attack it could be classified as cyber terrorism and excluded by the Pool RE. However, there are always going to be doubts in intermediate cases, such the case where the terrorist has used the IT systems to obtain the vehicle control –a train or a plane- but the attack will be commits through the mechanical or manual use of it.

The object which determines whether or not concur the **circumstances** -included in the transcribed **exclusion**- are focus on **how the attack could be perpetrate, but it do not put attention on how the damage could finally manifested**. In this way, the opposite cases could also produce the same doubts because their complexity. Moreover, there is the possibilities that a physical attack on the IT infrastructure could produce a cyber-event and it could also trigger damages to different goods and rights which either could be part of cyberspace or stay aside of it.

Definitely, **the cyber risk exclusion affects to the nature of the insurance object**, and it has been limited through the use of a categorization based on changing cases and definitions, which belong to a continuous development cyberspace environment. Thereby, the main innovation introduces by cyber risks in the extraordinary risks area is the extraordinary complexity of them, so now the damage causes are more unknown than never. **This circumstance makes difficult the clearly delimitation of the insured object, and it could also let the contradictory interpretation of the policy limits and exclusions**.

Summing up, **it is important to underwrite the policies properly and define the cyber exclusion and limits clarify, in order to consider cyber damages coverage by the insurance industry, or for the institution of compensation**. Cyber events represent a complex reality with physical and non-physical implications. In fact, the IT systems may be also an essential tool for committing directly

[1] Matt McCabe, (2016), Cyber Terrorism: Does Your Insurance Cover the Gaps?, Marsh https://www.marsh.com/us/insights/risk-in-context/cyber-terrorism-does-your-insurance-cover-the-gaps.html

or indirectly terrorist attacks with the capacity or ability to extend their damages through the cyber space.

In this order, the framework of traditional scenarios, terrorist acts are commonly violence situations or produce by physical or psychological threats as real as they are able to cause into the affected the fear of being damaged. Nonetheless, the violence as a virtual phenomenon it is a new subject which have not been studying deeply yet.[1] Currently, the cybernetic violence is determine as their physical implication, among those: the identification of the psychological effects with the virtual damage; the behaviour modification as a result of violence in virtual environments; the physical traumas of virtual violence; and the use of virtual violence in military training (STONE, 1993[2]; WHITEBACK, 1993[3]). Secondly, the *"pure cyberterrorisim"* requires a terrorist act produced (in all its elements and characteristics) through the cyber space, so it could be one of the potential causes which would produce an extraordinary cyber event –as these will be considered then-. Anyway, this space has some characteristics which could help to develop the traditional terrorism, among those: the possibility to have meetings completely anonymously and easily; and, the speed to organize and manage a group[4]. In those cases, the IT systems help to the terrorist acts or complete them but they are not properly a cyber-attack[5] or a *"pure cyberterrorism"*.

4.3. The extraordinary cyber threats

Until this very moment, it was being explained how the IT could produce some catastrophic events and how they could be linked to the traditional threats such as the terrorist acts. Whereas, the **IT can takes part into the traditional catastrophic** as the inevitable consequences of the IT dependency growth (which links the socioeconomic affairs and the material world to the cyber space). Thereby, whenever those consequences have not changed the insured object the threat could be under cover.

Nonetheless, at that point there is going to be explained how the IT could introduce a **new kind of cyber extraordinary threats** which will be produced and expand through the cyber space as a natural consequence of this environment. In this case, **the IT dependence** –particularly regarding with IoT and Hyper-connectivity- **could makes that those cyber extraordinary events affects to the socioeconomic affairs and the material world**. Although, they are not regarding with the traditional catastrophic events, the hyper-connectivity and the IoT are the causal link between the

[1] Sarah GORDON y Richard FORD, (2003), Cyberterrorism?, Symantec Security Response, p. 6-7, https://www.symantec.com/avcenter/reference/cyberterrorism.pdf

[2] V. STONE, Social interaction and social development in virtual environments . Teleoperators and Virtual Environments, Vol. 2. (1993) pp. 153-161.

[3] C. WHITEBACK, (1993), op. cit., Teleoperators and Virtual Environments, Vol. 2. pp. 147-152.

[4] Sarah GORDON y Richard FORD, Cyberterrorism?, Symantec Security Response (2003), p. 8, https://www.symantec.com/avcenter/reference/cyberterrorism.pdf

[5] Op. cit World Economic Forum (2011).

IT systems and the material effects in both cases (traditional and cyber catastrophic events).

a. The elements of the IoT and hyper-connectivity

The Internet of Things (IoT) has developed through the hyper-connectivity which allows the connection between the everyday life devices and the IT systems. **So those systems** -with cloud computing technology and big data- **highlights the development of hyper-connectivity effects into the society, and those also remark the main position of the cyberspace in the physical world**. Nonetheless, at the same time, they have created important barriers in terms of cyber security (for example at the individual privacy rights) and the creation of new risks and threats[1].

The IoT allows the control of any device or system through their cyberspace connexion, so that extends and materializes the cyber risks (paralysis, blocking, sabotage, and any other threat) to the physical environment. Indeed, **the IoT generates risks in two different areas: on the one hand, into the personal and sensitive data** (Intellectual and Industrial property are part of it) which are collected and collected by the IoT systems; and on the other hand, in **the physical and material field where the connected devices operate**. In that case, those physical effects have been briefly regulated although the physical integrity of the subjects and goods could represent the most extremely cyber damage.

On the other hand, the protection of privacy and personal data has been widely regulated by the EU and international legislations, although these are usually not created for the new IoT systems. Indeed, the study *"Definition of a Research and Innovation Policy Leveraging Cloud Computing and IoT Combination"* (published by the EU)[2] considers there are certain cases where the regulation on data protection is a barrier and sometimes that slows down the development of IoT and the benefit they bring to society. For these reasons, the referred study sets up the importance to adapt the general regulation to the new circumstances created by IoT.

The IoT can be considered as the beginning of a new stage within the cyberspace and the physical environmental have lost the independence they used to have. This circumstance is due to the development of the connected devices and the hyper-connectivity. Nonetheless, the security of these systems still cannot be considered completely developed, and cyber threats are more damaging on them.

The Communication from the Commission of 31 May 2006: A strategy for a Secure Information Society *"Dialogue, partnership and empowerment"* (COM(2006) 251) has recognise the creation of *"ambient intelligence"* has constituted an important event for the IT systems which *"will become a ubiquitous part of everyday life in the near future"*. Although, this communication prevents *"this development brings with it many opportunities, but it will also create additional security and privacy-related*

[1] Definition of a Research and Innovation Policy Leveraging Cloud Computing and IoT Combination, Digital Agenda for Europe, European Commission DG Communications Networks, Content & Technology, pag. 9, http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=9472

[2] Idem., p. 73.

risks".

All of these elements show a difficult situation between the security –such as data protection- and the socioeconomic interest in the IT development, which are around three main elements:

- There is not software 100% secure, and those threats could increase because of the fast develop and implementation of IoT systems[1].
- There are any cases where the high level of the security standards (for example related to the data protection) could be reduce the IoT potential develop.
- The traditional technologies were focus on the data treatment, storage and transmission, now the IoT operate into the material and physical environment where the new threats will take place.

For all the mentioned reasons, we could **consider that the legal interest related to the IoT and the Critical Infrastructures are closely linked to the material and physical integrity of any person and goods**, and it is also forward to the industrial processes and the economic activities. Thus, the increased regulation focus just on the personal data protection is not running close to the future physical IoT threats.

Therefore, we cloud introduce the double cyber paradox: on one hand, the tech-develop paradox show that the speeds of IT development could make obsoleted the laws at the same time they are writing; on the other hand, the cyber security paradox thus the non-existence of a 100% secure system –in fact there are more insecure each time- contrasted with the cyberspace increased dependence and the socioeconomic interest of its development.

Definitely, as Giulio CORAGGIO[2] said the solution it should not be in the high regulatory standards which try to limit every kind of cyber security vulnerability because that widely regulation usually make difficult the IT development, and some of those standards are not forward to protect the real IoT and IC legal interest –related to the physical integrity-. Indeed, the cyberspace characteristics make to foster the freedom as the more efficient as any other regulated system (as long as the basics rights would be keep on the cyberspace).

For that reason, the best way to maintain the cyberspace status of freedom could be to foster a strong liability system so that let to keep the appropriate standard of cyber security and it would let to distribute the consequences of the damages. Furthermore, the mentioned author Giulio Coraggio considers the creation of an IoT industrial certifications those would guarantee the standards of cyber security[3].

---

[1] Giulio CORAGGIO, Cyber risk insurance – a solution to cybercrime? http://www.gamingtechlaw.com/2015/10/cyber-risk-insurance-cybercrime.html

[2] Giulio CORAGGIO, The Internet of Things cannot be 100% secure?, IoTLAW Law of the Internet of Things, https://iotlaw.net/2015/11/02/the-internet-of-things-cannot-be-100-secure/

[3] Giulio CORAGGIO, what is an adequate standard of security?, IoTLAW Law of the Internet of Things, https://iotlaw.net/2015/11/02/the-internet-of-things-cannot-be-100-secure/

b. The cyber systemic risks: the new catastrophic event

The Hyper-connectivity has developed the cyber ecosystems as an environment where it taken place more activities each day, so this circumstance was been called **the transfer of power to the technological world.** Therefore, the systemic cyber risks are already regarding to the global policies and governmental strategies, and those could produce serious **difficulties for traditional risk management and the insurance industry**[1]**,** especially the ***"mega-risks"*** with the **potential** to cause significant **damage to the systems and infrastructures**[2]**.**

Indeed, there are **some circumstances which define the extraordinary or catastrophic potential of cyber events** (HAMPTON, 2015)[3], those are regarding with their **effects**, **elements**, and especially with how they could **triggered damages**:

- **The effects of cyber events** are constantly increasing, currently every socioeconomic sector are affected by these threats; therefore they have been considerate for the financial analysts (Moody's) *"in a similar vein as other extraordinary event risks, such as a natural disaster"* (HEMPSTEAD, 2015)[4]. Those *"scenarios contain a vivid descriptions of the catastrophic effects"* linked to the national security[5].

- **The unpredictable and unknown scenarios** (produced for the develop of IT security breaches) constituted elements which are commonly showed by the random effects of some natural disasters; those catastrophic scenarios have been linked with cyber events because they are able to produce *"cyber doom scenarios"*[6] so-called *"digital pearl harbour"*, *"cyber 9/11"*, *"eWMDs"*, *"Cyber Kathrarina"* or *"Cyber gaeddon"*; all of these, represents the kind of cyber events that are the least predictable and least modelled of the catastrophe events[7].

---

[1] Emerging Risks in the 21st Century, the Secretary-General Emerging Risks, OECD, https://www.oecd.org/futures/globalprospects/37944611.pdf

[2] Emerging Risks in the 21st Century, the Secretary-General Emerging Risks, OECD, https://www.oecd.org/futures/globalprospects/37944611.pdf

[3] John J. HAMPTON, (2015), Fundamentals of Enterprise Risk Management, American Management Association, P. 227

[4] James HEMPSTEAD and William L. HESS, (2015), Threat of cyber risk is of growing importance to credit analysis, Moody's, https://www.moodys.com/research/Moodys-Threat-of-cyber-risk-is-of-growing-importance-to--PR_339656

[5] Karsten FRIIS and Jens RINGSMOSE, Conflict in Cyber Space: Theoretical, Strategic and Legal Pespectives, Routledge.

[6] The cyber-doom effect: The impact of fear appeals in the US cyber security debate, 2016 8th International Conference, Cyber Conflict (CyCon), (2016)

[7] Robert CHILDS (2017), London Market looks ahead Preparing for the next big insurance event, Hiscox, p. 4, http://www.hiscoxgroup.com/~/media/Files/H/Hiscox/results-centre/london-market-looks-ahead.pdf

– The cyber event, like terrorism, natural catastrophes or nuclear risks, "***could be the trigger*" for a new group of stress scenarios,** for example a successful disruption of utility services "*would trigger material knock-on effects to all other sectors*", and finally they could produce the so-called "*mega risks*" whenever the highest-risk sectors as critical infrastructure (Electric, natural gas, water and power plants…) will be affected[1].

The cyber extraordinary threats are the catastrophic risk of the 4º Revolution which have increased by the hyper-connectivity and materialized through IoT systems, so that characteristics indicate that a "*wide-ranging cyber events could create a catastrophe much more complex than any previously seen*" (CHILDS, 2017)[2]. These catastrophes are not completely modelled[3] yet, so we may anticipate they are an unknown insurance potential risks, as long as they possible affect to a huge range of sectors and policies.

Recently, there was an studied example of non-modelled cyber catastrophe event so-called "*Halloween blackout*" the scenario proposed by some of Lloyd's insurance companies would produce 45 billion of USD in total insured losses which will not be only relates to cyber policies, the report shows that losses will surely affect to the rest of insurance policies[4]. Definitely, **those are unidentified and unknown, they also have the potential to trigger damages to every sector and device, and they could affect to a wide range of insurance.**

After all, it is important to pay attention on the effects that could be made on Critical Infrastructure and the material damages which could be extended by IoT**. Those could produce the same consequences than any other extraordinary risk, and that makes us to consider them as a potential catastrophe threats**; which is the best reason to study the cyber extraordinary threats as an **individual category of catastrophic risks**. In that case, **they could be included under the coverage of some kind of fund or pool** -as those we have been referencing-.

5. Conclusions: The Cyber extraordinary risks Insurance

The cyber extraordinary risks are a new kind of catastrophic threats which have their own space, elements and potential damages with the same characters of the natural disasters but a completely different shape. As an example, the DDoS attacks. Precisely, on October 21st, 2016, the DDoS attack so called "*Mirai*" affected the servers of DNS (Domain Name System) services supplier Dyn and

[1] Dustin VOLZ (2015) Cyber attacks loom as growing corporate credit risk: Moody's, http://www.reuters.com/article/us-cybersecurity-moody-s/cyber-attacks-loom-as-growing-corporate-credit-risk-moodys-idUSKBN0TC2CP20151123

[2] Robert CHILDS, op. cit., HISCOX, (31st January 2017), p. 8.

[3] Robert CHILDS (2017), op. cit., Hiscox, p.22.

[4] Idem, p, 26.

that affect to the global internet traffic hardly (KENNEDY, 2016)[1]. The attack was perpetrated through different kinds of connected elements (IoT) with electronic components produced by XiongMai (KREBS, 2016)[2]; they had the same password and user name because those were automatically assigned by their producer.

Indeed, **the IoT systems are the causal link between those events which have taken place in the cyber space and material damages**, and these situations have been increasing by the hyper-connectivity. Therefore, **the traditional catastrophes could now produce** by IT systems, or by the use of them combined with **some material elements**; and the **cyber catastrophes** could produce **effects into the material world** through the IoT systems. Those considerations set out *"the liability in a hyper-connected world"*[3] scheme, which allows us to compare the above mentioned situations with the next causes and consequences:

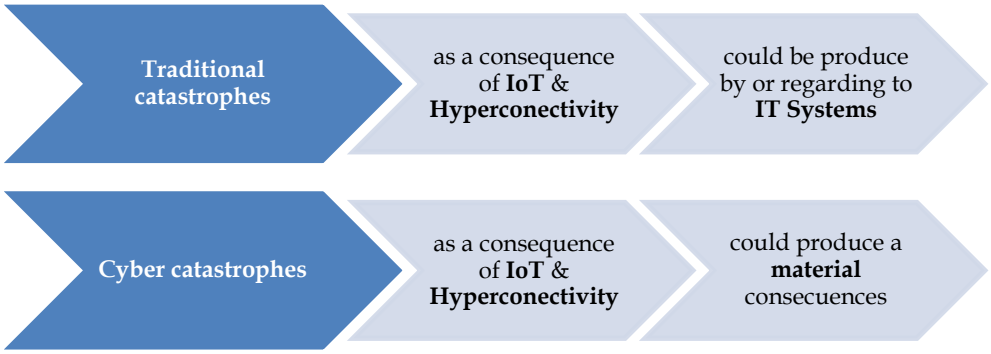


Figure 4: Causes and consequences of Cyber & Traditional Catastrophes

The Hyper-connectivity links IT systems, arising interconnected system. Those links change any kind of systems into a target, and they also would trigger damages to other systems. For this reason, the users and any kind of institution risk management systems (community responses) should be considered in the liability scheme, with the traditional catastrophic warranties and compensatory policies (traditional responses).

[1] John KENNEDY, Attack of the machines: Internet's biggest meltdown caused by Mirai botnet (October, 23rd 2016) https://www.siliconrepublic.com/machines/internet-meltdown-mirai-botnet

[2] Brian KREBS, (2016) IoT Device Maker Vows Product Recall, Legal Action Against Western Accusers, https://krebsonsecurity.com/

[3] Figure 41: Framework for Cyber Threats and Responses, Global Risks 2012,World Economic Forum (2012), p. 46.

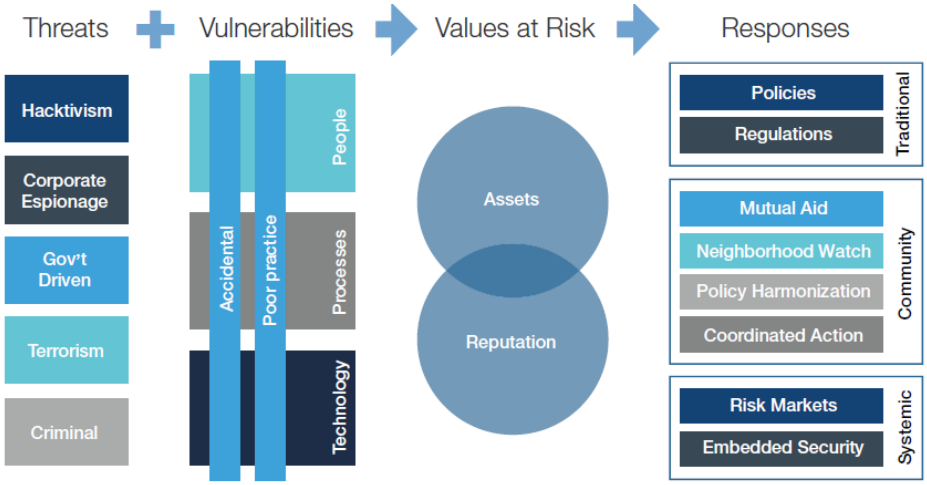


Figure 5: the liability in a hyper-connected world, World Economic Forum 2012[1].

The new manner of causing damages has two main characteristics: the anonymity of the agents and the cyberspace as digital environment. These characteristics require a new system of liability, because the traditional liability rules will not suffice to manage the damage caused by those elements. For that reason, in cyber risks it does not seem **possible to identify the party responsible** for providing compensation, since the complexity of cyber threats have increased and the causal relationship between damage and the human actions could be difficult to determine.

With the intention to provide a solution, the EU Report January 27th, 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)) *"considers that the civil liability for damage caused by robots is a crucial issue which also needs to be analysed and addressed at Union level"*. Thus, that recommendation expresses the possibility to create an obligatory insurance to cover these complex damages. Under this consideration, the report attempts to find a possible solution for allocating responsibility derivate to the damage caused by autonomous robots, this insurance system **should cover the human acts and the failures** –such the cars insurance-, and it should also **provide solution for the potential responsibilities in the casualty chain**.

Whereas, the large range of cases of the **concurred responsibilities or unknown link damages actions the report recommends to allow to the IoT manufacturer, programmer, owner or user to limited their liability** if they contribute to a compensation fund or contract an insurance to cover those damages. Moreover, it has expressed as a effectively solution the creation of a fund –based on the cars system of insurance funds- in order to ensure that reparation can be made for damage derived to some cases such when no insurance cover exists. Furthermore, **this compensatory fund could allow to the insurance industry to lead with the damages derivate to the cyber catastrophes, whose extraordinary characteristic could prevent to consider individual liabilities**.

As it has said, damages caused by cyber terrorism may be under the terrorism compensation fund and pool (even if they are produce by or regarding to IT Systems); so all kind of cyber terrorism

[1] Figure 41: Framework for Cyber Threats and Responses, Global Risks 2012, World Economic Forum (2012), p. 46.

are not cyber extraordinary risks. Cyber extraordinary risks are based on IT system dysfunctions or human actions (both unintentional and intentional), while terrorism is defined by its reasons or causes. Consequently, cyber extraordinary risks **may also derivate to cyber-attacks or cyber terrorist actions** (pure cyber terrorism), which are able to produce catastrophic consequences in, by or through the cyber space. In those cases, **the Insurance limits of cyber terrorism coverage should be focus on both elements (reasons and circumstances) forward to the reinsurance protection**.

Finally, every single action which taken place at the cyberspace has a lot of consequences and implications, those are more powerful and extreme if it affects the critical infrastructures, so these situations need to undertake the double perspective –public and private- of risks managing and responsibility. Farther this consideration, all institution and users will ensure their own systems, and the Insurance Industry –companies and compensatory systems- should develop a complete financial warranty system of IT threats as a part of the risk management solutions.

6. Bibliography

"Cyberpower and National Security: Policy Recomendations for a Strategic Framework," in Cyberpower and National Security, FD Kramer, S. Starr, L.K. Wentz (ed.), National Defence University Press, Washington (DC) (2009).

"Terrorism Risk Insurance Program". U.S. Treasury Department Website. U.S. Treasury Department. (March 20th 2013).

2016 Terrorism Risk Insurance Report, Marsh, (July 2016) P, 7. https://www.marsh.com/content/dam/marsh/Documents/PDF/USen/2016%20Terrorism%20Risk%20Insurance%20Report.pdf

A White Paper to the Industry on Systemic Risk , DTCC (October 2014), p. 1.

Advanced Targeted Attacks: How to Protect Against the New Generation of Cyber Attacks, FireEye, (2015), p. 4, http://www2.fireeye.com/rs/fireye/images/fireeye-advanced-targeted-attacks.pdf

Alexander W. VACCA (2012), "Military Culture and Cyber Security", Survival, vol. 53, nº6, p. 159.
Alistair SMOUT, (2017) Briton who promoted Islamic State with special cufflinks jailed for eight years, Reuters, http://www.reuters.com/article/us-britain-security-library/briton-who-promoted-islamic-state-with-special-cufflinks-jailed-for-eight-years-idUSKBN17Y17S?il=0

Brian KREBS, IoT Device Maker Vows Product Recall, Legal Action Against Western Accusers (October 24th 2016) https://krebsonsecurity.com/

Jeremy G. BUTLER, "A History of Information Technology and Systems", University of Arizona.

Careful how you code: Cyberterrorism coverage under TRIA and stand-alone cyber policies, Willis Towers Watson, (July 26th 2017), https://www.willistowerswatson.com/en-GB/insights/2017/07/decode-cyber-brief-careful-how-you-code

M. CASTELLS, The Rise of the Network Society. Oxford: Blackwell. (1996)

COBIT 5 for Risk, ISACA (2013) http://www.isaca.org/COBIT/Documents/COBIT-5-for-Risk-Preview_res_eng_0913.pdf

Cyber Risk– a Global Systemic Threat, a White Paper to the Industry on Systemic Risk, DTCC (October 2014)

Cyberspace, Oxford living Diccionaries, Oxford University, http://www. oxforddictionaries .com/us/definition/american_english/cyberspace

Daniel WILSON, ISIS-Linked Hacker Pleads Guilty In Cyberterror Case, Law360, https://www.law360.com/articles/808220/isis-linked-hacker-pleads-guilty-in-cyberterror-case

Definition of a Research and Innovation Policy Leveraging Cloud Computing and IoT Combination, Digital Agenda for Europe, European Commission DG Communications Networks, Content & Technology, pag. 9, http://ec.europa.eu/newsroom/dae/ document.cfm?doc_id=9472

Derek O'HALLORAN, Tech utopia or cybergeddon?, (January 22sd, 2013) https://www.weforum.org/agenda/2013/01/tech-utopia-or-cybergeddon/

Dustin VOLZ, Cyber attacks loom as growing corporate credit risk: Moody's, 23 November 2015, http://www.reuters.com/article/us-cybersecurity-moody-s/cyber-attacks-loom-as-growing-corporate-credit-risk-moodys-idUSKBN0TC2CP20151123

Eguskiñe LEJARZA ILLARO "Ciber guerra los escenarios de confrontación", Instituto Español de Estudios Estratégicos nº 14 (February 2014), p. 2-4.

Emerging Risks in the 21st Century AN AGENDA FOR ACTION, OECD (2003), p. 12. https://www.oecd.org/futures/globalprospects/37944611.pdf

Emilio SÁNCHEZ ROJAS (2010), "¿Ciber…qué? La ciberseguridad", Ejército, vol. 837, p 138.

Eneken TIKK (2011), "Ten Rules for Cyber Security", Survival, vol. 53, nº3, p 119.

Financial Stability Report, EIOPA, (2017), p. 19, https://eiopa.europa.eu/Publications/Reports/Financial_Stability_Report_June_2017.pdf

Frederick WAMALA, The ITU National Cybersecurity Strategy Guide, CISSP (September 2011).

Gary STONEBURNER, Alice GOGUEN y Alexis Feringa RISK, (2002), Management Guide for Information Technology Systems, National Institute of Standards and Technology NIST SP 800-30

Giulio CORAGGIO, Cyber risk insurance – a solution to cybercrime? http://www.gamingtechlaw.com/2015/10/cyber-risk-insurance-cybercrime.html

Giulio CORAGGIO, The Internet of Things cannot be 100% secure?, IoTLAW Law of the Internet of Things, https://iotlaw.net/2015/11/02/the-internet-of-things-cannot-be-100-secure/

Giulio CORAGGIO, what is an adequate standard of security?, IoTLAW Law of the Internet of Things, https://iotlaw.net/2015/11/02/the-internet-of-things-cannot-be-100-secure/

Global Risk Report, World Economic Forum (2011).

Global Risks 2012, World Economic Forum (2012), pp. 24-25.

ISO/IEC 27005:2011, Terms and definitions, ISO, Online Browsing Platform (OBP), https://www.iso.org/obp/ui/#iso:std:56742:en

ISO/IEC 27032:2012 Information Tecnology Security Techniques, Guidelines for Cybersecurity, ISO, http://www.iso.org/ iso/iso_catalogue /catalogue_tc/catalogue _detail.htm ?csnumber=44375

James HEMPSTEAD and William L. HESS (2015) Threat of cyber risk is of growing importance to credit analysis, Moody's, https://www.moodys.com/research/Moodys-Threat-of-cyber-risk-is-of-growing-importance-to--PR_339656

James J. CEBULA y Lisa R. YOUNG (2010), A Taxonomy of Operational Cyber Security Risks, Carnegie Mellon University, Software Engineering Institute, Pittsburgh, PA, http://bit.ly/1NEBcTU

John J. HAMPTON (2015), Fundamentals of Enterprise Risk Management, American Management Association, p. 227

John KENNEDY, (2016) Attack of the machines: Internet's biggest meltdown caused by Mirai botnet, https://www.siliconrepublic.com/machines/internet-meltdown-mirai-botnet

Jason KRAUSS, Carefull How you Code…, Willis Towers Watson, https://www.willistowerswatson.com/api/sitecore/Article/Download?itemId=07ca0cd8-23b3-479d-96e1-3f17c23da863&lang=en-GB

Jhon Perry BARLOW (1996) A Declaration of the Independence of Cyberspace, Electronic Frontier Fundatio EFF, https://www.eff.org/es/cyberspace-independence

José María MOLINA MATEOS (2013), "Ciberdilema", Instituto español de estudios estratégicos nº 115, p.1 http://www.ieee.es /Galerias/fichero /docs_opinion/2013 /DIEEEO115-2013_Cyberdilemma_JM.MolinaMateos.pdf

Julian ENOIZI (2016), Message from the Chief Executive, Pool RE, https://www.poolre.co.uk/newsletters/PoolRe-Newsletter-0416-for-web.pdf

Karsten FRIIS and Jens RINGSMOSE, Conflict in Cyber Space: Theoretical, Strategic and Legal Pespectives, Routledge.

Harold J. LEAVITT and Thomas L. WHISLER (1958), Management in the 1980s, Harvard Business Review, p. 11.

Matt MCCABE, Cyber Terrorism: Does Your Insurance Cover the Gaps?, Marsh (July 15th, 2016), https://www.marsh.com/us/insights/risk-in-context/cyber-terrorism-does-your-insurance-cover-the-gaps.html

Chip MORNINGSTAR and F. Randall FARMER (2003), The Lessons of Lucasfilm's Habitat. The New Media Reader. Ed. Wardrip-Fruin and Nick Montfort: The MIT Press.

Owen COTTON-BARRATT, Sebastian FARQUHAR, John HALSTEAD, Stefan SCHUBERT, Andrew SNYDER-BEATTIE, Global Catastrophic Risks 2016, Global Catastrophic Foundation, http://globalprioritiesproject.org/wp-content/uploads/2016/04/Global-Catastrophic-Risk-Annual-Report-2016-FINAL.pdf

Pan American World Airways, Inc. V. Aetna Casualty & Surety Co. en Jason Krauss, op. cit., Willis Towers Watson, https://www.willistowerswatson. com/api /sitecore/ Article/Download?itemId=07ca0cd8-23b3-479d-96e1-3f17c23da863&lang=en-GB

POOL RE TERRORISM ENDORSEMENT, http://www.lmalloyds.com/CMDownload.aspx?ContentKey= e1df14f4-f0 66-41b7-a635-23298fc58 0d4&Conte ntItemKey= d3219f2e-9772-4e92-a9c1-c28dbfea3fb0

Pool RE Terrorism Endorsement, LMA5225 (October 1st, 2015) www.lmalloyds. com%2FCMDownload.aspx%3FContentKey%3De1df14f4-f066-41b7-a635-23298f c580d4%26ContentItemKey%3Dd3219f2e-9772-4e92-a9c1-c28dbfea3 fb0&usg=A FQjCNGNBkly-aVlqHSG75uF66kFtg9rjQ

Risk and Responsibility in a Hyperconnected World, World Economic Forum (February 2014), p. 5, http://www3.weforum.org/docs/WEF_IT_Pathways ToGlobal Cyber Resilience _Report_2012.pdf

Robert CHILDS (2017), London Market looks ahead Preparing for the next big insurance event, Hiscox, p. 4, http://www.hiscoxgroup.com/~/media/Files/H/Hiscox/results-centre/london-market-looks-ahead.pdf

Sebastián KOCH MERINO, "Libertad en el ciberespacio", Revista de Ensayos Militares vol. 1 nº2 2015 p. 92

Systemic Risk Barometer, DTCC (2014), http://www.dtcc.com/~/media/Files/Downloads/issues/ risk/Systemic_Risk_Summary_Report.ashx

Terrorism pool or Reinsurance Mechanism, 2016 Terrorism Risk Insurance Report, Marsh, (July 2016) P, 8. https://www.marsh.com /content/dam/marsh /Documents /PDF/USen/2016%20Terrorism%20Risk%20Insurance%20Report.pdf

The cyber-doom effect: The impact of fear appeals in the US cyber security debate, 2016 8th International Conference, Cyber Conflict (CyCon), (august 2016)

The role of Pool Reinsurance Company Ltd, Pool RE, (June 9th, 2017) https://www.treasury.gov/initiatives/fio/acrsm/Documents/ACRSM_Presentation_By_Pool_Re.pdf

Top 5 Risk Identified, Risk to Broader Economy, Systemic Risk Barometer, DTCC (2014), p. 3 http://www.dtcc.com/~/media/Files/Dow nloads/issues/risk/Systemic_Risk_Summary_Report.ashx