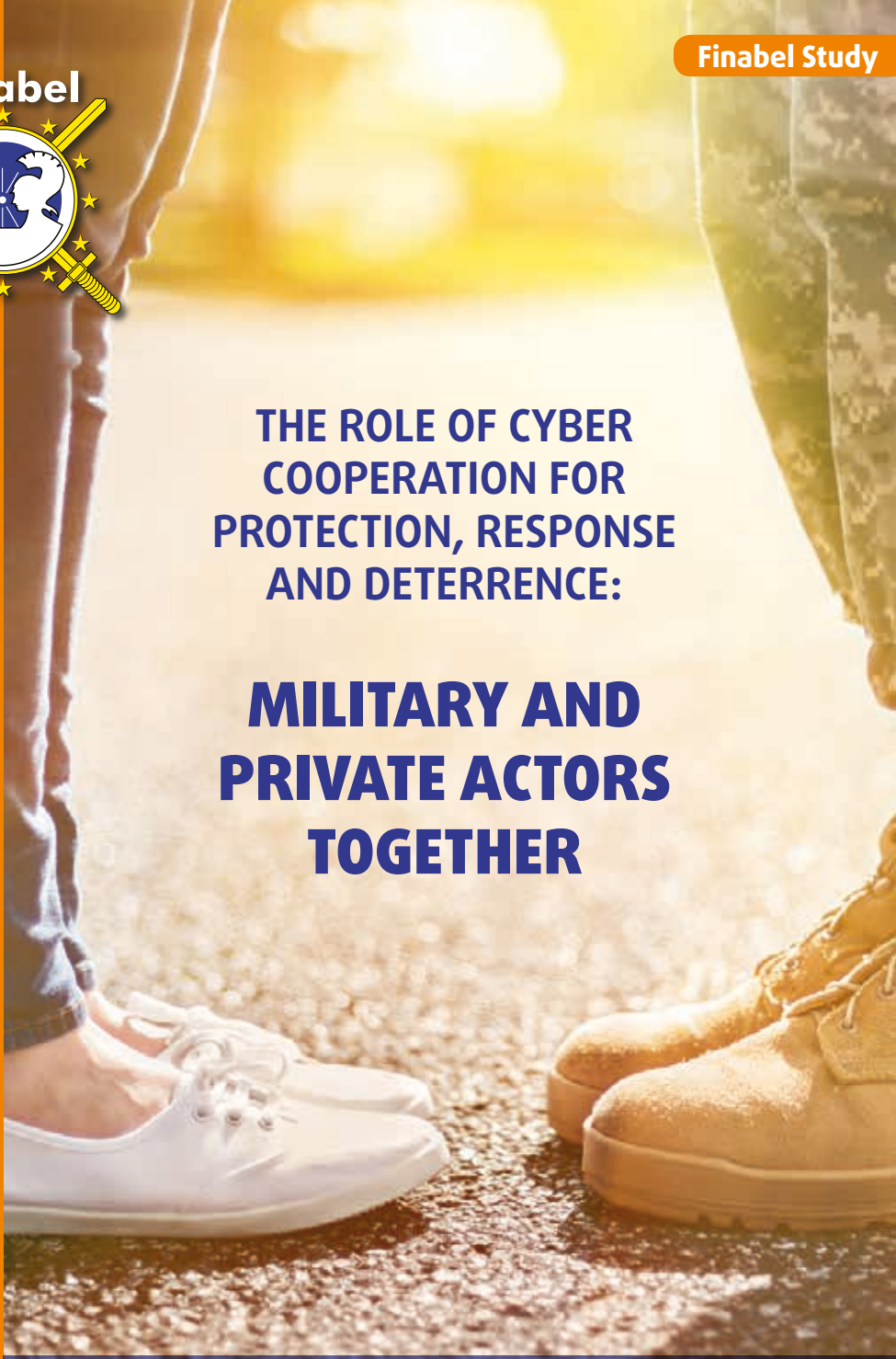
Finabel

Finabel Study

THE ROLE OF CYBER COOPERATION FOR PROTECTION, RESPONSE AND DETERRENCE:

MILITARY AND PRIVATE ACTORS TOGETHER



AN EXPERTISE FORUM CONTRIBUTING TO EUROPEAN ARMIES INTEROPERABILITY SINCE 1953

FINABEL
European Army Interoperability Center

This text was drawn up with the help of **Mrs. Gaia Morosi**, trainee, under the supervision of the Permanent Secretariat.

TABLE OF CONTENTS

LIST OF ABREVIATIONS

CEO	Chef executive officer
CERT-EU	Computer Emergency Response Team of the European Union
EDA	European Defence Agency
ENISA	European Union Agency for Network and Information Security
EU	European Union
ICANN	Internet Corporation for Assigned Names and Numbers
ICT	Information and Communications Technology
IETF	Internet Engineering Task Force
NATO	North Atlantic Treaty Organization
NCIRC	NATO's Computer Incident Response Capability
OSCE	Organization for Security and Co-operation in Europe

INTRODUCTION

In 1997, during a conference in San Francisco, the CEO of Google – Eric Schmidt – affirmed: "The Internet is the first thing that humanity has built that humanity doesn't understand, the largest experiment in anarchy that we have ever had." (Singer, Friedman, 2014: 35).

These words introduce perfectly the complexity of the cyber security sphere and the challenge that all the international actors have to face every day, especially in the defense sector. The necessity to guarantee their security and stability face off against the impossibility to completely govern and control this new sphere. In fact, as no-state concept, cyber presents some characters that are completely different from the traditional security dimensions, making inefficient all the previous defense measures used by the actors for their defense (Terzi, 2015: 13-17).

The consequence is a necessity to elaborate a new way in which the actors consider security. In this new vision, the action of single agencies and entities could no more be sufficient. Due to the absence of hierarchy in this system, cyber asks for the creation of networks for its efficient management. A constant and consolidated work of States, international organizations, private and public actors is the only way to go completely out from the anarchy created by the new technology. Military actors are not excluded by this work. On the contrary, their key role must be recognized not only for the identification of responses to attacks but also for the elaboration of efficient measures for prevention and deterrence (Christou, 2016: 35).

Despite all the attempts made in the last years in the sense of cyber cooperation, the creation of a real network is far from being created: most of the existent partnership put together actors of the same nature. A solid collaboration between public and private actors is the central condition for the future management of this new dimension of security: the only way to have a complete vision on the cyber sphere and its characteristics based on different point of analysis and at different levels.

The coordination between civilian and military actors goes perfectly in this direction. In particular, differently from other entities, this partnership could directly

The role of cyber cooperation for protection, response and deterrence: military and private actors together

have an impact on prevention, deterrence and response to cyber-attacks, once they are in place. In fact, the capacities of the civilians together with the experience on defense field offered by the military actors could elaborate multiple-level measures for the guarantee of security, especially through security information sharing, common exercises and joint researches.

Estonia offers today a great example of method of management of the cyber sphere: the solution to the cyber-attacks in 2007 was possible only though the comprehension of the necessity to create a network. Starting from that moment, the state has developed an efficient system of management of cyber, based on collaboration at different level. This is the reason why this State is considered today a leader in the sphere and a guide followed by the other states at the domestic level. Nevertheless, at the international level, the network is far to be created. Especially in terms of collaboration between civilians and military actors, there is a lot of work that needs to be done.

The objectives and the organization of the paper

This study has the objective to explain the importance of a cooperation between civilian and military actors in order to encourage future attempts in this sense, both domestically and at the international level. The two entities must understand why their partnership is central and which could be its benefices. At the same time, also the explication of the limits that the partners will experience is fundamental in order to create stable basis for a future efficient joint action. These factors must not be considered as obstacles and reasons of failure but as elements that must be considered for create a real success.

For all these reasons, this work will be divided in three parts: necessities of the cooperation, advantages and limits.

The first part will be devoted to the explications of the elements that make cyber different from all the previous security dimensions. These characteristics – or necessities - have to be taken into account in every attempts of management of the cyber sphere, especially in the case of collaboration between different actors. In fact, only knowing these elements, the elaboration of efficient policies and strategies will be possible.

The second chapter will analyze the main benefice that the collaboration between civilian and military actors will have for the cyber sector. In particular, the attention will be focused on the security information sharing and the creation of common exercises, training and researched on the sector. The different nature of military and civilian actors will help in elaborating a complex vision on the cyber sphere: a key element for creating efficient policies and strategies.

Finally, the third part will furnish an explication of the main limits that a future cooperation will experience. The absence of an international unique definition of cyber is one of the main factor of block, together with the necessity of trust between the actors: an element that could be developed only after years of collaboration. Even in this case, the knowledge of these elements could help the future attempts of collaboration with the actors in order not to incur in blocks and failures.

Reading this work will furnish the first and most important guidelines for the creation of strong, durable and efficient forms of cooperation. Only if they have in mind this factor, civilian and military actors could cooperate in an efficient way for the elaboration of policies and strategies in the cyber domain.

WHY COOPERATION IS FUNDAMENTAL FOR CYBER DIMENSION

The uniqueness of the cyber security has always been evident: it presents a level of complexity that is completely new in the security domain. In particular, cyber has some characteristics that are unknown to the previous type of defence technologies (Terzi, 2015: 13-17).

This difference is due to the origins of the digital system, which is outside international relations and defence. In fact, at the moment of its creation – at the beginning of the 90s - the term "cyber" was used exclusively inside the scientific context. Its introduction in political studies was possible only some years later when the "networked computer" technology was introduced by national institutions and organizations as facilitator of their work. Nevertheless, even if this new instrument guaranteed to increase the efficiency of the public entities, also their weakness augmented: non-authorized actors could enter into the system and capture secret information and data. This concern was the reason why States started to be careful about the new dimension already during the last years of the Cold War. From that moment on, cyber risks were considered as new challenge for their national and international security (Hansen, Nissenbaum, 2009: p.1155).

Nevertheless, it was in 2007 that the prospective of states changed toward completely. The cyber-attack[1] on the Estonian public and private institutions in that

[1] In 2007, Estonia was the victim of a massive cyber-attack that completely blocked the online systems of state institutions, banks and media. Some of these services were blocked for weeks. This attack had dimensions never seen before and it was the first big chance to understand the limits in the elaboration of responses, like the difficulty in the identification of the origin (McGuinness, 2017). This element make the Estonian cyber-attack as particularly important for the definition of the following international policies in this field. In fact, after this case, the international institutions have developed the international pillars of the sector, starting from the general recognition of cyber as new dimension of security, together with the most traditional ones, as we will see in the first chapter. It is important also to underline that after 2007, Estonia has become one of the most engaged country in the cyber security sector: today, it offers a great example for other actors in the international scene.

year was the demonstration of the great risk that every country would face: in a few hours, a State could be completely blocked and the possibilities of reaction are really limited. It was at this occasion that for the very first time in history a government officially used the terms "cyber war" and "cyber arm" (Nye, 2011: 19). At the international level, the perspective toward this domain changes completely: cyber was considered officially a new dimension of the international security after space, air, naval and land (Terzi, 2015: 13-17).

The attention and will of action of the States face off against the complexity of a no-state sphere that is mostly impossible to be completely controlled or governed. The measures used until that moment for guarantee defense appear insufficient for the cyber sphere (Christou, 2016: 35).

Therefore, the actors must use new forms to protect their security. Their efficiency could be guaranteed only through the knowledge of the principle characteristics of the cyber technology.

1. The proliferation of cyber and its dual use

Proliferation is not a concept unknown by all the other security dimensions different from cyber. In fact, every time that an arm is introduced in the international system, the arms race is an obligation for all the States in order to be competitive. This element guarantees to the new technology to gain a global dimension. We have observed this phenomenon all the times that a new arm was created: the case of the nuclear technology is the most evident in the contemporary époque.

Nevertheless, the case of cybersecurity presents some differences from the previous ones due to its particular character of "dual use" technology. Everyone can use it in any kind of situation: individuals, states, private and public national, international agencies, terrorist and criminal groups are all actors that use the cyber instruments for different activities. Therefore, in this case, the term "proliferation" takes a new sense in the cyber dimension: it is not a fight of States for the possession of an arm but is the multiplication of different actors in the same sphere. The consequence in the security sphere is a difficulty in the identification of cyber as a possible military arm and at the same time an insufficiency of the traditional measures of control that normally were used in the security dimension (Terzi, 2015: 13-16).

This factor has a major impact in the management of a no-state concept, like the cyber one: systems where the traditional borders are completely absent and where anarchy is the governing rule. In fact, the geographical delimitation typical of the Westfalian system cannot be applied to the new security dimension (Demchak, Dombrowski, 2014: 30). Cyber technology goes beyond the traditional limits that the States have fixed for their territory (Hare, 2009: 1).

The consequence is a redefinition of the concept of border this time using a symbolic prospective at the place of the geographical one: a substitution of the tangible elements with symbolic ones. Therefore, the limits of demarcation become virtual and characterized by social communities and networks. The result is a more elastic definition compared to the traditional one: it can cause confusion especially in case of the elaboration of strategies in response to cyber attacks (Jiménez, Orenes, Puente, 2010: 215-218).

2. Difficulties in the identification of the origin of the menace

The particular type of proliferation of the cyber dimension is also at the basis of another characteristic of this field: the difficulty in the identification of the origins of the threat. Differently from other traditional arms, in the case of cyber-attacks the analysis of the traces is mostly impossible: the absence of physical evidences make more and more difficult the identification of the responsible. Moreover, the constant technological evolution of this dimension does not help the creation of measures to face an attack[2] (Singer, Friedman, 2014: 31-34).

Therefore, in many cases, the international cooperation has appeared as the only guarantee of solution to this problem: the States could try to identify the origin of the attack thanks to consultations and exchange of information (Kramer, Teplinski, 2013: 8).

3. Constant technological evolution

The management of the cyber security dimension is also made difficult by the constant technological evolution of this sphere. The "daily" improvements in the cyber performances increase the complexity in the prevention and response to the attacks: very time, their efficiency augment. As consequence, the measures elaborated and used since that moment for the recognition and response appears as obsolete (Singer, Friedman, 2014: 13). Therefore, the ability of states and armies to elaborate plans of short or long term is very limited.

Nevertheless, it is also important to notice that the technical evolution of the cyber dimension has also positive aspects. In fact, the new discoveries have guaranteed the elaboration of solutions that have greatly improved the everyday life. Therefore, at the same time, a great number of technological evolutions have produced both positive and negative effects. The biggest example in this case is represented by the creation of the "Big Data": a new type of data that "contains" others. This technological evolution has allowed the creation of systems of communication more simple and efficient thanks to the collection of a series of information in a unique data. These large datasets have been existed for a long time but they became widely available thanks to the creation of computers capable of analyzing them. Starting from this time, this system has been greatly used by libraries – for their catalogues- and governmental institutions (Cukier, Mayer-Schöenberger, 2013). Nevertheless, the natural consequence has been the increase in the efficiency of the cyber-attacks to the systems of communication. In fact, a strike to one of these data is sufficient in order to have access to a great number of information, which could also be linked to national security. The "Snowden" case is only an example of the efficiency of these kinds of attacks (Lyon, 2014: 7). This double effect prevent from a total ban in the use of these technological discovery. The only possibility to control them is a constant action of prevention to the attacks that must be conduct through a collaboration of multiple actors.

4. The big dilemma of decision-makers: web freedom or national security?

The cyber dimension is also the responsible for the birth of a new and great dilemma in the policy field: which elements must be privileged between web freedom and national security?

This dilemma has had a great influence in the decision-making choices for the elaboration of cyber policies and measures to face attacks: the necessity to guarantee both elements has had a great impact. From one side, the respect of the web freedom is directly linked to the rights of expression and information: internet is an instrument that permits to communicate, express and spread ideas without censorships (Singer, Friedman, 2014: 16). Therefore, a strict control of the network would have as consequence a limitation of this liberty and of the privacy of every citizen (ENISA, 2012: 29).

[2] The problems linked to technical evolution will be explained in details in the following paragraph, chapter 1.3

Nevertheless, the monitoring of internet guarantees another priority: the national security. In fact, the need for state actors to prevent and respond to possible cyber-attacks implies a direct control on the activities that are done on the web (Terzi, 2015: 21). This is a consequence of the possibility of every actor to use this technology without limits: governments could effectively avoid cyber-attacks only though the reduction of the web freedom and the individual privacy.

Here is the dilemma that every democratic country[3] has to face also at the general intelligence and military level: one factor seems to prevent the other and vice versa. The necessity to guarantee the national security seems in opposition with the right of freedom and privacy of the individuals. This will be the future challenge for the democratic countries that must show the possibility to combine security and freedom (Singer, Friedman, 2014: 107).

Also in this case, the creation of global cyber governance seems to be the only solution to the dilemma: an international collaboration would avoid the necessity of a direct and strict control of the national authorities through the identification of efficient ways of management of the cyber dimension.

[3] In the case of authoritarian regimes this dilemma is completely absent for the decision makers. In these countries, the reduction of all the freedoms is justified as a necessity to guarantee the internal stability of the state. In particular, these governments use internet as instrument of control of the internal oppositions and the foreign enemies (Singer, Friedman, 2014: 107). The democratic countries must keep on being an alternative to these regimes, showing that it is possible to guarantee at the same time freedom and security.

THE BENEFICES OF A MILITARY-CIVILIAN COOPERATION

As seen in the previous chapter, the particular characters of the cyber dimensions require special measures for prevention, identification and response to future attack: the strategies used for the traditional security dimensions are not applicable because of the characteristics of the new technology. In particular, single actors will not be able to elaborate and put in action successful cyber policies without the collaboration with public and private partners (Drent, Homan, Zandee, 2013: 57).

In this context, cooperation has to be defined as a strategic alliance that guarantee a coordination *"between two or more partners to pursue shared objectives"* (Das, Teng, 1999: 491). The result is a networking action between different entities, which has to be considered as the corner stone of all types of cyber security policies.

An important part of this network is surely represented by the collaboration between civilian and military actors. Its role from an operative point of view is undeniable. In fact, it could solve some of the main limits of the elaboration of strategies in case of offensives, through the exchange of information and the creation in researches and trainings. These actions could help to understand completely the rapid technological evolution of the cyber sphere and at the same time find efficient answers to prevent and response to attacks.

Therefore, this type of alliance could guarantee benefice to both entities and more in general to the entire international scene. In fact, the two actors could offer an example of cooperation and give some basis for the harmonization of rules, the signature of future agreements and consequently the elaboration of common strategies in the cyber security domain.

This chapter is devoted to the explication of the main activities that could be promoted by the collaboration between civilians and military actors: the security information sharing and the creation of common researches and trainings. Why are these actions so important in the cyber sphere? Which benefices could they provoke for civilians and military actors? These questions will be the focal point of the analysis of this chapter.

1. Security information sharing

The connection of dots between the actors has always been considered as central for all dimensions of security, despite the difficulties in its realization. This importance is due to its fundamental role in the creation of a law force defense intelligence, able to give strong answers to the threats under different points of view.

More than other sectors, in the cyber domain, the exchange of information between different entities acquires a special role due to the particular characters of this technology. In fact, in an anarchical system where traditional borders have been substituted by virtual ones, only collaboration could give more possibilities to understand the origin and the dimension of the attack: the only way to elaborate efficient strategies to counter-attack[4].

In the experienced cases of cyber-attacks – including the Estonian one – this aspect has been evident: the security information sharing and the cooperation between systems of intelligence became central for the solution of the crisis. In this sense, the case of the Sony Picture offers a great example of the success of this strategy. In 2014, the systems of the company had been the victim of a big cyber-attack, which make some of its sensitive information public. Since the beginning, North Korea claim the act: their objective to block the creation and diffusion of the movie "The interview", a story of the Korean president Kim Jong Un. During this offensive, the collaboration between China[5] and United States was fundamental in the elaboration of an efficient answer and solution to the attack. After this case, the two States showed the will to establish stable basis for a future cooperation between them and their systems of intelligence but the actions in this sense are currently limited (Terzi, 2015: 17-18).

In any case, today the importance of security sharing for cyber is globally recognized: this is not a case that it is one of the basic point of cooperation between a series of private, public and international actors. For example, the exchange of dots is one of the pillars of

[4] As we have seen in the first chapter (1.2), the new virtual boards and the special character of dual use of the cyber strategy made the identification of the origin of the menace as particularly difficult. Only the exchange of information between actors could help in this sense.

[5] The presence of Korean technicians in China was central in this collaboration with United States (Terzi, 2015: 18)

the recent agreement[6] between the NATO's Computer Incident Response Capability (NCIRC) and the European Computer Emergency Response Team (CERT-EU) (Sarma, 2016). Moreover, the security information sharing is considered one of the main strategies of the European Union Agency for Network and Information Security (ENISA) for the coordination of the member states of the European Union (ENISA, 2015: 47).

Nevertheless, compared to states and international organizations, the security information sharing between civilian and military actor would acquire a further and special importance in the management of the cyber security dimension. In fact, in this case, the exchange of information will not only be important for the elaboration of strategies in case of attacks but it will allow the actors to better understand the general characteristic of this new security dimension, especially concerning the rapid technological evolution. Thanks to the security information sharing, civilian and military actors would conduct common researchers and exercises, which will guarantee to use measures in line with the constant changes of the cyber sphere and the new strategies used for the attacks. The force of this type cooperation will be in the different nature and prospective used by these two entities: an element that will guarantee to take into account different factors, obtaining a complex and complete analysis of the cyber dimension.

Therefore, considering the increase of the cyber-attacks in the last years, the creation of the collaboration between civilian and military actors appears more and more necessary for the destiny of the international systems of security. The security information sharing must be considered as one of the pillars of this cooperation if we want to obtain the best results in the elaboration of strategies for response and prevention.

[6] In 2016, the staffs of NCIRC and CERT-EU signed the Technical Arrangement on Cyber Defence: "a framework for exchanging information and sharing best practices between emergency response teams of both the organisations, keeping into account their decision-making autonomy and procedures." (Sarma, 2016). It was the main result of this joint work in the new security field. In fact, for the very first time in history, the cyber collaboration is officially recognized as one of the new priorities of the EU-NATO cooperation that has to be followed through the share of good practices and the exchange of information. In order to achieve this second objective, in 2017 the Alliance has also guaranteed the access NATO's Malware Information Sharing Platform to the CERT-EU (Sarma, 2016).

2. Common training and researches

As seen in the previous chapter, the constant evolution of the cyber technology is one of the main factors that make it different from the other dimensions of security, creating problems in the prevention and response to attacks. In fact, the "daily" changes[7] of the technology ask for a constant analysis of this domain in order to have a fast adaptation to the new assets, understanding the new dynamics and elaborating efficient measures.

Nevertheless, this constant analysis of the cyber sphere ask for a great effort in terms of abilities, energies and costs. Concerning this last point, only in the last year the average annualized cost of cyber security per each organization that works in the sector is $11.7 million: it represents a general increase of 22.7% only compared to 2016. These data are independent from the type of actors and the action that is put in place: an increase in the attention towards this dimension can be observed for every entity. Surely, the dimension and objective of each organization determine a different amount of energies used in the cyber research. In particular, it was possible to observe that the entities that work on financial services have a major involvement in the cyber research, also compared to actors of the defense sector (Ponemon Institute, 2017).

Nevertheless, the last study presented by the Ponemon Institute on the costs of cyber underlines the particular investments made by cyber criminals for the development of new technologies. In general, the efforts of these actors change on the base of the attack that is put in place: especially the actions on malware require a major involvement compared to others. Nevertheless, the investments and the interests towards the cyber dimension are always major than the ones of other legal entities. The consequent result is a gap of capabilities between cyber criminals and the other actors, included international organizations, governments and privates: a difference that is evident in the case of attacks for the impossibility to find an efficient answer (Ponemon Institute, 2017).

The inability of the non-criminal organizations to lead research at the same level of the criminal actors is in particularly due to the large amount of money requested by this type of analysis. Especially international organizations and governments do not have the necessary financial capabilities to do a constant action on this sector (Ponemon Institute, 2017).

In this context, cooperation can offer the best solution to this problem, putting together the economical energies and the operational abilities of different actors – private and public.

Surely, also the collaboration between civilian and military actors must be included in this context: an effective way to maintain security and guarantee defense both at the big data[8] and at the small data[9] level. The use of the same hardware and software technology[10] by both entities could help the two spheres to collaborate in producing common researches, standards and trainings. In the same way, also the security information sharing can go in the same direction, facilitating a common action between the different entities (Röhrig, Smeaton, 2014: 26).

Surely, common researches and training could facilitate particularly the action of these actors in the small data sector: a new topic, which ask for special efforts in terms of costs. This aspect of the cyber technology has been ignored in the past but it has showed to have special implication in the military domain because it will guarantee to put in action rapid and efficient attacks. Nevertheless, compared to the big data analysis, the particular character of the small data and the absence of past researches in this sector ask for additional costs in order to understand their functioning and evolution.

[7] To have more details concerning the technological evolution of cyber sphere, please consult chapter 1 section 3. This character of the cyber security dimension is one of the reasons of the difficulties in the creation of a common definition of this sphere and the elaboration of efficient ways to respond to the attacks.

[8] See chapter 1.3

[9] The term "Small Data" refers to data that has small enough size for human comprehension. While big data have been at the center of the debate for many years, small data have not usually been considered in the analysis despite their importance in the management of the cyber dimension. Nevertheless, they represents the chance to understand better the cyber dimension in every aspect. In fact, small data can also guarantee a simplification of the big one and a real analysis of the main characteristic of this technological element (Pollock, 2013).

[10] It is important to notice that, concerning the military sphere, the use of hardware and software technology is the same in the case of classified and unclassified information (Röhrig, Smeaton, 2014: 26).

Therefore, for the military actors, the collaboration with civilian entities in this context could be particularly interesting, guarantying to lead an efficient analysis with a financial effort that can be support without particular problems. Moreover, this cooperation would be also a way to limit the requests for cyber experts for the army. This aspect is particularly central: in the last years, all the countries have experimented a difficulty in recruit new components with high qualification in the new security dimension. The collaboration with the civilian sector could help in surpassing this limit and develop great abilities thanks to the use of experience coming from outside.

Therefore, the creation of this type of collaboration between civilians and military actors will be the real turning point in the cyber security analysis and management: the crucial step for the future of defense and security.

HOW CREATE COOPERATION: THE FACTORS TO TAKE INTO ACCOUNT

The centrality of the cooperation between civilian and military actors in the management of the cyber security dimension does not preserve it from difficulties in its elaboration. Limits could interest all the process from the creation to the realization of the partnership, independently from the form of collaboration chosen by the actors. Constant or occasional meetings, common trainings or researches, signature of pacts and agreements, security information sharing: the same type of weaknesses could block all these types of cooperation. Only the understanding of these factors could facilitate the successful realization of the collaboration, by promoting the identification of possible solutions.

In the particular case of relations between civilian and military actors, two are the main elements that could block the dialogue on the new security dimension: the absence of a unique international definition of cyber and the difficulty in the definition of trust between the different entities. This chapter has the objective to analyze these two elements in details, underlining their characteristics and which could be the best way to surpass them. As underlined before, this explication is fundamental for each attempts of elaboration of a cooperation between civilian and military actors:

the creation of an efficient relation could be possible only considering these elements, their effects and the possible solutions.

1. The formulation of a common definition of cyber

The impossibility to identify a unique global definition of cyber is the main limit for the creation of an efficient cooperation. So far, States, national and organizational institutions, private and public actors have never been able to find a point of contact on what for them cyber is and which elements must be considered as priorities. This inability of the international entities is due to the complexity of the sphere, his great dimension and the continuous technological evolution: all factors that make this step difficult to be realized.

Even the different attempts made by literature have not been able to create sufficient results in this sense (Bayuk et al., 2012: 2). In fact, in each study, the authors elaborate definitions, which are completely different the one from the others, underlining opposite aspects of the same dimension. Moreover, the results also appear to be very generic, vague and unable to capture the attention on the main elements of the technology[11]. One of the major examples is furnished by the definition elaborated in 2008 by a team of experts of the US Pentagon. In fact, for them, cyber is "the global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the internet, telecommunications networks, computer systems, and embedded processors and controllers" (Singer, Friedman, 2014: 12). The inclusion of the major elements of the cyber does not guarantee to have a clear and specific definition: the work seems too vast and vague (Singer, Friedman, 2014: 12-13).

A result is the fact that also linked terms such as "cyber-attack", "cyber arm" and "cyber security" have not been defined since now in a way that could be accepted by all international actors (Singer, Friedman, 2014: 12-13).

As consequence, the majority of times, the term is abused because of the confusion that exists about its meaning. Especially the political leaders show to be unprepared on the main characteristics of this dimension, influencing their attitude towards this sphere (European Parliament, 2015: 20). Randall Dipert affirms that the consequence of this lack of preparation of the leaders is an evident "virtual policy vacuum" that interests both security and warfare sector on the cyber questions. In fact, this unfamiliarity with the technology prevents the possibility to create measures in response to possible attacks: the elaboration of a global cyber-terminology and the identification of all the different types of cyber threats are almost impossible in such a context (Taddeo, Glorioso, 2017: 2).

The absence of a definition generally accepted is not only a formality in the management of the new security dimension. In fact, it is a real and great limitation in the collaboration at the practical level because it prevents from having a common starting point between the actors. Each entity uses a different attitude towards cyber and consequently a divergent type of prevention and response to attacks: everyone reserves its attention to different aspects of cyber (European Parliament, 2015: 19).

The majority of the authors consider these differences as a difficulty present "in all the emerging areas of study" (Kremer, Muller, 2014: 23) and a normal condition in a technology – like cyber - that has suffered such a quick development since the beginning of its existence (Singer, Friedman, 2014: 13).

Nevertheless, the absence of a unique global definition has a great impact in the ability to manage the cyber dimension in an efficient way. In fact, this element could be indicated as the main limit for the creation of policies and theories in this sector more than a block for the harmonization of rules and applicability of international law to the new technology.

Concerning this last point, the numerous initiatives of public and private actors to promote the harmonization have not registered particular successes. The most recent example is the proposal made by Brad Smith - President of Microsoft Corporation – during the RSA cybersecurity conference in San Francisco: following the example of the Geneva Convention of 1949, the State would create a similar document on cyber - a "Digital Geneva Convention on cyber space". The ob-

[11] For example, in some definitions, cyber has been defined only as an environment dedicated to communication. All the other characteristics of this sphere are completely absent (Singer, Friedman, 2014: 13).

jective is the creation of an international independent organization and the elaboration of common rules that would guarantee the protection of "civilians on the internet in times of peace" and the prevention of state-hacking (Volz, 2017). For the moment, the proposal has not produced results but it is destined to produce important effects in the future, considering the international approval that we have registered around this project.

These efforts towards the creation of international or European cyber norms have a key role considering that they could have a positive effect also for the process of elaboration of a general recognized definition of this security dimensions. Moreover, they can exercise also other positive effects in the general management of the cyber sphere. In fact, international norms could be effective for the creation of rules in the exchange of information and for the definition of a lawful behavior during wars and military actions.

Therefore, it is evident that the creation of a definition globally accepted and the international cooperation are strictly connected. Only the dialogue between the actors - including civilian and military entities – will allow the definition of general elements of cyber. Once this definition is created, a strong and efficient cooperation on the new security dimension will be created.

2. The importance of trust for cooperation and the difficulties in creating it

Organizational studies are more and more considering trust as a central element to create a strong cooperation, independently from the actors that are involved in this process (Mayer, Davis, 1995: 709). In fact, if trust is a fundamental condition for the success of a negotiation, its central role is particularly evident in all types of social interactions where people "depend on others in various ways to accomplish their personal and organizational goals" (Mayer, Davis, 1995: 710). In this context, we have also to include the cases of the creation of cooperative relations between different actors, such as the cooperation between military and civilian entities.

Only a mutual work can guarantee the success and the reach of common strategic goals, as underlined by economic and sociological theories on this subject. This factor is particularly true when the collaboration established by the entities is not constant, not frequent and unfamiliar, such as for the relations between large entities. In fact, in these cases, the reputation could not be helpful for the creation of a successful relationship: they ask for a particular effort of each actor in order to function in a good way. On the contrary, in the case of familiar relationship, this work is much easier because of a more frequent and constant exchange of views between all the individuals involved (LaPorta, Lopez, Shleifer, Vishny, 1997: 334-335).

Nevertheless, in all kind of relations, the level of trust is created on the results of the past performances experienced by the actors: only the common action can give basis for the future activities with the partners (LaPorta, Lopez, Shleifer, Vishny, 1997: 336-337). Moreover, also interpersonal relationships between the individuals exercise a special influence in cooperation. The level of trust between leaders or other people involved in the partnership have a particular impact on the effectiveness of the collaboration, whether it depends on cognitive elements or emotional basis (McAllister, 1995: 24-26).

Therefore, the creation of trust as basis of cooperation is complex and influenced by multiple factors. A trustful relationship requires a lot of time in order to be created: only great efforts in the contacts and a mutual understanding between the actors could guarantee to create strong basis for the collaboration.

This is the reason of the difficulties in the creation of completely new type of cooperation, such as in the case of the cyber ones: the absence of a previous form of collaboration requires particular efforts to the actors.

The best possibility they have is to refer to the trust at the base of their other security relations with the partner. Nevertheless, this work is not so easy.

Firstly, the absence of a global recognized definition of cyber can limit the cooperation if the actors are not able to identify common basis for their common action. In order to do that, the partners must surpass the confusion created by the authors regarding the main actions that must be considered when they are involved in the process (Mayer, Davis, 1995: 712-713).

Moreover, especially in the context of cyber cooperation, the creation of trust is more and more difficult because of the reluctance of entities in sharing security

information. This element is particularly true when the main actors are States: the share of classified information with others is considered as a sort of "loss of sovereignty" by the countries (Mayer, Davis, 1995: 709-711). In this way, they show absence of trust towards their partners, limiting also the coordination of the investigations and the collaboration between their intelligence systems (Terzi, 2015: 31).

This is the main limit in the security information sharing: the connection of dots would be possible only if the collaboration has its basis on trust, as for all the other types of relations in the security fields. "Members of a community want to know with whom they share data and whether the data will be handled appropriately" (ENISA, 2015: 47).

Differently from these cases, the civilian and military cooperation presents more problems than in other contexts: in the majority of cases, we are in the presence of a real new collaboration that has no basis or examples in the past, even in other fields. Therefore, the actors must create their relations starting from a zero point: there are no general guidelines on how create an efficient cooperation.

This limit becomes sometimes a real block. The difficulties in clarifying the relationship between the actors and the link between risk and trust do not help in finding solution to this problem. In fact, the authors have tried to understand if risk/common goal must be a pre-requisite of cooperation or not. The result has been a series of different or even opposite interpretations (Mayer, Davis, 1995: 709-711).

Therefore, in order to obtain positive results, actors must show the will to be trusted and to create a climate of confidence though regular dialogue. Informal meeting could help in this sense, especially if it involves a limited number of participants: small groups could have a better control on the channels of communication. Moreover, the identification of rules at the basis of cooperation could help in limiting the risk of absenteeism and promoting the success of the partnership (ENISA, 2015:47).

These are all elements that must be considered by civilian and military actors: once they decide to create a cyber cooperation, they will put in place an effective action only after having identified solutions to these main questions.

CONCLUSIONS

In national defense and security, the cooperation between civilian and military actors is central: a large collaboration between different entities could help in obtaining the best results possible. The European Union - especially thanks to its civilian missions - furnishes a great example in this sense. In fact, in these cases, the success of the operations is guarantee by the collaboration between armies and civil society: two actors that are considered in the same way thanks to the fact that their differences in nature are not taken into account (Röhrig, Smeaton, 2014: 26).

This reality is particularly true in a context such as the cyber one: a completely new dimension of security in which the actors have to develop new competences, measures and policies. Only an international collaboration could help in obtaining fast these objectives with limited costs and efforts: an efficient way to find measures for prevention, deterrence and response to possible attacks. This is the reason why constant official and unofficial dialogue, agreements, security information sharing, harmonization of rules, common researches and exercises have to be considered so fundamental in the management of the cyber technology.

The case of the military and civilian cooperation is not an exception in this sense. On the contrary, it would be considered the best type of collaboration for an efficient management of the cyber sphere. In fact, the different competencies between the entities guarantee to take into account all the particular aspects of the technology, obtaining a really complex way to response and prevent attacks. Especially the security information sharing and the creation of common exercises and researches on cyber security allow civilian and military actors to create their cooperation.

Nevertheless, since now, the attempts to create a collaboration between these type of entities are limited or completely absent. The different nature of the two actors have caused a block in the development of their relationships in the cyber field.

On the contrary, in the past, other type of cyber collaboration have been established, with more or less success, in order to try to create a real governance of the cyber sphere. It is really important to know these attempts because they could offer errors, problems and positive aspects to take into account for the future elaboration of the military and civilian collaboration.

Since the early days of use of internet, especially engineers and researchers have tried to elaborate standard rules that could help in the day-by-day management of the net. One of the main results of these efforts has been the creation of a new organization: the "Internet Engineering Task Force" (IETF). Through the work of thematic groups composed by researchers, engineers, firms, private actors, IETF tries to elaborate or modify standards and protocols of the World Wide Web (Singer, Friedman, 2014: 29).

Some years later, in 1998, another attempt in this direction was the creation of the Internet Corporation for Assigned Names and Numbers (ICANN): an entity composed by regional authorities of the five continents. This organization was supposed to be the first step towards an international cooperation. Even if ICANN exists also today, its inability to act in a neutral way makes it unable to operate. In fact, every member tries to represents its interests, preventing from the possibility to indicate common measures to govern the cyber sphere (Terzi, 2015: 21).

In addition to these technical and civilian attempts, also States, international organizations and actors has tried to promote in other ways the cooperation on the cyber sector but the results are limited or inadequate. A first example is the Cyber Stability Board: an international arrangement elaborated on the example of the Financial Stability Board and composed United States, Canada, New Zeeland, France, Germany, Great Britain, Australia, Korea and Japan. Even if this organism has shown the will to find a collaboration, for the moment its discussions have had no practical effects (Kramer, Teplinski, 2013: 9). Even China and Russia had tried to elaborate a common proposal that was addressed to the United Nations on January 2015: an international code of conduct. Supported also by Tajikistan, Kazakhstan, Uzbekistan and Kyrgyzstan, the text suggested the idea of the creation of international cooperation in order to "in addressing common threats and challenges in the information space, in order to establish an information environment that is peaceful, secure, open" (United Nations General Assembly, 2015: 4). Nevertheless, this initiative was opposed by the European Union because of the absence of protection for human rights (Pawlak, 2017: 2).

More recently, the question of the international cyber cooperation has been discussed during the G7

of Ministers of Foreign Affairs, which took place in Lucca (Italy) in April 2017. During the meeting, the ministers approved the "Declaration of Responsible States behavior in Cyberspace": an attempt to develop and implement common measures for cooperation on exchange of information, stability and security of ICTs based on the objective indicated by the United Nations. Nevertheless, the no-binding nature of the document is the main limit of this declaration (Paganini, 2017). Anyway, this Declaration was not the most recent attempt of creating international cyber cooperation. In fact, in May 2017, a series of states[12] signed a Project Arrangement for "Cyber Defence Pooling and Sharing", based on a project proposed by the European Defence Agency (EDA).

From this list of efforts, the absence of a common action between civilian and military is evident. More generally, also between private and public entities, the efforts have always been divided the ones from the others. In fact, each actor has preferred to collaborate only with partners of the same nature.

In the last years, the increase in the number of cyber-attacks towards private and public entities has put in evidence more than ever these limits in the management of the new security dimension. Only a complete and comprehensive vision of the cyber will help in identifying all its characteristics and consequently elaborate forms of prevention, deterrence and response to attacks. Nevertheless, this action is not possible without collaboration: the only way to put together different experiences, visions and point of views in this field.

Civilian and military actors have to be aware of their key role in this sense in order to start a real cooperation that will prevent the system from new big crisis in the future.

[12] These states are: Austria, Belgium, Germany, Estonia, Greece, Finland, Ireland, Latvia, the Netherlands, Portugal and Sweden (EDA website, https://www.eda.europa.eu/info-hub/press-centre/latest-news/2017/05/12/cyber-ranges-eda-s-first-ever-cyber-defence-pooling-sharing-project-launched-by-11-member-states?utm_source=EDA+e-newsletter&utm_medium=newsletter&utm_campaign=18052017+part1)

REFERENCES

- BAYUK J. L., HEALEY J., ROHMEYER P., SACHS M. H., SCHMIDT J., WEISS J. (2012), *Cyber Security Policy Guidebook*, Hoboken: John Wiley & Sons
- BOEKE LL.M. S., HEINL C.H., VEENENDAAL M.A. (2015), *Civil-Military Relations and International Military Cooperation in Cyber Security: Common Challenges & State Practices Across Asia and Europe*, 2015 7th International Conference in Cyber Conflict, Tallinn: NATO CCD COE Publications, pp. 69-80, https://ccdcoe.org/cycon/2015/proceedings/05_boeke_heinl_veenendaal.pdf
- CHRISTOU G. (2016), *Cybersecurity in the European Union. Resilience and adaptability in Governance Policy*, London: Macmillan Publisher
- CUKIER K.N., MAYER-SCHÖENBERGER V. (2013), *The rise of the big data. How it's changing the way we think about the world*, Foreign Affairs, https://www.foreignaffairs.com/articles/2013-04-03/rise-big-data
- DAS T. K., TENG B.-S. (1999), *Between trust and control: developing confidence in partner cooperation in alliances*, Academy of Management Review, vol. 23, n. 3, pp. 491-512
- DEMCHAK C., DOMBROWSKI P. (2014), *Cyber Westphalia: Asserting State Prerogatives in Cyberspace,* Georgetown Journal of International Affairs, pp. 29-37
- DRENT M., K. HOMAN AND D. ZANDEE (2013), *Civil-military capacities for European Security*, The Hague: Clingendael Report, December 2013
- EUROPEAN NETWORK AND INFORMATION SECURITY AGENCY-ENISA (2012), *National cyber Security Strategies. Practical Guide on Development and Execution*, https://www.enisa.europa.eu/publications/national-cyber-security-strategies-an-implementation-guide
- EUROPEAN NETWORK AND INFORMATION SECURITY AGENCY-ENISA (2015), *Cyber Security Information Sharing: An Overview of Regulatory and Non-regulatory Approaches,* Final version 1.0, Public, https://www.enisa.europa.eu/publications/cybersecurity-information-sharing/at_download/fullReport
- EUROPEAN PARLIAMENT (2015), *Cybersecurity in the European Union and beyond: exploring the threats and policy responses*, Directorate-General for international policies-citizens' rights and constitutional affairs, Study for the LIBE Committee, http://www.europarl.europa.eu/RegData/etudes/STUD/2015/536470/IPOL_STU(2015)536470_EN.pdf
- HARE F. (2009), *Borders in cyberspace: adapt to the challenges of cyber security?*, In Czosseck C, Geers K, "The Virtual Battlefield: Perspectives on Cyber Warfare" In Tallinn: Cryptology and Information Security Series, http://www.ccdcoe.org/publications/virtualbattlefield/06_HARE_Borders%20in%20Cyberspace.pdf
- JIMÉNEZ A. G., ORENES P. B., PUENTE S. N. (2010), *An approach to the Concept of a Virtual Border: Identities and Communication Spaces,* Revista Latina de comunicación social, art. 2, pp. 214-221, http://www.revistalatinacs.org/10/art2/894_Madrid/RLCS_art894EN.pdf
- KRAMER F.D., TEPLINSKI M. J. (2013), *Cybersecurity and Tailored Deterrence*, Washington: Atlantic Council
- KREMER J.F., MULLER B. (2014), *Cyberspace and International Relations: theory, prospects and challenges*, London: Springer
- LA PORTA R., LOPEZ-DE-SILANES F., SHLEIFER A., VISHNY R. W. (1997), *Trust in large Organizations*, American Economic Review Papers and Proceedings, vol. 87, n. 2, pp. 333-338
- LYON D. (2014), *Surveillance, Snowden, and Bid Data: Capacities, consequences, critique*, Big Data & Society, pp. 13
- MAYER R. C., DAVIS J. H. (1995), *An integrative model of organizational trust*, Academy of Management Review, vol. 20, n. 3, pp. 709-734
- MCALLISTER D. (1995), Affect- and cognition - based trust as foundations for interpersonal cooperation in organizations, Academy of Management Journal, vol. 38, n. 1, 24-59
- PAGANINI P. (2017), *G7 Declaration on Responsible States Behavior in Cyberspace*, Security Affairs, http://securityaffairs.co/wordpress/57932/cyber-warfare-2/g7-declaration-responsible-states-behavior-cyberspace.html
- PAWLAK P. (2017), *Cyber security woes: WannaCry?*, EU Institute for Security Studies, Alert n°13, http://www.iss.europa.eu/publications/detail/article/cyber-security-woes-wannacry/
- PERKOVICH G., LEVITE A. E. (2017), *Understandng cyber conflict: 14 Analogies,* Georgetown University Press

- POLLOCK R. (2013), *Forget big data, small data is the real revolution*, The Guardian, 25.04.2013, https://www.theguardian.com/news/datablog/2013/apr/25/forget-big-data-small-data-revolution
- PONEMON INSTITUTE (2016), *2016 Cost of Cyber Crime Study & the Risk of Business Innovation*, pp. 36, https://www.ponemon.org/local/upload/file/2016%20HPE%20CCC%20GLOBAL%20REPORT%20FINAL%203.pdf
- PONEMON INSTITUTE (2017), *2017 Cost of Cyber Crime Study: insights on the security investments that make a difference*, pp. 55, https://www.accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf
- RÖHRIG W., SMEATON R., *Cyber Security and Cyber Defence in the European Union. Opportunities, synergies and challenges*, European Defence Agency- Cybersecurity review.com, Summer 2014, pp. 23-27
- SARMA S. (2016), Cyber Security Mechanism in European Union, Indian Council of World Affairs: Viewpoint
- SINGER P.W., FRIEDMAN A. (2014), *Cybersecurity and cyberwar. What everyone needs to know*, New York: Oxford University Press
- TADDEO M., GLORIOSO L. (2017), *Ethics and policies for cyber operations: a NATO cooperative cyber defence centre of excellence initiative*, Philosophical Studies Series, Volume 124
- TERZI G. (2015), *Sfida cybernetica: la quinta dimensione della sicurezza*, Rivista di Studi Politici Internazionali, Year 82, Dossier 325, pp. 11-31
- UNITED NATIONS GENERAL ASSEMBLY (2015), *Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General*, https://ccdcoe.org/sites/default/files/documents/UN-150113-CodeOfConduct.pdf
- VOLZ D. (2017), *'Digital Geneva Convention' needed to deter nation-state hacking: Microsoft president*, Reuters, http://www.reuters.com/article/us-microsoft-cyber-idUSKBN15T26V

Created in 1953, the Finabel committee is the oldest military organisation for cooperation between European Armies: it was conceived as a forum for reflections, exchange studies, and proposals on common interest topics for the future of its members. Finabel, the only organisation at this level, strives at:

- Promoting interoperability and cooperation of armies, while seeking to bring together concepts, doctrines and procedures;
- Contributing to a common European understanding of land defence issues. Finabel focuses on doctrines, trainings, and the joint environment.

Finabel aims to be a multinational-, independent-, and apolitical actor for the European Armies of the EU Member States. The Finabel informal forum is based on consensus and equality of member states. Finabel favours fruitful contact among member states' officers and Chiefs of Staff in a spirit of open and mutual understanding via annual meetings.

Finabel contributes to reinforce interoperability among its member states in the framework of the North Atlantic Treaty Organisation (NATO), the EU, and ad hoc coalition; Finabel neither competes nor duplicates NATO or EU military structures but contributes to these organisations in its unique way. Initially focused on cooperation in armament's programmes, Finabel quickly shifted to the harmonisation of land doctrines. Consequently, before hoping to reach a shared capability approach and common equipment, a shared vision of force-engagement on the terrain should be obtained.

In the current setting, Finabel allows its member states to form Expert Task Groups for situations that require short-term solutions. In addition, Finabel is also a think tank that elaborates on current events concerning the operations of the land forces and provides comments by creating "Food for Thought papers" to address the topics. Finabel studies and Food for Thoughts are recommendations freely applied by its member, whose aim is to facilitate interoperability and improve the daily tasks of preparation, training, exercises, and engagement.

FINABEL
Quartier Reine Elisabeth
Rue d'Evere 1
B-1140 BRUSSELS

Tel: +32 (0)2 441 79 38
GSM: +32 (0)483 712 193
E-mail: info@finabel.org

You will find our studies at
www.finabel.org

Responsible publisher: Mario BLOKKEN - Finabel Permanent Secretariat - QRE - Rue d'Evere,1 - B-1140 Brussels - +32 (0)2 441 79 38