Università
Ca'Foscari
Venezia

Ca' Foscari
Dorsoduro 3246
30123 Venezia

Master's Degree programme – Second Cycle
(*D.M. 270/2004*)
In Relazioni Internazionali Comparate-
International Relations

Final Thesis

Information and Communication Technology (ICT) and cyber threats: the main fields of analysis

Supervisor
Ch. Prof. Stefano Soriani

Co-supervisor
Ch. Prof. Antonio Trampus

Graduand
Flavia Quaglia
Matriculation Number 831898

Academic Year
2014/ 2015

CONTENTS

CHAPTER THREE: CYBERSECURITY IN THE EUROPEAN UNION

CHAPTER FOUR: ITALY AND CYBERSECURITY

SINTESI

La diffusione delle tecnologie dell'informazione e della comunicazione, che iniziò negli anni novanta e prese il nome di information revolution, portò dei grandi cambiamenti a livello sociale, economico e culturale nel mondo. Grazie all'invenzione di Internet, dei computer e di tutti gli altri sistemi di comunicazione che si sono poi sviluppati e sono diventati sempre più all'avanguardia, la comunicazione tra le persone è divenuta molto più veloce, superando quindi le barriere temporali ma anche quelle spaziali, permettendo una condivisione di informazioni e di idee anche a distanza di migliaia di chilometri ma fornendo anche la possibilità di attuare dei pagamenti via web, quindi scambi di denaro o prenotazioni di visite mediche o di viaggi, evitando le lunghe attese e gli alti costi. Questo è stato uno dei cambiamenti più importanti prodotto dallo sviluppo delle tecnologie dell'informazione e della comunicazione, ma non è stato l'unico. Dalla scuola al settore sanitario, finanziario, economico, dei trasporti, e così via, tutti i settori della società hanno cominciato a funzionare sulla base di sistemi di informazione e comunicazione.

Si può quindi dire che da quando, con l'information revolution, Internet, il computer e il network hanno invaso e pervaso i nostri modi di vivere, agire, comunicare, sono aumentati la crescita e la competitività degli stati che divenivano sempre più all'avanguardia e i cui servizi erano sempre più digitalizzati.

Tuttavia, ed è quello che cercherò di dimostrare attraverso i quattro capitoli in cui è organizzata la mia tesi, l'information revolution è stata importante non solo per i benefici e le conseguenze positive che ne sono derivate ma anche per quelle meno positive. Infatti, le tecnologie dell'informazione e della comunicazione rappresentano una vera e propria fonte di minacce alla nostra società. Ciò potrebbe sembrare strano alla luce di quanto sopra detto. Invece è proprio dallo spazio cibernetico o cyberspace, dimensione composta da Internet, computer, cavi, satelliti, hardware e software in cui avviene la comunicazione, che derivano le cosiddette minacce cibernetiche o cyber threats.

Il dominio digitale da cui noi stessi e le società in generale dipendono sempre più emerge essere allo stesso tempo una dimensione così minacciosa da essere considerata un dominio di guerra, più nello specifico, il quinto dominio di guerra dopo i tradizionali

acqua, aria, terra e spazio. Ciò significa che la diffusione delle tecnologie dell'informazione e della comunicazione ha modificato la natura dei conflitti che non sono più tradizionalmente combattuti su un terreno di guerra per mezzo di armi convenzionali, violenza fisica, causando spargimento di sangue e morti ma sono dei conflitti che hanno luogo in una dimensione digitale in cui non ci sono barriere né temporali né spaziali e vengono combattuti per mezzo di strumenti non convenzionali che gli hacker utilizzano con lo scopo di danneggiare o distruggere i sistemi di informazione e comunicazione dell'avversario, cercando di proteggere i propri, senza utilizzare la violenza fisica e provocare morti.

Di conseguenza è emerso il termine cyber war per indicare, in generale, qualsiasi tipo di conflitto con una componente cibernetica. In questo nuovo modo di fare la guerra è il dominio delle informazioni o information dominance la chiave vincente per raggiungere il successo. Emerge quindi come l'informazione risulti essere una fonte strategica di potere molto desiderata a livello internazionale dagli stati con lo scopo di vincere un conflitto.

Un'altra dimostrazione dell'importanza della diffusione delle tecnologie dell'informazione e della comunicazione è che sostanzialmente il concetto tradizionale di sicurezza ha subito un cambiamento. Più nello specifico, per far fronte al nuovo tipo di minacce che, come ho precedentemente detto, derivano da una dimensione digitale, lo stato ha di conseguenza dovuto modificare le proprie strategie di risposta nel garantire la sicurezza ai propri cittadini. Quindi per lo stato garantire la sicurezza non significa più elaborare strategie per la difesa dei confini geografici da tradizionali attacchi sferrati da paesi avversari per mezzo di armi convenzionali ma consiste nell'elaborare strategie volte a proteggere il nuovo dominio di guerra che è il cyberspace. Ecco che emerge un nuovo concetto di sicurezza, la cosiddetta sicurezza cibernetica o cybersecurity, che sfida il tradizionale concetto di sicurezza.

Inoltre, anche l'idea che lo stato come attore unitario debba occuparsi di proteggere i propri cittadini e le proprie strutture dalle minacce è stata modificata nel senso che più attori, e quindi l'intera società, sono responsabili della gestione della minaccia cibernetica. Quindi fare sistema diventa di fondamentale importanza nel nuovo contesto cibernetico, tanto da far emergere il concetto di sicurezza partecipata per andare proprio a sottolineare la necessità di cooperare e comunicare tra i diversi attori nella società. La

cooperazione a livello nazionale, il dialogo, la partnership tra organismi pubblici e il settore privato, le collaborazioni con università e centri di ricerca ma anche la cooperazione a livello internazionale tra stati e tra questi e organizzazioni internazionali diventano elementi cruciali per garantire la sicurezza cibernetica.

Nel primo capitolo della mia tesi cercherò di fornire al lettore una visione d'insieme riguardo la tematica del cyber, così recente e ancora poco conosciuta dalla maggior parte delle persone, in modo tale da fare chiarezza su alcune tematiche e passare poi a una fase successiva un po' più complessa. In una prima parte introduttiva viene fatto riferimento all'importanza delle informazioni nell'era attuale, chiamata infatti era dell'informazione o Information age, per poi passare alla descrizione del cyberspace e delle sue caratteristiche, fornendo diverse definizioni dello stesso e descrivendo quali tipi di attacchi possono avere luogo in questo dominio, fino a definire il suddetto un dominio di guerra. Viene quindi fatto riferimento a come la natura dei conflitti sia cambiata, a come abbiano perso la loro naturale simmetria per divenire sempre più asimmetrici. Infine viene sottolineata l'importanza dell'intelligence come strumento utilizzato dagli stati per raccogliere informazioni importanti per garantire la sicurezza dei cittadini che viene messa in pericolo dalla minaccia cibernetica, descrivendo il sistema di intelligence italiano e il mercato di sicurezza cibernetica che si è creato in Italia.

Successivamente, dopo questa prima parte introduttiva, viene trattata la tematica della sempre maggiore dipendenza delle società dal cyberspace e quindi l'aumentata vulnerabilità dei moderni sistemi di informazione e comunicazione alla minaccia cibernetica, sottolineando che la conseguenza più diretta di questa vulnerabilità è la cyber war. Questa vulnerabilità è dovuta a delle vulnerabilità tecniche intrinseche nei sistemi di informazione e comunicazione, perciò l'unica soluzione possibile per evitare la cyber war sarebbe quella di creare dei sistemi più sicuri in partenza. Si passerà dunque ad un'analisi della tematica della cyber war che risulterà essere una questione abbastanza complessa e in continua evoluzione, riguardo il cui status ci sono opinioni contrastanti di diversi studiosi e non c'è un'unica definizione della suddetta che possa accomunare tutti.

Viene comunque dedicato un paragrafo al legame tra la cyber war e il concetto di letalità, dimostrando come un attacco cibernetico possa costituire un atto di guerra

anche in assenza di morte e quindi la cyber war possa avere luogo, smentendo gli studiosi che, come Thomas Rid, ritengono che la cyber non sia mai avvenuta e mai avverrà poichè è assente l'elemento della letalità, elemento necessario per poter parlare di guerra. In seguito, un altro paragrafo è dedicato ancora agli attacchi cibernetici ma questa volta al loro legame con la Just War Tradition (JWT) per dimostrare in presenza di quali condizioni un attacco cibernetico possa fornire al paese attaccato una giusta causa per rispondere utilizzando la violenza militare. Gli attacchi verranno suddivisi in tre categorie (una composta da quelli che rappresentano, per il paese attaccato, una giusta causa per rispondere con la violenza, una composta da quelli che non rappresentano una giusta causa e una composta da casi ambigui) che verranno poi analizzate in maniera dettagliata.

Poi, viene riportato l'esempio di due grandi e potenti paesi come la Cina e gli Stati Uniti i quali, a partire dall'introduzione delle tecnologie dell'informazione e della comunicazione negli anni novanta, sono legati a livello diplomatico anche sul fronte della sicurezza cibernetica. A questo proposito infatti, dopo una descrizione di come si sono evoluti i loro rapporti diplomatici a partire dagli anni settanta, verrà descritto come sono cambiati a seguito dell'information revolution. La questione della cybersecurity è divenuta un elemento cruciale di discussione durante i diversi incontri che si sono succeduti tra i presidenti dei due paesi i quali tuttavia non hanno la stessa visione riguardo il cyberspace, come regolarlo e riguardo la governance di Internet. Più nello specifico, in un incontro avvenuto tra i presidenti Obama e Jinping nel 2013 in California, la tematica della cybersecurity è stata centrale nella discussione, dato che entrambi i paesi si accusarono di spionaggio cibernetico o cyber espionage.

Infine viene fatto riferimento alla sicurezza nazionale che viene messa sempre più in pericolo dalle minacce non tradizionali in un mondo globalizzato sempre più interdipendente ma che allo stesso tempo è anche ricco di incertezze e insicurezze. Considerando il fatto che risulta impossibile raggiungere un livello di sicurezza assoluta ma che un minimo di rischio rimane, risulta necessario per gli stati modificare le proprie strategie di risposta di fronte alle nuove minacce includendo l'elemento della resilienza, la quale permette di gestire e ridurre, se non si può eliminare, il rischio delle minacce, permettendo quindi ai sistemi attaccati di funzionare anche sotto attacco per poi tornare a livelli di operatività standard.

Tutte queste considerazioni si possono dunque applicare anche al contesto cibernetico e della cybersecurity, all'interno dei quali la resilienza diventa resilienza cibernetica o cyber resilience. Quest'ultima permette ai sistemi di informazione e comunicazione, che sono i target degli attacchi cibernetici, di poter funzionare ad un regime minimo anche sotto attacco e quindi assicurare un continuo e buon funzionamento della società dato che questa, come precedentemente detto, basa il suo funzionamento proprio su sistemi di informazione e comunicazione tecnologici. La cooperazione e lo scambio di informazioni a livello nazionale e internazionale tra diversi attori risultano essere elementi fondamentali per il raggiungimento della cyber resilience.

Dopo questo primo capitolo teorico, segue un secondo capitolo dedicato alla descrizione di attacchi cibernetici avvenuti con modalità diverse, ricordando i più famosi nella storia ma anche i più recenti e meno conosciuti, in modo tale da dare più concretezza a quanto detto nel primo capitolo e quindi dimostrare quanto la minaccia cibernetica sia così reale e vicino a noi.

Tra gli attacchi cibernetici compiuti attraverso il cyberspace con lo scopo di colpire oggetti fisici nel mondo reale viene ricordato il famoso attacco Stuxnet lanciato da Stati Uniti e Israele contro una centrale nucleare iraniana nel 2009 con lo scopo di bloccare la produzione di uranio. Questo attacco prende il nome dal verme informatico o worm che è stato inserito all'interno dei sistemi di controllo dei processi industriali della centrale nucleare iraniana e, approfittando delle vulnerabilità qui presenti, ha causato un danneggiamento della produzione di uranio. Contemporaneamente a questo attacco, gli Stati Uniti ne sferravano un altro contro la centrale di produzione di armi nucleari nella Corea del Nord, tramite l'utilizzo dello stesso tipo di worm utilizzato per l'attacco contro l'Iran ma non andando a buon fine in Corea. Due anni prima, nel 2007, l'Israele attaccò una centrale nucleare siriana sabotando il sistema di difesa aereo siriano che non riconobbe un aereo da guerra israeliano che riuscì a sorvolare la centrale rilasciando una bomba che la fece esplodere.

In seguito vengono riportati esempi di attacchi cibernetici compiuti attraverso il cyberspace con lo scopo di interrompere il buon funzionamento della rete informatica del paese avversario. Tra questi vengono ricordati il primo attacco cibernetico contro una rete moderna e cioè l'attacco sferrato dalla Russia contro i siti web dell'Estonia nel 2007 causando un mal funzionamento della rete, chiamato appunto denial of service. Un

attacco simile venne lanciato ancora dalla Russia l'anno seguente contro i siti web della Georgia, provocando ancora un malfunzionamento di questi. Successivamente nel 2012 il cyberspace ha rappresentato un terreno di scontri anche tra Arabia e Israele, i quali si sono attaccati reciprocamente andando a colpire i siti web dei rispettivi governi e banche.

Più recentemente sono avvenute delle intrusioni cibernetiche negli importantissimi siti web del Pentagono e della Casa Bianca con lo scopo di compromettere dati e informazioni personali. In particolare nel 2014 la Cina ha sferrato un attacco contro il sito web dell'Ufficio di gestione del personale della Casa Bianca, compromettendo le informazioni personali di 4 milioni di impiegati grazie alle credenziali di accesso che gli hacker cinesi erano riusciti ad ottenere per poi accedere al sistema informatico della Casa Bianca. L'anno successivo gli hacker russi sono riusciti a penetrare nei sistemi informatici del Pentagono e della Casa Bianca accedendo a informazioni private del presidente Barack Obama e del personale tramite l'invio di una mail che una volta aperta forniva automaticamente agli hacker le credenziali di accesso al sistema informatico.

Un riferimento viene poi fatto agli attacchi cibernetici sferrati dal noto gruppo hacktivista Anonymous che nel 2012 attaccò i siti web israeliani con lo scopo di interrompere il loro funzionamento come forma di protesta in risposta al cattivo comportamento israeliano nei confronti dei palestinesi della striscia di Gaza e il più recente attacco lanciato nel 2015 contro i siti web del governo canadese per protestare contro l'approvazione di una legge anti-terrorismo.

Infine vengono riportati degli esempi di terrorismo cibernetico, ricordando l'attacco compiuto nel 2015 da un gruppo chiamato Lizard-Squad, che sembrerebbe essere collegato all'ISIS, contro i siti della compagnia aerea Malaysia airlines, causandone un malfunzionamento temporaneo e l'attacco compiuto nello stesso anno dal gruppo Islamic State Hacking Division contro i siti web del governo statunitense con lo scopo di compromettere dati del personale.

Negli ultimi due capitoli viene affrontato il tema della cybersecurity a livello europeo e italiano. In particolare, nel terzo capitolo viene fornita al lettore una descrizione dell'approccio legislativo alla tematica della sicurezza cibernetica a partire dal 2000 fino ad arrivare al 2013, anno in cui l'Unione Europea (UE) presentò la propria strategia

di cybersecurity. Un primo focus viene fatto appunto su questa strategia il cui obiettivo è quello di assicurare un cyberspace aperto, in cui le persone possano liberamente muoversi usufruendo dei servizi offerti dalla rete e comunicare in maniera sicura. Vengono poi descritte le tre sezioni in cui è organizzata la strategia.

Nella prima parte viene fatto riferimento a come le moderne società siano sempre più dipendenti da Internet e dal cyberspace e quindi allo stesso tempo sempre più vulnerabili agli attacchi cibernetici. Inoltre viene sottolineata la necessità di applicare nel dominio digitale le stesse norme e regole che si applicano nel mondo reale e cioè i diritti fondamentali, la democrazia e lo stato di diritto per raggiungere la sicurezza cibernetica.

Nella seconda parte vengono analizzate le cinque priorità strategiche che l'UE deve adottare per garantire un cyberspace libero e sicuro. Queste consistono in: raggiungere la resilienza cibernetica, ridurre il crimine cibernetico, sviluppare capacità e politiche di difesa cibernetica, sviluppare risorse industriali e tecnologiche per la cybersecurity, stabilire un politica del cyberspace internazionale.

Nella terza parte della strategia vengono descritti i ruoli e le responsabilità dei diversi attori che a livello nazionale, europeo e internazionale sono coinvolti nell'ambito della sicurezza cibernetica.

Dopo questa dettagliata descrizione della strategia europea vengono descritti i principali documenti, leggi, direttive, comunicazioni prodotte e strutture e organismi coinvolti nella questione della cybersecurity a livello europeo a partire dal 2000. Fin dall'inizio la Commissione europea emerge come uno degli organismi più importanti che svolge un ruolo cruciale nella produzione di leggi e direttive in ambito di sicurezza cibernetica. Un'altra struttura molto importante in questo ambito è l'Agenzia europea per la sicurezza delle reti e dell'informazione o ENISA (European Network and Information Security Agency), fondata nel 2004 a Creta con il compito di garantire un alto livello di sicurezza delle reti e delle informazioni all'interno dell' UE, fornendo inoltre consigli e assistenza alle istituzioni europee e agli stati membri per prevenire e reagire a problemi di sicurezza cibernetica.

Tra le importanti iniziative intraprese dall'Agenzia viene ricordata l'organizzazione degli esercizi di crisi cibernetica a livello europeo che consistono nel simulare attacchi cibernetici e hanno lo scopo di rafforzare la cooperazione tra gli stati membri

dell'Unione in caso di conflitto. Un'altra importante iniziativa elaborata dall'Agenzia è stata la pubblicazione di un manuale guida nel 2012 dedicato ai diversi stakeholder pubblici e privati in cui vengono raccolte tutte le raccomandazioni per un corretto sviluppo e una corretta realizzazione delle strategie di sicurezza cibernetica.

Infine viene affrontata la tematica della protezione delle infrastrutture critiche che sono tutte quelle infrastrutture essenziali per il funzionamento di una società e quindi la fornitura di acqua, gas, energia, i trasporti la cui distruzione avrebbe un impatto molto significativo sul benessere di una nazione. Vengono quindi descritte le varie iniziative e leggi elaborate dalla Commissione in questo ambito che, insieme alla lotta al crimine informatico, rappresenta una priorità per l'Unione in ambito di sicurezza cibernetica.

Infine nel quarto capitolo viene fornita una panoramica delle principali leggi e dei principali organismi coinvolti nell'ambito della cybersecurity a partire dagli anni novanta quando l'Italia cominciò ad interessarsi di crimine cibernetico o cyber crime fino ai più recenti sviluppi del 2016 in materia di cybersecurity.

Una prima parte del capitolo viene dedicata all'analisi del decreto "Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale" elaborato nel gennaio del 2013 dal Presidente del Consiglio in cui, attraverso undici articoli, viene definita l'architettura istituzionale responsabile della sicurezza cibernetica, descrivendo i compiti e le responsabilità dei diversi attori coinvolti, tra i quali il Presidente del Consiglio risulta essere in cima alla piramide, ma vengono anche descritti i meccanismi e le procedure da seguire per prevenire i rischi, ridurre le vulnerabilità e rispondere adeguatamente agli attacchi cibernetici. Il suddetto decreto stabilisce inoltre la creazione del Quadro strategico Nazionale di cybersecurity e il Piano Nazionale di cybersecurity che insieme rappresentano la strategia italiana di sicurezza cibernetica pubblicata nel 2014.

Alla descrizione del suddetto decreto segue quindi la descrizione del Quadro e del Piano che insieme hanno lo scopo di rafforzare la preparazione nazionale nel rispondere alle minacce cibernetiche e sottolineano l'importanza di adottare soluzioni comuni nel campo della sicurezza cibernetica. Il Quadro, composto di due capitoli e due annessi, fornisce una descrizione della natura e della tendenza evolutiva della minaccia cibernetica e stabilisce 6 linee guida strategiche e 11 operative da seguire in modo da rafforzare le capacità di difesa nazionali nell'ambito della cybersecurity. Il Piano ha lo

scopo di dare una piena realizzazione al Quadro descrivendo quindi linee d'azione e obiettivi da seguire.

Successivamente alla descrizione del Quadro e del Piano nazionale vengono analizzate le principali leggi, documenti, decreti prodotti e i principali organismi e strutture coinvolti nella cybersecurity a partire dagli anni novanta quando l'Italia cominciò ad interessarsi al cyber crime che, insieme alla protezione delle infrastrutture critiche, rappresenta una priorità in ambito di sicurezza cibernetica a livello nazionale così come a livello europeo. Tra i più recenti sviluppi viene ricordata: la direttiva pubblicata nell'agosto del 2015 dal Presidente del Consiglio Matteo Renzi recante linee guida per un cyberspace sicuro; la legge di stabilità approvata nel dicembre 2015 in cui, tra le importanti novità a livello finanziario, viene annunciata la decisione di dedicare 150 milioni alla sicurezza cibernetica soprattutto dopo gli attentati di Parigi e infine la nomina avvenuta all'inizio del 2016 di Marco Carrai, amico del Presidente del Consiglio, come consulente tecnico presso il nucleo di sicurezza cibernetica a Palazzo Chigi, destando numerose polemiche.

Per concludere, attraverso il mio lavoro di tesi ho cercato non solo di fare chiarezza su un argomento ancora poco conosciuto dalla maggioranza delle persone e quindi aiutare un lettore disorientato a trovare la giusta via nel complicato, rischioso, minaccioso, recente e in continua evoluzione mondo del cyber ma ho anche tentato di rendere più consapevoli i lettori del fatto che la minaccia cibernetica esiste ed è molto vicina a noi perciò, essere a conoscenza di questa realtà, aiuterebbe gli web users a difendersi meglio dalla cyber threat. L'introduzione delle tecnologie dell'informazione e della comunicazione ha segnato un passo importante nella storia, ma ha anche creato un mondo ricco di incertezze e insicurezze provocate dalla minaccia cibernetica alla quale risulta difficile rispondere in maniera adeguata essendo una realtà in continua evoluzione. Sviluppare strategie di sicurezza cibernetica è diventata una necessità per gli stati che devono difendersi dal nuovo tipo di minaccia ma ciò su cui si deve puntare maggiormente è la cooperazione e il dialogo a livello nazionale tra diversi attori pubblici e privati e a livello internazionale tra stati e organizzazioni internazionali, oltre ad investire ulteriormente nel settore della cybersecurity.

Tuttavia, i recenti attacchi terroristici compiuti dall'ISIS in diverse parti del mondo, seppur pianificati attraverso l'utilizzo del web da parte degli attentatori, fanno pensare

che la guerra tradizionale, il sangue, la violenza, la morte, non siano oggi realtà poi così lontane da noi.

INTRODUCTION

The goal of my thesis is to demonstrate the importance of Information and Communication Technology (ICT)[1] in the Twenty-First Century through an analysis of different areas of interest linked to the ICT topic.

A demonstration of the importance of ICT is the fact that modern societies are increasing dependent on computers, the Internet and other technological tools for the communication, basing their functioning on them. Many or almost all sectors of societies, from the health-care sector to schools, means of transport, finance, governments, economy, work on the basis of Information Technology (IT) systems. In addition, thanks to ICT people can communicate at great distances in a few time, they can make on-line payments or book a trip or a medical exam, reducing time and costs. Therefore, a positive consequence of the evolution and spread of ICT is that it favors the growth and competitiveness of nations, making them more and more digitalized.

However, a negative consequence of the development of ICT is the fact that modern societies are menaced by new threats, called cyber threats, as they stem from the cyberspace. The latter, which is a digital domain composed of the Internet, computers, software, hardware and ICT networks[2], becomes the new realm of war. This means that ICT is relevant as it has changed the nature of conflicts which are no longer fought on the traditional battlefield by means of conventional weapons, violence and physical force. New conflicts are fought in an unconventional domain, where no borders exist, by means of hackers who use computer networks and technologies in order to hit anonymously the information and communication system of the adversary nation. It is on the basis of the information dominance[3] that the success in the new way of making war depends.

From a security perspective, the relevance of ICT emerges in the sense that, being it a source of cyber threats, it makes states change their strategy of response in order to

[1] The term "Information and communication technology" refers to communication tools such as computer, television, radio, etc. and services and application linked to them.

[2] Collins A., *Contemporary security studies*, third edition, oxford university press, 2013, pp. 363;415

[3] The information dominance consists in the ability of damaging the information and communication systems of the adversary trying to collect as much information as possible about it and, at the same time, protecting one's own information systems. It means that information is at the core of information warfare, which is the new type of war that derives from the spread of ICT.

provide security to their citizens and protect them and the society in general form cyber attacks. It means that strategies are no longer focused on the protection of geographical borders but, since threats come from the cyberspace, on the protection of the digital domain, giving life to the concept of cybersecurity. In addition, the provision of security is no longer a task of the state as single actor but the international cooperation between states and between them and international organizations, the partnership between public and private actors but also the dialogue with universities are crucial in the security field.

In order to achieve the goal just described, which is that of demonstrating the importance of ICT, my thesis is organized in four chapters.

In the first chapter an overview of the cyber topic is given. After an introductory section focused on the central role that information has achieved in international relations[4], becoming also a source of power for states in order to win a conflict, a focus on the cyberspace is made, providing a definition of it according to the International Telecommunication Union[5], followed by a description of the crucial characteristics of the digital domain and of the cyber attacks that could stem from it. As a consequence, the topic of the vulnerability of modern societies to cyber attacks caused by their increasing dependence on the Internet is considered, together with the idea that IT systems possess some technical vulnerabilities which, if not solved, will lead societies toward the cyber war. As regards the cyber war topic, a section is dedicated to the analysis of its relationship with lethality in order to understand if a cyber attack could constitute an act of war therefore if a cyber war could take place. In addition, a reflection on the link between cyber attacks and the Just War Tradition (JWT)[6] is made so as to describe when a cyber attack could provide the attacked country with a just cause to react using military violence. Then, a reference is made to two countries in particular, such as China and the United States (US), and their link with the cyber topic. First, an analysis of the evolution of their diplomatic relationship starting from the seventies is made, focusing on how their relationship has changed with the introduction of ICT in the twentieth-century. Given that the cyber issue represents a core element of discussion between the two countries, their competing visions about cyberspace, the

[4] Collins A., *Contemporary security studies*, oxford university press, 2013, p. 363

[5] The International Telecommunication union is a united nation specialized agency responsible for issue in the field of information and communication technologies.

[6] Eberle C., *Just war and Cyberwar*, Journal of military ethics, Vol. 12, No. 1, 54-67, 2013, p.54

governance of the Internet and the topic of cybersecurity are analyzed. In specific, a reference is made to one of their diplomatic meeting that took place in 2013 in which a type of cyber threat, in particular cyber espionage, was the most discussed theme between the US and China. Finally, the national security threatened by non-traditional threats, such as cyber threats, in the globalized world is considered. Resilience emerges as an essential element adopted by states in their security strategies in order to protect the society from new threats. From a cybersecurity point of view, cyber resilience can be achieved mainly by means of public-private partnership (PPP) and cooperation and dialogue at international level between states and international organizations.

In the second chapter an analysis of some concrete examples of cyber attacks launched against physical objectives and computer networks is made. As regards the first, the famous Stuxnet[7] attack which hit the Iranian nuclear programs in 2009 is described. In addition, other cyber attacks launched against nuclear programs in order to damage nuclear facilities are described, such as the attack against North Korea's nuclear program which took place simultaneously to the Stuxnet attack, the Israel's cyber attack against Syria's nuclear facility in 2007 and the more recent North Korea's attack against South Korea's nuclear program in 2014. As regards the second type of cyber attacks, that is, those conducted against computer networks, the attack launched against Estonian websites by Russia in 2007 is described, together with the similar attack launched the following year against Georgian websites by Russia. In addition, a description of the cyber attacks that Israel and Arabia mutually launched against their websites in 2012 will be portrayed. Then, the recent cyber attacks launched against the computer systems of the Pentagon and the White House by Russia and China, which are considered the countries that possess the most advanced cyber programs in the world, are described. Finally, a reference is made to the phenomenon of hacktivism which consists in launching cyber attacks in order to damage the imagine of the target or causing the disruption of ICT systems for ideological reasons[8]. In particular, the cyber attacks perpetrated by the hacktivist group Anonymous against Canadian government

[7] Stuxnet is a computer worm which was used to conduct an attack against the SCADA systems that control the Iranian nuclear production in order to inflict damage to centrifuges. It was discovered in 2010 and the US and Israel appear to be the perpetrators of the attack.

[8] Sistema di Informazione per la Sicurezza della Repubblica, *National strategic Framework for cyberspace security*, consulted at http://www.sicurezzanazionale.gov.it/sisr.nsf/archivio-notizie/la-cyber-strategy-italiana.html on 15/09/2015, p. 15

websites in 2015 and Israeli government websites in 2012 are depicted. In addition, the phenomenon of cyber terrorism is mentioned, taking as examples the cyber attacks launched in 2015 against the Malaysia airlines website and the US government website by hacker groups linked to ISIS.

In the third chapter an analysis of the European Union (EU) legislative landscape in the cybersecurity field is made, starting from its inception in 2000 until the development of the EU cybersecurity strategy in 2013. First, a focus on the EU cybersecurity strategy, whose goal is assuring an open, free and secure cyberspace, is made. In specific, the three sections in which is organized the strategy are described: the first part, in which a reference to the increasing dependence of modern societies on the Internet and the cyberspace is made, together with a reference to the idea of the application, in the cyberspace, of the same norms and rules which are applied in the physical world in order to achieve the cybersecurity; the second part, in which an analysis of the five strategic priorities (achieving cyber resilience, reducing cybercrime, developing cyberdefence policy and capabilities, developing industrial and technological resources for cybersecurity, establishing an international cyberspace policy for the EU)[9] that the EU has to adopt so as to provide a free and secure cyberspace is made; the third part, in which a description of roles and responsibilities of the different actors involved in the cybersecurity issue at national, EU and international level is made. Then, a focus on the main documents produced and structures involved in the cybersecurity issue at EU level is made, starting from the year 2000. Since the beginning, the Commission has emerged as one of the most important organisms playing a crucial role in the development of communications, documents and decrees on the cybersecurity topic. Another relevant structure involved in the cybersecurity issue is the European Network and Information Security Agency (ENISA) established in 2004, whose main tasks are described. Then, the description of a significant initiative of ENISA, which consists in organizing European cyber crisis exercises aimed at enhancing the cooperation among EU member states in case of cyber attacks is given. Finally, a reference is made to the communications and directives elaborated by the Commission for the protection of critical infrastructures which, together with the fight against cyber crime, represents a priority in the cybersecurity field at EU level.

[9] Ibidem, pp. 4-5

In the fourth chapter the Italian legislative approach to cybersecurity is analyzed, starting from the nineties until the more recent developments in 2016. First, a focus on the Prime minister's decree of the 24th January 2013 "Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale"[10], which defines the institutional architecture (composed by different actors and organisms) in charge of providing cybersecurity but also establishes the creation of a National cybersecurity strategic Framework and a National Plan which together represent the National cybersecurity strategy, is made. Second, a description of the National Framework, which defines the nature of cyber threats and the strategic and operational guidelines to follow in order to enhance the defence capabilities of Italy in the cybersecurity field, is made, together with the description of the National Plan which aims to give full implementation to the Framework by developing lines of action and specific objectives. Third, an overview of the evolution of the Italian legislative approach to cybersecurity is made. The starting point was in the nineties, when the interest in cyber crime rose and many documents started being issued in this field. Then, when Italian authorities became more aware of cyber threats and the risks for the security of the nation that derive from them, they developed other laws and organisms in order to make Italy a safer place from the cybersecurity point of view, focusing also on the protection of critical infrastructures at national level which, together with the fight against cyber crime, represents a strategic priority in the cybersecurity field.

[10] Sistema di Informazione per la Sicurezza della Repubblica, *Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale*, consulted at http://www.sicurezzanazionale.gov.it/sisr.nsf/archivio-notizie/direttiva-sulla-sicurezza-cibernetica.html on 25/10/2015

CHAPTER ONE

CYBERSPACE AND CYBER THREATS

1.0 Introduction

The current era is called Information age. The latter derives its name from the advent of the information revolution which took place in the nineties and consisted in the evolution and spread of Information and Communication Technologies (ICT) in every aspects of life[11]. Therefore, not only changes in the way in which information were transferred, processed, collected, communicated occurred[12] but also the nature of information changed. More in specific, electronic information challenged the traditional information, becoming free from any physical and material link, dematerializing itself. It left the paper support and moved toward the information technology (IT) one.

A consequence of the information revolution was that it eroded the hierarchies which represented the fundamentals of institutions favoring the growth of forms of networks, such as communication and social networks, providing different actors the possibility to communicate rapidly across great distances[13], crossing geographical and time borders. As a result of the spread of ICTs, things are done differently and better with respect to the past and activities are more efficient[14]. In fact, modern societies base their functioning on IT systems, becoming more and more dependent on them.

What emerges from this framework is that in the nineties information started obtaining a central role in international relations[15], becoming a strategic resource and a source of power desired by states at international level, with the same value and influence that capital and labor possessed in the industrial era[16].

---

[11] Collins A., *Contemporary security studies*, third edition, oxford university press, 2013, p. 419

[12] Arquilla J. and Ronfeldt D., *Cyberwar is coming!*, In Athena's camp: preparing for conflict in the information age, chapter 2, pp. 23-60, 1997, p.25

[13] Ibidem, p.27

[14] Ibidem, p.26

[15] Collins A., *Contemporary security studies*, oxford university press, 2013, p. 363

[16] Arquilla J. and Ronfeldt D., *Cyberwar is coming!*, In Athena's camp: preparing for conflict in the information age, chapter 2, pp. 23-60, 1997, p.25

Another consequence of the information revolution was that it changed the nature of conflicts to the extent that the term information warfare[17] emerged in order to refer to a modern way of warfare where information take a central position[18]. Modern conflicts are not fought on the traditional battlefield, geographical borders are not relevant, conventional weapons are not used or only in part, physical violence and blood are absent. The modern field of war is called cyberspace. There are various definitions of the term cyberspace. In general with this term we refer to a man-made domain[19] where online communication takes place as it is composed of all ICT networks that process data, software, hardware, databases, cables, satellites, computer and the Internet[20]. According to the International Telecommunication Union (ITU) the cyberspace is "the physical and non physical-terrain created by and/or composed of some or all the following: computers, computer systems, network and their computer programs, computer data, content data, traffic data and users"[21].

In this digital arena, cyber operations or computer network operation (CNO)[22] take place. This term refers to the "impiego delle capacità cibernetiche con il proposito primario di raggiungere obiettivi all'interno o mediante l'uso del cyberspazio"[23].

Three types of CNO can be analyzed:

- computer network exploitation (CNE)[24];
- computer network defence (CND)[25];
- computer network attack (CNA)[26].

[17] There are various definitions of information warfare. One definition that can be remembered is the official definition of the American aviation derived from *Cornerstones of information warfare,* in which the term refers to any actions aimed to destroy, disrupt and contaminate the adversary's information and its functions, protecting one's own information from similar initiatives and developing one's own military informative activities.

[18] Collins A., *Contemporary security studies*, oxford university press, 2013, p. 419

[19] Sistema di Informazione per la Sicurezza della Repubblica, *National strategic Framework for cyberspace security*, consulted at http://www.sicurezzanazionale.gov.it/sisr.nsf/archivio-notizie/la-cyber-strategy-italiana.html on 15/09/2015, p.9

[20] Collins A., *Contemporary security studies*, third edition,oxford university press, 2013, pp. 363;415

[21] Greco E., *Cyber war e cyber security, diritto internazionale dei conflitti informatici, contesto strategico e strumenti di prevenzione e contrasto*, Istituto di ricerche internazionali archivio disarmo (IRIAD) SIS-11/2014, consulted at http://www.archiviodisarmo.it/index.php/en/publications/magazine/magazine/finish/87/1020 on 14/09/2015, p. 20

[22] Ibidem, p. 18

[23] Ibidem

[24] Ibidem

[25] Ibidem

[26] Ibidem

The latter consists in operations aimed to destroy, modify, manipulate, disrupt information resident in computers and computer networks[27]. This type of attack is realized by human attackers called hackers. This term can have both positive and negative aspects: from the positive point of view, a hacker is an expert of computers; from the negative one it is considered an intruder or cyber criminal. The attack is implemented using tools called malware which consist in viruses, worms, Trojan horses through which the hacker is able to penetrate into the adversary's computer system and get the full system control[28].

Since our critical infrastructures, defined by the UN General Assembly as "those used for, inter alia, the generation, transmission and distribution of energy, air and maritime transports, banking and financial services, e-commerce, water supply, food distribution and public health, and the critical information infrastructures that increasingly interconnect and affect their operations"[29], are controlled by IT systems, if the latter are attacked the results in the physical world could be destructive and the well-being of citizens could be compromised. For instance, electrical generators could be destroyed, trains could derail, airplanes could crash, weapons could not work, money could disappear[30]. Therefore, our increasing dependence on the Internet[31] and cyberspace makes our society and systems more vulnerable to possible cyber attacks.

Since the possibilities of being attacked from the cyberspace are growing simultaneously to our increasing dependence on it, some scholars claim that the cyberspace could represent a privileged arena of war. This digital arena possess some unique characteristics that allow scholars to define it a domain of warfare[32]:

---

[27]Brantly A., *Cyber actions by state actors: motivation and utility,* International journal of intelligence and counterintelligence, 27:465-484, 2014, p. 466

[28] Collins A., *Contemporary security studies,* third edition, oxford university press, 2013, p. 364

[29] Greco E., *Cyber war e cyber security, diritto internazionale dei conflitti informatici, contesto strategico e strumenti di prevenzione* e contrasto, Istituto di ricerche internazionali archivio disarmo (IRIAD) SIS-11/2014, consulted at http://www.archiviodisarmo.it/index.php/en/publications/magazine/magazine/finish/87/1020 on 14/09/2015, p. 39

[30] Clarke R., *War from cyberspace,* 2009, consulted at http://users.clas.ufl.edu/zselden/coursereading2011/Clarkecyber.pdf on 18/09/2015, p. 31

[31] The origins of the Internet date back to the seventies, when researchers of the Defence Advanced Research Projects Agency (DARPA) of the United States Department of Defence developed the Advanced Research Project Agency Network (ARPANET), which represented the forefather of the current Internet. Not only its basics (software) remained unchanged until today but also its academic and experimental nature.

[32] Even S. and Siman-Tov D., *Cyber warfare: concepts and strategic trends,* Memorandum No. 117, May 2012, consulted at

geographical borders and time limit are absent in the cyberspace and this allow the attacker to attack a possible target far away and in a few seconds; its creation and management are entrusted to both military structures and private civil companies so the possible targets of the attack are many; the more civil and military systems depend on cyberspace the more vulnerable they are to possible attacks; the cyber attacker has the advantage of attacking anonymously and in secret therefore making very difficult for a nation target to identify the source of the attack. This is called attribution problem. In addition, cyber weapons, that consist of malware, are able to reproduce themselves in the cyberspace and can be less lethal. This means that cyber weapons possess the advantage of causing damage to the functioning of the state without killing people or destroying critical infrastructures[33].

In addition, three levels of warfare appear to exist in the cyberspace[34]:

- The first level is the tactical level which is the lower level of warfare. Everyday companies, governments, private citizens computers are hit by cyber attacks and technicians have to fight against adversaries on the net to protect computer systems from cyber threats[35].
- The second level of warfare is the operational or warm level. It refers to occasional important attacks such as the Stuxnet attack against Iranian nuclear centrifuges in 2010 and the distributed denial of service attack (DDoS)[36] against Estonia in 2007, which will be analyzed hereafter. Internationally, this level of warfare has produced tensions among nations as there is an increasing evidence of countries that use sabotage and extraction tools in their cyber attacks. Domestically, it has produced political tension as a huge amount of legislation on the cyber topic is being drafted and consequently public sector, private sector and civilians find difficult to agree on what the legislation should or should not include[37].

---

http://mercury.ethz.ch/serviceengine/Files/ISN/152953/ipublicationdocument_singledocument/f3e19de1-bcf7-4d07-b088-f3d477b4329c/en/INSS+Memorandum_MAY2012_Nr117.pdf on 19/09/2015, p.14

[33] Ibidem, pp. 14-15

[34] American foreign policy interests, *Cyberpower and National Security*, 35: 45-58, 2013, p.50

[35] Ibidem

[36] The DDoS attack consists in saturating the computer system of the adversary with so many communication requests that the targeted system cannot respond to the legitimate traffic and become unavailable to users.

[37] American foreign policy interests, *Cyberpower and National Security*, 35: 45-58, 2013, p.50

- The third level is the strategic level or hot war level. In this case a hot war produces devastating and long term effects, causing disruption, damage, death, destruction and devastating economic loss, which are called the "5Ds"[38].

What emerges is that in the information warfare the success does not depend on the physical force or the use of traditional weapons but on the information dominance, that is to say, on the ability to disrupt or damage the information and communication systems of the adversary, collect and exploit as much information as possible about the adversary, while protecting one's own information systems. Some of the strong points of the information warfare are:

- the low cost for the actor that decides to attack as it has not to make huge investment nor possess particular technological skills;
- the absence of traditional borders, such as geographical, jurisdictional and time boundaries;
- the effectiveness and the fact that it is almost within everyone's reach.

Therefore, the development of ICTs did not entail only benefit and advantages for nations but, making societies more dependent on the cyberspace, it increased the number of possible targets vulnerable to cyber attacks. The consequence is an environment characterized by insecurity and uncertainty. In addition, being ICT widespread in the world and almost within everyone's reach, also minor actors, weak states, individuals or non-state sponsored organizations are able to conduct cyber attacks very easily in order to cause huge damages to powerful nations and paralyze their functioning because:

- there are no borders in the cyberspace;
- attacks can be perpetrated anonymously;
- particular technical skills or weapon system are not required;
- the attacker can disappear without leaving traces;

Therefore, ICT has strengthened the asymmetry of modern conflicts which have lost their natural symmetry, that is to say, they are not fought on equal terms between armed forces of states which possess the same strength and which know who the attacker is. Asymmetric conflicts are fought on unequal terms between heterogeneous parties which

[38] Ibidem, p.51

use different means and methods and pursue different objectives. In this type of conflict the weaker is able to attack the stronger which, in turn, is unable to respond and react to the attack as it does not know who the enemy is.

In the military field, the previously cited information dominance, which is at the basis of the information warfare, has always been the key for the success in a conflict since the past. In the military context the term cyber war emerged in order to refer to "conducting, and preparing to conduct, military operations according to information-related principles"[39]. A cyber war consists in destroying or disrupting the information and communication systems of the adversary, in order to know as much as possible about the adversary, who it is, what it does, where it is, impeding the adversary from knowing about oneself[40]. In so doing, the success depends on knowledge and information, therefore capital and labor are less necessary. As Carl von Clausewitz claimed in *On War*, "Knowledge must become capability"[41] and in that sense who possess more knowledge wins.

The first conflict of this type in the information age was the Gulf war of 1991, which involved Iraq and a group of states headed by the United States (US), in which, in addition to the physical force, the information dominance was required in order to win[42]. In fact the US military won the conflict as it collected much knowledge about the adversary and used ICTs in order to paralyze the Iraqi information and communication systems. Therefore, cyber war can be considered as an innovation in warfare[43]. However, cyber war does not require the presence of advanced technology since it can be waged even with low technology[44]. A demonstration of that was the Mongol way of warfare which represented a primitive example of cyber war[45]. In the thirteen century, the Mongol army was able to defeat large armies, such as those of China and Islam which were bigger than the Mongol one, by striking at the heart of their communication systems without using advanced technology. The key for the success was the Mongol

[39] Arquilla J. and Ronfeldt D., *Cyberwar is coming!*, In Athena's camp: preparing for conflict in the information age, chapter 2, pp. 23-60, 1997, p.30
[40] Ibidem
[41] Ibidem, p. 23
[42] Collins A., *Contemporary security studies*, third edition, oxford university press, 2013, p. 369
[43]Arquilla J. and Ronfeldt D., *Cyberwar is coming!*, In Athena's camp: preparing for conflict in the information age, chapter 2, pp. 23-60, 1997, p.31
[44] Ibidem, p. 32
[45] Ibidem, p. 34

superior knowledge and communication system between the command and the troops[46]. Mongol messengers, called Arrow Riders as they rode horses to move, provided the general with information about the adversary's intentions and position within few days[47]. In so doing, the Mongols knew much information about the adversary while keeping information about themselves secret, reaching an overview of the situation.

In one of the most important Mongol campaigns, that against the empire of Khwarizm, the Mongols captured a messenger of the Khwarizm army disrupting the communication between the battlefield and the general, who took the silence from the front as a positive sign[48]. That is a demonstration of the strategy used by the Mongols, focused first on blinding the adversary on the information side, then striking at his heart[49]. What emerges is the crucial role and the strategic value of information in war. Information is equivalent to the victory on the battlefield. Who knows more possess the comparative advantage that allow it to reach the success.

Another demonstration of the fact that the nature of conflicts is changing consists in the idea that states increasingly compete on the basis of their economic strength rather than on the basis of their military force to the extent that the term economic warfare emerges. Actually, economic wars have always been fought but, after the spread of ICTs, states started used the information warfare as a tool in order to fight the economic war. It means that also in the economic field the information dominance is crucial in order to win the war. Therefore, an economic war in the information age consists in cyber attacks launched by a state against the IT system of a company placed in another state in order to gather strategic economic information, know-how and industrial secrets in its own economic favor. This deals with cyber espionage, that will be deeply described after, focusing on China as one of the main country responsible for cyber espionage in the world, especially against the US companies.

The cyber attacks launched against the IT systems of companies represent a threat for the economic competitiveness of nations. Intelligence, in particular economic intelligence, emerges in order to support the economic competitiveness. Intelligence is a tool used by states in order to collect and spread, to public or private actors, important

[46] Ibidem, p. 36
[47] Ibidem
[48] Ibidem, pp. 34-35
[49] Ibidem, p. 35

information for the security of citizens, institutions and companies which, in the twenty-first century, is threatened by new threats such as those that stem from the cyberspace. In Italy, on the basis of the law n. 124/2007[50], the intelligence system consists of three organisms:

- the Department for Intelligence and Security (DIS)[51];
- the Intelligence Agency for the External Security (AISE)[52];
- the Intelligence Agency for the Internal Security (AISI)[53].

The activities conducted by the intelligence can be organized into three phases:

- acquisition of the news, through research, collection and assessment of data that derive from various sources such as the media and the web;
- management of the information, transforming the rough information into a well-structured element of knowledge;
- communication of the information to the government, administrations and public bodies in order to take the right decisions and implement the right activities.

There are different types of collection and elaboration of information, among which Open Source intelligence (Osint)[54], Human intelligence (Humint)[55] and Signal intelligence (Sigint)[56] can be remembered[57].

In the economic field, the economic intelligence refers to activities of research, collection and elaboration of economic information in order to protect the economic competitiveness of a nation. It means that activities of economic intelligence deals with

[50] The law n.124/2007, published in Gazzetta ufficiale n. 187 the 13 august 2007, established the Intelligence System for the Security of the Republic and reformed the Italian intelligence on the basis of three structures: DIS, AISE and AISI.

[51] As stated in the law 124/2007, DIS coordinates the whole intelligence system for the security and monitors and coordinates the activities of the two intelligence agencies AISE and AISI. It gives support to the Prime minister for the implementation of his activities.

[52] By law 124/2007 AISE is in charge of elaborating information for the protection of the security and integrity of the republic from foreign threats. In addition it has to address foreign espionage activities against Italy and the national interest.

[53] By law 124/2007 AISI is in charge of elaborating information for the protection of the security and integrity of the republic from internal threats. In addition it has to address internal espionage activities against Italy and the national interest.

[54] The term Osint refers to the collection of information through the analysis of open sources.

[55] The term Humint refers to the collection of information through interpersonal contacts.

[56] The term Sigint refers to the collection of information through the interception of signals between both people and machines.

[57] Sistema di Informazione per la Sicurezza della Repubblica, *L'Intelligence,* consulted at http://www.sicurezzanazionale.gov.it/sisr.nsf/cosa-facciamo/l-intelligence.html on 18/12/2015

the protection of the strategic know-how, secret industrial information, sensitive information with a huge economic value and the economic heritage in general from threats, for instance cyber espionage, that comes from adversary states and that could damage the economic competitiveness of a nation. It is of outmost importance highlighting the fact that the intelligence collaborates with the private sector, universities and research centers.

From a security perspective, with the spread of ICTs new threats emerged and the consequence was that the state, which has always been the main actor responsible for the provision of security, had to change the strategy of response. More in specific, its nature and structure have been transformed.

As regards the nature, the importance of its functions in providing security is changing in the sense that a state does not focus anymore on the protection of geographical borders but, since the threat comes from the cyberspace, the priorities are different. It means that the state turns its focus on the protection of the cyberspace from cyber threats. Therefore, with the spread of ICT the concept of cybersecurity has emerged, challenging the traditional concept of security.

As regards the structure, the idea of a state as a single actor in charge of providing the security has disappeared and has been replaced by the idea of a state as a system. The latter means that the whole society, public and private actors, is involved in the management of the cyber threat. Hierarchy has been replaced by network and interdependence among different actors that together decide how to act. Therefore, the concept of "sicurezza partecipata"[58] has emerged in order to refer to the fact that, in the face of new threats, the cooperation and the dialogue among public entities, private actors, companies, universities are essential to guarantee the security.

In Italy, a real cybersecurity market has developed. As stated by the Assinform[59] report of 2015 the Italian cybersecurity market is growing since 2013, notably there has been an expansion of 2%, that is to say, 772 million euro[60]. Considering the different parts of the market, the software one experimented a positive trend, notably + 3,5%, focused on

[58] Cencetti C., *Cybersecurity: Unione Europea e Italia prospettive a confronto*, edizioni nuova cultura, Roma, 2014, consulted at www.iai.it/sites/default/files/iaiq_12.pdf on 15/09/2015, p. 81

[59] Assinform is the National Association that groups the main companies involved in the IT sector in Italy.

[60] Assinform, *Security & Cybersecurity*, consulted at http://www.rapportoassinform.it/Sintesi/Segmenti_mercato/Security--Cybersecurity.kl on 19/12/2015

projects aimed to securitize traditional system but also innovative systems such as mobile and social[61]. The services part experimented a positive trend too, notably +1,6%[62]. On the contrary, the hardware part experimented a decrease of 1%[63].

Recently, Poste Italiane has emerged as a company involved in the cybersecurity sector, notably in the fight against cyber crime and the security of digital communication. In that sense, Poste Italiane has developed three main technological centers for the cybersecurity:

- the Cybersecurity Innovation Lab[64], located in Trento and created in collaboration with the association Trento RISE, aimed to develop scientific and technological innovation;
- the Computer Emergency Response Team (CERT), which is composed of experts in the cybersecurity field in order to provide security services and responses in case of IT emergencies;
- the Cybersecurity Technological District, which is located in Calabria and whose aim is to realize solutions for the protection of electronic payments. 30 million euro have been invested.

In addition, Poste Italiane takes part to two international organizations in the cybersecurity field:

- the European Electronic Crime Task Force (EECTF)[65], founded in 2009 by Poste Italiane, Postal police and other organisms, has the task of creating a strategic alliance at EU level in order to repress and prosecute activities linked to cyber crimes;
- the Global Cybersecurity Center (GCSEC)[66] which is a no-profit organization at international level aimed to study, search and spread new techniques in the cybersecurity field.

[61] Ibidem
[62] Ibidem
[63] Ibidem
[64] Poste italiane, *Cybersecurity*, consulted at http://www.posteitaliane.it/it/innovazione/cyber_security/index.shtml on 19/12/2015
[65] Ibidem
[66] Ibidem

1.1 The vulnerability of modern systems and its consequences

As previously stated, the modern society is increasingly dependent on ICT. In fact, our critical infrastructures, from water supply to financial services are controlled by information systems. However, the more we depend on the Internet the more we are exposed to the risk of being attacked from the cyberspace. The reason lies in the technical vulnerabilities intrinsic to the information systems[67]. Therefore, if these vulnerabilities are not solved, the rush toward a cyber war is inevitable[68]. The only solution to this situation is build security into systems since their creation[69].

The vulnerabilities resident in the IT systems are so many that conducting an attack is very easy. These vulnerabilities, also called '0day' vulnerabilities[70], are exploited not only by sophisticated hackers but also by non-technical experts who can conduct magnificent attacks without relatively difficulty.

Among the various types of cyber attacks, cyber crime is the most pervasive problem with respect to cyber espionage or cyber war and it costs a lot to the global economy[71]. It consists in conducting criminal activities on the web such as fraud or identity theft. However, it is the less discussed among politicians[72].

As regards cyber espionage, which will be the topic of the following paragraph, it is a common problem today due to the difficulty of keeping secrets in a world so interconnected. A huge quantity of information can be stored and transferred on the web but at the same time and very easily the same information can be manipulated or stolen[73]. The activity of cyber espionage is not conducted with the aim of damaging or disrupting the enemy's systems but it is mainly aimed at gather intelligence (military, economic, commercial and technological) about the enemy's intentions so as to develop strategies or gather the cyberspace assets of the enemy, that is to say, steal software and databases. The first event in the history of cyber espionage took place in the seventies

[67] McGraw G., *Cyber war is inevitable (unless we build security in)*, The journal of strategic studies, Vol. 36, No.1, 109-119, 2013, p. 109
[68] Ibidem
[69] Ibidem, p.110
[70] Ibidem
[71] Ibidem
[72] Ibidem
[73] Ibidem, p. 111

when Russia was able to connect to ARPANET and had access to the US websites[74]. Although cyber war does not represent the major cyber threat it is the most discussed problem among policy makers. However, there is not a clear definition of cyber war. The main problem with cyber war is that it is difficult understanding if an action that does not produce effects on the real world, such as infecting a computer using malware, could constitute an act of war. What is necessary in order to determine if a cyber action constitutes an act of cyber war is the presence of the so called "kinetic effect"[75], that is to say, an impact on the real world. An example of cyber war could be infecting the command and control system of the enemy nation using malware and making the drones of the adversary attacking the wrong target causing destruction. Therefore, as previously stated, the term cyber war can be used to refer to a situation in which, as a result of the malicious use of computer technologies, targets in the physical world are damaged. Concrete examples can be the Stuxnet attack conducted by Israel and United States against Iranian nuclear program in 2010 and the bombing of a nuclear facility in Syria by Israel in 2007[76].

However, according to John Stone, defining the meaning of the term war is not very simple. The origins of the unclear understanding of the concept of war and, in specific, of the means of war (force or violence) are to be found in the field of Strategic Studies[77]. During the Cold War, when nuclear weapons were invented, Strategy as an intellectual field emerged in response to this invention[78]. Its aim was to find solutions, methods in order to deter another future war based on the use of the nuclear weapons. What was important, according to strategists, was that the strategy of deterrence worked[79]. At that time, war, force, violence and their meanings were not object of study for them. Even after the Cold War, when the topic of deterrence was no longer important, strategists did not commit themselves to study and analyze the fundamentals of war because, during that period, Strategic Studies was considered only a part of the

[74] Even s. and Siman-Tov D., *Cyber warfare: concepts and strategic trends,* Memorandum No. 117, May 2012, consulted at http://mercury.ethz.ch/serviceengine/Files/ISN/152953/ipublicationdocument_singledocument/f3e19de1-bcf7-4d07-b088-f3d477b4329c/en/INSS+Memorandum_MAY2012_Nr117.pdf on 19/09/2015, pp.20-21

[75] McGraw G., *Cyber war is inevitable (unless we build security in),* The journal of strategic studies, Vol. 36, No.1, 109-119, 2013, p. 112

[76] Ibidem

[77] Stone J., *Cyber war will take place*, The journal of strategic studies, Vol. 36, No. 1, 101-108, 2013, p.101

[78] Ibidem

[79] Ibidem, p.102

bigger and important field of Security Studies[80]. Therefore, when the thematic of war became important again, with respect to international terrorism or ethnic conflict, there was not a solid understanding of the concept yet[81]. This means that if there is not a clear understanding of the concept of war, which is the basis, it is difficult to reach an agreement about the status of cyber attacks and decide whether or not they constitute an act of war[82]. An analysis of the concept of lethality and its relationship with force and violence will be made after and the possibility that a cyber attack could constitute an act of war, which means that a cyber war could take place, will be demonstrated.

Going back to the topic of cyber vulnerability, a curious characteristic is its balancing effect on power[83]. For example, in the Stuxnet attack the balance of power was not in favor of Iran at the beginning in fact its nuclear centrifuges were destroyed by the US. However, in a second moment, Iran was able to respond to the US attack intercepting a US drone that was flying in the Iranian airspace. What emerges is that the more developed a country is the more vulnerable to cyber attack it is because its great reliance on ICT[84]. Therefore developing cyber defence is as important as cyber offence[85]. However, if offence is too much developed this encourages the enemy to attack first in order to avoid being attacked in turn; if defence is equal or superior to offence, the adversary is not encouraged to attack[86]. The US is an example of country which is very good at offence (exploitation, penetration) but not at defence because of the insecurity of modern systems from which we depend on, and this is the problem[87].

Cyber war will be inevitable if the defence side will not be strengthened. Building more secure systems by means of software security is of outmost importance as the main security problem is a software problem due to the fact that software is full of imperfections which are exploited by hackers[88]. Building more secure systems means designing software that can continue to function in spite of being attacked by malware. Software security involves both the implementation of security features like secure

[80] Ibidem
[81] Ibidem
[82] Ibidem, pp. 102-103
[83] McGraw G., *Cyber war is inevitable (unless we build security in)*, The journal of strategic studies, Vol. 36, No.1, 109-119, 2013, p. 113
[84] Ibidem
[85] Ibidem
[86] Ibidem
[87] Ibidem
[88] Ibidem, p.116

software layers (SSL) and project a strong software since its inception[89]. Since 2001 much progress has been made in the field of software security and best practices have been developed and put into use.

To conclude, it is necessary to solve the security vulnerabilities intrinsic to software in order to avoid the inevitable. It is exactly this vulnerability that make very easy to develop a cyber weapon on the example of Stuxnet and conduct a similar attack.

1.2 From espionage to surveillance

The cyber espionage has been previously described as one of the threats that could stem from the cyberspace. Two countries in particular, the US and China, are involved in this issue.

Espionage was one of the themes discussed in June 2013 in California, at the Sunnylands meeting between the US president Barack Obama and the Chinese president Xi Jinping[90]. The two presidents discussed also about other topics such as trade, maritime disputes, nuclear programs but the issue of cybersecurity was at the core of the meeting. The US has been pushing Beijing to stop Chinese cyber attacks against its territory for years and this meeting was seen as the final stage of this long path.

China, which is one of the main country in the world responsible for cyber espionage above all against the US, conducts its cyber attacks in order to collect not only political and military intelligence but also improve its economic competitiveness[91]. As stated by a Washington Post report, a huge quantity of information has been stolen by Chinese hackers, from weapons programs but also from offices of foreign ministries, embassies, governments of different countries such as India, United Kingdom, Germany, Taiwan, Romania and also various important newspapers were hacked[92]. The fundamental reason why Chinese cyber attackers steal commercial information and intellectual property from other industries is due to the fear that China has of being technologically

[89] Ibidem
[90] Segal A., *Cyberspace: the new strategic realm in US-China relations*, Strategic analysis, Vol. 38, No. 4, 577-581, 2014, p. 577
[91] Ibidem
[92] Ibidem

dependent from the US, European or Japanese firms[93]. Doing so, China hopes to transform its industries which are labor intensive and high-polluting into more technology intensive one[94].

The US, in response to Chinese espionage, started a campaign of 'naming and shaming' against China[95]. This means that if previously the US officials did not name directly the country suspected of being behind the attack but called for expert in order to confirm their suspicion, now the US officials clearly announce the name of the attacker[96]. In fact in 2013 the Pentagon publicly announced that the People's Liberation Army (PLA)[97] was involved in Chinese cyber attacks against the US industries[98].

However, the day after the Sunnylands meeting ended, the US campaign of naming and shaming against Chinese espionage was interrupted and the focus became the US surveillance program[99]. The cause was Edward Snowden revelations in Hong Kong about the US surveillance of Internet data. The National Security Agency (NSA)[100] technician told that the NSA, using a program called PRISM[101], was able to penetrate the biggest American technology companies such as Google, Microsoft, Facebook and have access to data[102]. In this way documents, phone calls, messages, email of millions of people worldwide were under the US control. The NSA was able to listen to the phone calls of various leaders such as the Brazilian president and the German chancellor and hacking the computers of the European Union offices and Indian embassy in New York and Washington[103].

After Snowden revelations on the US surveillance program, China described the US as the "real hacking empire"[104], attracting support from other like-minded countries.

---

[93] Ibidem, p. 578
[94] Ibidem
[95] Ibidem
[96] American foreign policy interests, *Cyberpower and National Security*, 35: 45-58, 2013, p.53
[97] The PLA is the armed force of China. It emerged in 1927 when communist won against nationalist. The original name was red army. It evolved under Mao ze dong control.
[98] Segal A., *Cyberspace: the new strategic realm in US-China relations*, Strategic analysis, Vol. 38, No. 4, 577-581, 2014, p. 578
[99] Ibidem
[100] The NSA is an intelligence organization of the US. It was created in 1952 with the aim of protecting the US national security systems from foreign adversary's attempts to gather sensitive information.
[101] The PRISM is the Planning Tool for Resource Integration, Synchronization, and Management, it is a surveillance program used by the NSA to collect and process internet data
[102] Segal A., *Cyberspace: the new strategic realm in US-China relations*, Strategic analysis, Vol. 38, No. 4, 577-581, 2014, p. 578
[103] Ibidem
[104] Ibidem, p. 579

However, the US replied arguing that there is a difference between industrial espionage and cyber activities conducted to gather military and political intelligence. While the former represents a violation of international norms, the latter does not[105]. The activities carried out by the US, as argued the Director of National Intelligence James Clapper, were aimed at enhancing security and were part of an anti-terrorist strategy, not at stealing commercial secrets as does China[106]. Another consequence of the revelations was that the US partners and friends such as Brazil and Germany wanted to limit the US digital surveillance, focusing on the right of privacy in the cyberspace[107]. However, the same countries that pushed for a reduction of American influence over the Internet were the same that spied foreign politicians in their turn. Furthermore, the most important American technology companies reacted to the surveillance program organizing movements against the government program. For instance, Microsoft introduced a set of privacy features such as encryption[108]. Together with other companies, a set of guidelines for regulating surveillance was developed and it included the limitation of the collection of data by the government and the respect of the free flow of information[109].

Washington announced that in the future it will continue its battle against Chinese cyber espionage and, as claimed by the president Obama, the American intelligence agencies will continue to gather information about the intentions of foreign governments in the same way other countries' intelligence agency do[110]. To conclude, the absence of transparency means to the US that it is very difficult to keep a cyberspace open, global and secure[111].

1.3 The evolution of the US-China diplomatic relationship

The relation between the US and China is said to be one of the most important bilateral relations as they share same interests from political, economic, security perspectives.

[105] Ibidem, p.578
[106] Ibidem, p.579
[107] Ibidem
[108] Ibidem, p. 580
[109] Ibidem
[110] Ibidem
[111] Ibidem

After the end of the Second World War the US-China diplomatic relationship was characterized by the silence until the seventies, notably April 1971, when China invited a US ping-pong team to Beijing, introducing the so called "Ping-Pong diplomacy"[112]. That event represented the first step of a path of reconciliation between the US and China. In fact in 1971 the US National Security Advisor Henry Kissinger met Chinese leaders in Beijing two times in order to organize the subsequent visit of the US President Nixon[113].

On February 1972 the US President Nixon arrived in China and, after a meeting with Mao Zedong and Zhou Enlai, signed the Shanghai Communiquè[114] in which the US and China expressed their common opinion about opposing the soviet expansionism in Asia, improving their economic and cultural relations and solving the Taiwan issue[115]. That was the first time that an American head of state had a direct contact with the Chinese land[116]. Therefore, the Shanghai Communiqué marked a fundamental change in the relationship between the US and China after twenty years of non-recognition[117], making their link focused more on cooperation than on contrast.

However, the process of normalization[118] of US-China relationship started in 1972 was completed only in 1978 when the two governments established a joint communiqué on full diplomatic relations and when, the following year, they established officials embassies in Beijing and Washington[119]. By the joint communiqué the People's Republic of China (PRC) was recognized by the US as the only legitimate government

[112]US department of state, office of the historian, *Cronology of us-china relations, 1784-2000*, consulted at https://history.state.gov/countries/issues/china-us-relations on 11/12/2015
[113] Ibidem
[114] Ibidem
[115] The Taiwan issue emerged in 1949 after the China's civil war, when the People's Republic of China was founded and the members of the Kuomintang went from the mainland to the island of Taiwan, a China's province, which, signing a mutual defence treaty with the US, caused its separation from the mainland. Since that event, the China's government strove for a peaceful reconciliation of the mainland and the island following the One-China principle while Taiwan wanted the independence under the Two-China principle. The Taiwan issue was one of the main element of discussion in the diplomatic relations between the US and China.
[116] US department of state, office of the historian, *Cronology of us-china relations, 1784-2000*, consulted at https://history.state.gov/countries/issues/china-us-relations on 11/12/2015
[117] Ibidem
[118] Ibidem
[119] Ibidem

of China and Taiwan was considered a part of it[120]. In addition, the US claimed the end of its diplomatic relations with Taiwan authorities[121].

During the eighties the relationship between the two countries continued to be normal and characterized by mutual visits of American and Chinese leaders and the signing of agreements. In 1979, after the visit of the Chinese president Deng Xiaoping in the US, a trade agreement between the US and China was signed[122]. In 1982 the two countries established a joint communiqué in which the US announced a reduction of arms sales to Taiwan and China claimed a resolution of the Taiwan issue[123]. In 1984 the American president Ronald Reagan went to China and in 1985 the Chinese president Li Xiannian visited the US[124]. In 1989 tensions emerged between the two countries after the Chinese military suppression of demonstrations in Tiananmen Square and the consequent imposition of economic sanctions on China by the US[125]. However, the US president Bush assured Chinese leaders that diplomatic relations would not have been compromised. What emerged from this framework was the commitment of both countries to improve dialogue and cooperation on different level, from the economic, military and diplomatic perspectives.

In the nineties, under the presidency of Clinton in the US and Jiang Zemin in China, the information revolution took place and ICTs invaded every aspects of everyday life, introducing a new element of discussion in the diplomatic relationship between the US and China: the cyber issue. The introduction of this topic in their relations caused mistrust and diffidence as, on one hand, the US considered China a source of cyber threats and, on the other hand, China believed the cyberspace an instrument that could be used by the US in order to contaminate the Chinese culture by imposing western values.

Over the years, the tension on this topic between the two powers increased to the point that in 2001, under the Bush administration, the "first cyber world war" broke out after that a US surveillance plane was forced to land on Chinese territory[126]. The mutual

[120] Ibidem
[121] Ibidem
[122] Ibidem
[123] Ibidem
[124] Ibidem
[125] Ibidem
[126] Collins A., *Contemporary security studies*, third edition, oxford university press, 2013, pp.370-371

mistrust of the countries increased a lot when GhostNet, a Chinese cyber espionage system, was discovered in 2009.

It is under the presidency of Obama that the cyber issue, in particular the threats that the cyberspace poses to the security, the well being and the economy of a nation, emerged as one of the main element of interest to care about, not only from the military perspective. Obama claimed that the cybersecurity issue had to be faced on the basis of dialogue and cooperation with the Chinese government. On the other side, more dialogue and cooperation seemed to be promoted by the president Xi Jinping who, since 2013, is following an approach focused on the security of the cyberspace at a national level as his predecessors Jang Zemin and Hu Jintao did but at the same time he refused considering the cyberspace a battlefield, emphasizing the importance of cooperation. 2013 has been considered the cybersecurity year and, as regards the US-China relationship in the cyber field, both negative and positive events influenced it. As regards the negative events, they dealt with episodes of cyber espionage and cyber attacks like the previously described Snowden case but also the Mandiant case. The latter refers to a report entitled "Exposing One of China's Cyber Espionage Units"[127] issued by the Mandiant security agency in order to demonstrate the involvement of Chinese government organisms in cyber attacks against the entire world. Those events enhanced the necessity of more dialogue between the countries.

In fact, from a positive perspective, 2013 was a year characterized by cyber cooperation between the US and China. In that sense, an important moment was represented by the previously cited Sunnylands meeting between the two presidents which took place in California in June 2013. During that meeting the cybersecurity issue was a core element of discussion but also cyber espionage, as previously stated. Efforts have been made by both countries in order to reach a bilateral cooperation in the cyber field but doubts about an efficient cooperation and trust emerged. An effective dialogue between the US and China is impeded by their different ideas about cyberspace and cybersecurity. In addition, the absence of a central organism in charge of cybersecurity both in the US and in China increases the difficulty to cooperate.

---

[127]Rizzini Cancarini P., *Cina, Stati Uniti e cyber security: anno nuovo vita nuova?*, Il caffè geopolitico, consulted at http://www.ilcaffegeopolitico.org/15139/cina-stati-uniti-e-cyber-security-anno-nuovo-vita-nuova-ii on 12/12/2015

During one of the last meeting between the two presidents that took place in 2015 at the White House, the topic of cybersecurity was the core of the discussion again. The two governments promised to stop cyber theft of intellectual property for commercial reasons and president Obama argued that they reached an agreement on avoiding cyber intrusion and finding common rules in the cybersecurity field[128]. However, the US President warned the Chinese government that it will punish China with sanctions if it will not stop cyber attacks against American targets. Actually, it seems that despite the agreement on cybersecurity has been reached, differences on this topic between the two nations remain. In fact, on one hand the US president stated that they agreed on the principle of avoiding cyber espionage against companies, on the other hand Mr. Xi did not talk about cyber espionage but only cyber crime[129]. Another issue that remains open refers to critical infrastructures and governments commitment not to attack them as a unique definition of critical infrastructure is absent. Therefore, what emerges is that cooperation is illusory while mutual mistrust in the cyber field remains.

1.4 US and China's competing visions on cyberspace

As stated in the previous paragraph, the cybersecurity issue has become one important element of discussion between the US and China. However, their visions about cyberspace, how to regulate it and how to govern the Internet can diverge sometimes.
In the US international strategy for cyberspace, Internet and cyberspace are depicted as "open, secure and global"[130]. As regards the openness of the Internet, Chinese government aims at controlling information and keeping them outside China: in fact it has applied the Great Firewall in order to block Google, Facebook and Twitter[131]. On the other side, Chinese blogger try to spread information and data on the web[132]. Therefore it appears that China does not share with the US the same interest about an

128 Hirschfeld J. and Sanger D., *Obama and Xi Jinping of China Agree to Steps on Cybertheft*, The New York times, consulted at http://www.nytimes.com/2015/09/26/world/asia/xi-jinping-white-house.html?ribbon-ad-idx=9&rref=world/asia&module=Ribbon&version=context&region=Header&action=click&contentCollection=Asia%20Pacific&pgtype=article&_r=1 on 11/10/2015
129 Ibidem
130 American foreign policy interests, *Cyberpower and National Security*, 35: 45-58, 2013, p.51
131 Ibidem
132 Ibidem

open Internet. However, China is moving toward a more open Internet policy as controlling all information and activities on the Internet is impossible for the government[133].

As regards the second theme, that of a secure Internet, it seems that both China and the US are worried about cyber crime and cyber terrorism against their critical infrastructures[134]. However, it is difficult to make a discussion on this topic because the two countries do not share the same definitions in the security field. In fact, while the US uses the term 'cybersecurity' to refer to the security of the Internet, China uses the term 'information security'[135]. This one involves the consequences of a security policy on the information that flow on the net.

As regards the development of global standards[136], which is important for innovation, Chinese are skeptical. In fact, Chinese policymakers think that being technologically reliant on the West could represent a problem. They would prefer developing Chinese industrial strategies in order to become more independent from US companies.

As for the cyberspace, China accuses the US to be hypocritical because if on one hand the US advocates a peaceful cyberspace, on the other hand it is militarizing it by establishing the US cyber command and developing cyber weapons such as Stuxnet[137].

1.4.1 Internet governance

China and the US do not share common vision about the Internet governance. In fact, the US aims at a multi-stakeholder, transparent and bottom-up[138] Internet governance while China aims at putting the Internet governance under control of the government. It can be said that China does not agree on the current Internet governance system and believes that the US does not want to change it because it produces benefits, but only for itself. In addition, China is shaping the Internet in order to obtain an economic, military and political advantage[139].

[133] Ibidem
[134] Ibidem
[135] Ibidem
[136] Ibidem, p.52
[137] Ibidem
[138]Ibidem
[139] Ibidem

From an economic point of view, as previously stated, China does not want to be dependent on the West[140]. Therefore, it is increasing the quantity of money to improve Research and Development (R&D)[141]. In addition, China can lean on millions of future scientists and engineers in order to become the great innovative power it hopes to be by 2049[142].

From the military perspective, China sees itself as the weakest part, with respect to the US[143]. Therefore, it is studying how to attack the US weaknesses by developing asymmetrical strategies[144] in the cyberspace. An example could be developing a strategy in order to impede that supply ships meet on time[145]. The strategic element here is the fact that if China demonstrates to the US that it is able to penetrate the network without leaving traces, the US has to consider the possibility that China, in case of escalation of a conflict, would be able to act.

From the political point of view, the Internet is used by China to respond to political issues such as the Tibetan one. In fact, many Tibetan activists and think tanks focused on the Tibet issue were hacked and flooded by spam by the Chinese government[146].

1.4.2 China's future behavior in cyberspace

The behavior of China in relation to the cyberspace and the Internet is likely to change in the future. In fact the structure of the Internet, which is easily monitored today because of few access points, is likely to become more open as China is becoming increasingly reliant on it[147]. In addition, its behavior will change over time because some groups might emerge within the Chinese government arguing that hacking for a long time and establishing its own Internet standard would not be helpful for China and its economic growth[148].

[140] Ibidem
[141] Ibidem
[142] Ibidem
[143] Ibidem
[144] Ibidem
[145] Ibidem
[146] Ibidem
[147] Ibidem, p.53
[148] Ibidem, p.54

It would be desirable if, in the future, the US finds more points of contact with China and defines common norms for the cyberspace[149]. However, this is difficult to realize because, as described above, their positions are often contrasting.

1.5 Cyber war and lethality

Going back to the topic of cyber war, its relationship with lethality is a very discussed theme among scholars in order to understand if a cyber war can take place because they do not share the same opinion.

Some scholars argue that a cyber attack could constitute an act of war despite the absence of lethality. On the contrary, other scholars like Thomas Rid argue that lethality is the necessary element in order to talk about war and, as a consequence, a cyber war exists if the cyber attack has produced death. In fact he claims that an act of war should be political in motivation, instrumental in character and lethal in potential[150]. However, he claims that a cyber war has never taken place in the past nor will take place one in the future as no cyber attacks possessed the characteristics of an act of war[151]. A cyber attack cannot constitute an act of war itself but can represents only a supplementary element to a real act of war[152].

When Rid gives his definition of act of war, and in particular when he argues that it should be political in motivation and instrumental in character, he makes a reference to the Clausewitz's idea of war. Clausewitz defines war as an act of force[153]. The word he uses to refer to force is the word 'gewalt'[154]. The latter can mean both force and violence[155]. The type of force considered by Clausewitz in his definition of war is the physical force that can produce a physical change[156]. Therefore, if "War is an act of force to compel our enemy to do our will"[157], how force can produce its effects? It can

[149] Ibidem
[150] Stone J., *Cyber war will take place*, The Journal of strategic studies, Vol. 36, No. 1, 101-108, 2013, p.103
[151] Ibidem
[152] Ibidem
[153] Ibidem, p. 104
[154] Ibidem
[155] Ibidem
[156] Ibidem
[157] Ibidem, p. 103

do it "by imposing physical change on human bodies"[158], which means causing death or injury. These effects are what we call violence. Therefore, "force implies violence which in turn implies lethality"[159] in a causal connection. However, force and violence do not always produce lethality. Force can be violent even if it does not kill anyone, but only causing damage. This means that violence can be directed toward buildings and other lifeless targets, not only toward human beings in order to kill them. A concrete example of what is stated above dates back to 1943, when the US Army Air Force conducted a raid over Germany in order to destroy a factory. During the bombing, thousands of people were killed but it was just an accident because the factories were the real target of the attack. When Rid refer to acts that do not involve lethality but damages to things he uses the term sabotage[160].

It emerges that insisting on lethality as the inevitable consequence of violence is wrong because, doing so, the raid attack in 1943 would not be an act of war. If lethality is no longer the focus of the reasoning, judging the status of cyber attacks on this basis is not correct.

However, another objection in addition to the Rid one can be made to the fact that a cyber attack could constitute an act of war. Analyzing the Clausewitzian definition of act of war and the relationship between force and violence, it appears that violence is a product of force[161]. Since it seems that cyber attacks are not reliant on force, it is not clear whether the violence that derives from cyber attacks is the result of an act of force. The solution to this question consists in considering the technology used in a cyber attack as a violence multiplier[162], as a medium to transform a small quantity of force into a great amount of violence[163].

To conclude, it can be stated that a cyber attack could constitute an act of war, therefore cyber war could take place, because as previously described, the relationship between violence and lethality is not inevitable. It is possible to talk about war even when violence breaks things rather than killing human beings[164].

[158] Ibidem, p. 104
[159] Ibidem, p. 103
[160] Ibidem, p. 105
[161] Ibidem, p. 106
[162] Ibidem
[163] Ibidem, p. 107
[164] Ibidem

1.6 Cyber attacks and the just cause for war

This paragraph too is focused on cyber attacks but from a different perspective: a reference to the Just War Tradition (JWT)[165] is made in order to understand under what conditions a cyber attack might constitute a just cause for war[166], that is to say, might provide the attacked country with a just cause to respond with military violence. Three categories of cyber attacks will emerge:

- one composed of those that satisfy the just cause requirement
- one composed of those that do not satisfy the just cause requirement
- one category will be composed of unclear cases[167].

The previously mentioned JWT is based on a important pillar, that of the just cause requirement[168]. From a moral point of view, a nation-state victim of an attack can wage war only if it has the just cause to do so. In order to better understand that pillar, an analysis of the morality of human beings is needed. Human beings possess some natural rights such has the right to life[169]. This one obligates each of us not to kill anyone. In addition, each of us belong to a group of people and this fact is very important for our identity because when we define who we are we make a reference to the type of group or community to which we belong. This allow us to argue that we are Catholics, Italian, American and so on. These human communities, like each human beings, have the right to life, that is to say, the right not to be attacked and at the same time are prohibited to employ military violence against another community[170]. However, this prohibition against waging war is not absolute. In fact in some specific cases, communities can use military violence against each other but, as required by the just cause requirement, they have to explain what the other community has done so as to become objective of military violence. For example, in case of a serious moral violation of human rights, a community can wage war against another one. Obviously, some violations clearly

[165] Eberle C., *Just war and Cyberwar*, Journal of military ethics, Vol. 12, No. 1, 54-67, 2013, p.54
[166] Ibidem
[167] Ibidem
[168] Ibidem
[169] Ibidem, p. 55
[170] Ibidem

provide a country with the just cause to use military violence, such as in case of invasion of the other country. Some other do not satisfy the just cause requirement, such as in case of denigration of the population, while other stay in a medium position between the first two.

Nevertheless, it is not always easy for a country to give the explanation required by the just cause requirement: this is the case of cyber attacks. During a traditional warfare where conventional weapons are used, it is easy to understand from what source the attack has been originated. On the contrary, when we are in presence of a cyber attack, the attribution problem emerges. As previously stated, it consists in the fact that, since the cyber attacker hides himself behind a computer while attacking, it results impossible for the victim to attribute with absolute certainty the action to the agent. Therefore, the victim cannot provide the above stated explanation. Consequently, if the victim possesses only suspicions but not certainty, on the basis of the JWT, it cannot use military violence in response because it is morally forbidden[171].

As regards the first category of cyber attacks, those that can satisfy the just cause requirement, it is important that a serious violation takes place. For instance, a country victim of an attack is allowed to respond using military violence in case of penetration of the software that controls the critical infrastructures of a country destroying them or, through the use of malware, sabotage of the air traffic control systems causing a plan to crash into another full of civilians[172]. All this is possible because of our increasing reliance on ICT which makes us more vulnerable to cyber attacks[173]. However, a simple cyber attack on critical infrastructures is not sufficient in order to satisfy the just cause requirement. What is important is the fact that the attack is destructive and provokes the death of civilians in order to provide a just cause for war. In addition, another significant element to take into consideration when analyzing if a cyber attack provides a just cause for war is understanding whether a cyber attack is an end in itself or it is a part of a wider plan[174]. However, due to the attribution problem, it is difficult not only to define the source from which the attack started but also whether the attack is a part of a plan and what type of plan. Therefore is not easy to assess if the just cause exists.

[171] Ibidem, p. 57
[172] Ibidem, p.60
[173] Ibidem
[174] Ibidem, p. 61

The majority of cyber attacks do not satisfy the just cause requirement. Two examples of cyber attacks that belong to this category could be: the theft of valuable information[175] and the cyber attacks conducted by Russia against Estonia in 2007. As regards the former, the Chinese espionage, which has been previously examined, is taken into account. Chinese hackers and the PLA were behind the theft of important data from industries, universities and governments. Formulas belonging to the field of bioengineering, nanotechnology, pharmacy, weapons programs have been stolen[176]. However, a cyber attack of this type does not satisfy the just cause requirement. This is because the country that suffer the theft of information cannot respond using lethal violence in order to prevent aggressor from stealing secret information, but only diplomatic tools such as sanctions or boycotts[177].

The second example taken into consideration refers to the DDoS attack perpetrated by Russia against Estonian websites after the removal of a soviet soldier statue by Estonian authorities. Some Estonian officials reacted in a strong way to this attack, arguing that it was similar to a nuclear attack. Actually, the result of the attack was that banks and government suffered damage but no Estonians were killed, no properties were destroyed and no territory was seized[178]. Therefore, the attack on Estonia did not satisfy the just cause requirement. Similarly to what is stated above with respect to Chinese espionage, also in this case, Estonia which suffered only economic loss, cannot respond using military violence.

The third category of cyber attacks includes those that do not clearly pertain to the first nor to the second category because of their ambiguous status. Three examples can be made: destruction of property, employment of a logic bomb and state's failure to prevent a cyber attack[179].

The first one refers to cyber attacks that destroy properties but do not kill human beings. The Stuxnet attack is a prime example: Iranian nuclear centrifuges were destroyed by means of a virus but anyone was killed. From a legal point of view, if the destruction of property is serious, it can constitute an act of armed force and the victim can react using

[175] Ibidem, p.57
[176] Ibidem, p. 58
[177] Ibidem, p. 59
[178] Ibidem, pp. 58-59
[179] Ibidem, pp. 61-63

military force in self-defence[180]. However, the non-lethal destruction[181] does not provide a just cause for war because, as stated in the paragraph above, preventing a destruction of objects by planning to use lethal military violence is impossible. A destruction of property can satisfy the just cause requirement if it represents a part of a plan, for instance a plan of invasion, whose aim is killing human beings. In this case, the attacked country can employ the lethal military violence in response.

The second example refers to the ambiguous status of logic bombs. A logic bomb consists of "a piece of code inserted into a software system that can lie dormant and undetected for extended periods of time but that can be activated to perform some malicious functions"[182]. However, the presence of a logic bomb that could destroy a critical infrastructure but is not activated yet does not provide by itself a just cause for war. There has to be the destruction of an infrastructure in order to consider the logic bomb satisfying the just cause requirement.

As regards the failure of a state in preventing a cyber attack that arises from its territory, the ambiguity has not been solved yet. The relationship between China and the US can be considered to demonstrate the above stated ambiguity. On one side, Chinese hackers could launch an attack against the US without the authorization of the Chinese government. On the other side, due to the open and free Internet policy, which is a legal policy, American Internet users are free to use the Internet and could, in their turn, launch a cyber attack against another country. In both cases, understanding if cyber attacks constitute a just cause for war is difficult therefore the ambiguity remains.

1.7 National security and resilience

As emerged from the previous paragraphs, the modern world, which is a globalized world, is characterized by interdependencies and interconnections, uncertainty, vulnerabilities and new threats and challenges. In such an environment, states represent the main actors responsible for the provision of security to their people and territory. Since it is assumed that an absolute security is impossible to achieve through national

[180] Ibidem, p. 61
[181] Ibidem, p. 62
[182] Ibidem

security strategies and that a minimal level of risk exists, a new concept has been introduced in national security strategies: the concept of resilience[183]. States, therefore, because of the emerging of new threats, are following a resilient approach to national security, with the aim of building more resilient nations states, applying a resilient approach to critical infrastructures which are critical for the functioning of the society because they provide essential services for the economic and social well-being of a nation and are often the targets of new threats such as cyber threats.

In the following paragraph, all these themes will be analyzed, starting from a focus on the concept of globalization and its impact on nation states and national security, passing through an analysis of the concept of resilience and national resilience[184], concluding with a focus on the protection of critical infrastructures through resilience.

1.7.1 Nation states and national security

Starting from the nineties, the concept of globalization[185] has been increasingly used to refer to a more interconnected world, without borders, as a result of a revolution in ICT and the opening of markets. However, globalization had an impact on nation states, from a cultural, economic, social and political perspective[186]. In fact, since the creation of the welfare state after the end of the second world war, states had a central role in these areas, being responsible for the provision of the so called positive political goods[187], such as health care, education, law and order, economic opportunity, security[188].

The impact of the globalization on the role of nation states has been analyzed from three different perspectives:

- the hyperglobalists[189], as Kenichi Ohmae and Susan Strange, who argue that states, because of globalization, lose the control over territory and their sovereignty, becoming obsolete construct[190];

[183] Fjader C., *The nation state, national security and resilience in the age of globalization,* Resilience, Vol. 2, No. 2, 114-129, 2014, p. 114
[184] Ibidem
[185] Ibidem, p. 115
[186] Ibidem, p. 116
[187] Ibidem, p.115
[188] Ibidem
[189] Ibidem, p. 116

- the sceptics[191], such as Robert Gilpin and Stephen Krasner who claim that the role of the states has changed a bit but they do not consider states as victim of globalization[192];
- the transformalists[193], including Anthony Giddens, David Held and John Ruggie who do not agree with the hyperglobalist idea and believe that globalization produces a spatial reorganization of the cultural, political, economic life, impacting the role of the nation-state[194]. However, they believe that globalization does not reduce the importance of states but everything depend on the reaction of states to it[195].

In addition to the impact on the role of nation states, globalization had an impact on the traditional concept of national security[196]. This one finds its origins in the thoughts of Thomas Hobbes and Max Weber and is based on the idea that states have the monopoly of force and are responsible for the provision of security[197].

However, with the advent of globalization, new security threats[198] emerged and, as a consequence, states had to securitize also these new threats in addition to traditional threats.

Therefore, their role has grown. Among the new threats, which are usually non-military threats and preformed by non state actors[199], international terrorism, organized crime, drug trafficking[200] can be remembered but also the particular category of cyber threats, which has been previously analyzed, can be taken into consideration.

The approach followed by states in order to securitize traditional and non-traditional threats is the securitization approach, which has been analyzed by the so called Copenhagen school on the basis of the works of Buzan and Waever. Security is considered a speech act by an actor which presents an issue as an existential threat to an

---

[190] Ibidem
[191] Ibidem
[192] Ibidem
[193] Ibidem
[194] Ibidem
[195] Ibidem
[196] Ibidem
[197] Ibidem
[198] Ibidem, p. 117
[199] Ibidem
[200] Ibidem

object and suggests extraordinary measures to secure it[201]. The issue moves therefore from the realm of normal politics to the realm of security politics.[202]

However, states realized that the environment within which they had to operate was full of uncertainties due to the emergence of new threats, which were difficult to recognize and were in a continuous evolution. In that situation, despite a perfect risk management[203] the risk could never be eliminated. As a result, they had to move from the prevention of threat to the management of its impact[204]. In fact, national security strategies had to adopt a new risk-based approach[205] that was based on an important element, that of resilience. The resilience itself becomes a strategy used by states in order to provide security within a new environment where it is necessary to react to new challenges.

That framework can be applied also to the cyber issue, introducing the concept of cyber resilience. The latter is based on the idea that the risk that an IT system is hit by a cyber attack, which represents one of the new threats in the twenty-first century, is impossible to eliminate therefore the solution is focusing on the management and reduction of that risk rather than eliminating it, making that system keep functioning at a minimal level despite the attack. The result is a resilient IT system.

In chapter three, in particular in the paragraph on the EU cybersecurity strategy, the way to achieve cyber resilience will be deeply analyzed. In general, cooperation between public and private sectors, information and best practices sharing and cooperation at international level are some of the crucial aspects for the achievement of cyber resilience.

1.7.2 Resilience and national resilience

There are various definitions of the term resilience. This term was first used in the field of material sciences. In that context, the measurement of resilience consisted in how much stress a material could withstand without breaking and how long it could resist to

[201] Ibidem, p. 117-118
[202] Ibidem, p.118
[203] Collins A., *Contemporary security studies,* third edition, oxford university press, 2013, p. 373
[204] Fjader C., *The nation state, national security and resilience in the age of globalization,* Resilience, Vol. 2, No. 2, 114-129, 2014, p. 128
[205] Ibidem, p. 119

that stress before returning to its original shape[206]. Therefore, it can be said that a resilient system is a system able to function following the normal parameters even in case of disruption and recover from the shock. This means that the system is able to adapt to the new circumstances.

As regards the concept of national resilience, there are different definitions too. In fact Philippe Bourbeau analyzes three types of national resilience:

- resilience as maintenance[207], which consists in the ability to adapt in order to maintain the status quo;
- resilience as marginality[208], which consists in maintaining the existential structures while keeping the changes at the borderline;
- resilience as renewal[209], which consists in transforming the existing structures.

In general, national resilience strategies are aimed at creating resilient nations not only able to face unexpected threats but also to assure a minimum level of supply of basic services under hostile circumstances and at all times and recover from the disruption in a reasonable time, reducing the potential negative effects of the disruption on people safety and well being[210].

However, the concept of national resilience challenges the traditional role of the state in the provision of security to all citizens equally. This is because when a nation state implements a resilience strategy it accepts the idea that the absolute protection is impossible to achieve for everyone and in every circumstance, therefore it has to make choices. For example, it has to prioritize[211] the resilience of a critical infrastructure of a densely populated region over another less populated. As a result, resilience does not produce benefits for everyone but inequality[212] between regions take place.

Finally, an important thing is understanding what is the relationship between resilience and security when a state has to provide national security following the resilient approach. It is necessary to understand if resilience is an additional element to national

[206] Ibidem
[207] Ibidem, p. 121
[208] Ibidem
[209] Ibidem
[210] Ibidem, p. 128
[211] Ibidem, p. 122
[212] Ibidem

security or a complementary element to it, which would require the state to balance between them[213].

Some differences can be found between the two elements: security has a preventing and proactive nature[214] and aims at protecting citizens against threats. Therefore, from a temporal perspective, it prevents the threat to materialize and from a spatial perspective it focuses on specific objects such as people, industries, territory. On the contrary, resilience has a reactive nature[215], in fact it aims at reducing or minimizing and not preventing the impact, the disruption on critical services. Spatially, resilience refers to more complex systems therefore it is less defined. As stated above, resilience allows systems to adapt and recover from a shock rather than protecting them from disruption. It appears that both security and resilience are necessary for the new national security paradigm[216] and that states should balance between them. In fact, if resilience is a part of national security due to the fact that, when employing preventative measures is impossible, it suggests solutions for preparedness against sudden threat, also security is a part of resilience in the sense that the aim is avoiding irreparable damages and minimizing the impact of the disruption.

As previously stated, the concept of resilience is applied also to critical infrastructures, as they are crucial for the functioning of the society and therefore have to be protected against different types of threats, included cyber attacks.

1.7.3 Critical infrastructures protection and resilience

The critical infrastructure protection (CIP) is a central field in national security. Since these infrastructures are critical for the well being of a nation, as they provide essential services to people and communities, states have to protect them from disruptions and avoid a complete interruption of the supply. For this purpose, states apply resilience to critical infrastructures. According to the National Infrastructure Advisory Council (NIAC)[217], critical infrastructure resilience refers to "the ability to reduce the

[213] Ibidem
[214] Ibidem
[215] Ibidem, p. 123
[216] Ibidem
[217] The National Infrastructure Advisory Council (NIAC) provides the President with recommendation on the security of critical infrastructures and the information systems linked to them.

magnitude, impact, or duration of a disruption"[218] while resilience refers to the ability to adapt and recover from a disruptive event. A resilient critical infrastructure is characterized by three features:

- robustness which refers to the ability to keep the critical functions at a minimal level in case of disruption[219];
- resourcefulness which consists in the ability to redirect resources in order to respond to and manage a crisis[220];
- rapid recovery which refers to the ability to recover from a shock, returning to the normal condition as fast as possible[221].

As these infrastructures are privately owned and managed, when a state has to elaborate its national resilient strategy, it is difficult to understand how to integrate them into the strategy. The problem is that private owners act in business terms, with the aim of maximizing revenues[222], rather than following national security criteria. Therefore the state finds itself in front of a dilemma because it has to solve the gap between national security interests and business interests of critical infrastructures[223]. However, in building resilience into critical infrastructures, the state cannot do without considering the expertise and knowledge of much operational information possessed by the private sector and unknown to the government. A possible solution could be the public-private partnership (PPP)[224] between government and private owners, based on information and best practices sharing.

[218] Fjader C., *The nation state, national security and resilience in the age of globalization,* Resilience, vol. 2, No. 2, 114-129, 2014, p. 120
[219] Ibidem
[220] Ibidem
[221] Ibidem
[222] Ibidem, p. 124
[223] Ibidem
[224]American foreign policy interests, *Cyberpower and National Security*, 35: 45-58, 2013, p.47

CHAPTER TWO

CONCRETE EXAMPLES OF CYBER ATTACKS

2.0 Introduction

In the previous chapter, cyberspace has been described as a new domain of warfare, in addition to land, see, air and space[225]. Societies are increasingly dependent on the Internet and ICT because they base their functioning and their economic growth on them. As a consequence, they are more vulnerable to possible cyber attacks. In fact, within and through this digital arena cyber attacks against the adversary nation's critical infrastructure or IT system can be conducted, using malware, in order to cause damage and disruption.

It can be said that the first cyber attack in the history of the cyber warfare took place in 1982 when the CIA[226] using malware was able to sabotage the software of an American computerized control system that was stolen by Russians and inserted on the trans-Siberian gas pipeline[227]. As a result, the pipeline exploded. The aim of this attack was stop Russia from stealing intellectual property from other countries.

However, in the eighties computer technologies were not as advanced as those in the modern era. The attack against Estonian websites in 2007 was the first important attack against a modern network[228] and the Stuxnet attack against Iranian nuclear program in 2010 marked a new era in the cyber war[229]. Another cyber attack against a nuclear program but conducted in a different way was the Israeli attack against Syria's nuclear facility in 2007, aimed at destroy directly the enemy's facility.

---

[225] Even S. and Siman-Tov D., *Cyber warfare: concepts and strategic trends,* Memorandum No. 117, May 2012, consulted at http://mercury.ethz.ch/serviceengine/Files/ISN/152953/ipublicationdocument_singledocument/f3e19de1-bcf7-4d07-b088-f3d477b4329c/en/INSS+Memorandum_MAY2012_Nr117.pdf on 19/09/2015, p.7

[226] The Central Intelligence Agency was established in 1947 with the aim of coordinating the nation's intelligence activities and evaluating and spreading intelligence related to national security.

[227] Even S. and Siman-Tov D., *Cyber warfare: concepts and strategic trends,* Memorandum No. 117, May 2012, consulted at http://mercury.ethz.ch/serviceengine/Files/ISN/152953/ipublicationdocument_singledocument/f3e19de1-bcf7-4d07-b088-f3d477b4329c/en/INSS+Memorandum_MAY2012_Nr117.pdf on 19/09/2015, p.7

[228] Ibidem, p. 36

[229] Ibidem, p. 37

In addition to these types of cyber attacks, cases of cyber intrusion or espionage and theft of personal and important data have been performed more recently by Russia, China, North Korea and other countries targeting the Pentagon[230], the White House, the US government computer systems, Israeli websites, Canadian websites. Different hackers were involved in those attacks, including hacktivist[231] like Anonymous which usually act using the DDoS method.

Finally, when in 2014 the South Korean nuclear program was attacked by North Korean hackers, according to the president Geun-hye, an act of cyber terrorism took place or when in 2015 hackers linked to a terrorist organization like ISIS[232] were able to hack the Malaysia airlines website and the US government websites, releasing personal data of federal employees.

2.1 Estonia

Estonia represents one of the most dependent country on the Internet in the world. In fact Estonians citizens can use Internet in order to do a lot of things such as pay taxes, book a medical examination, vote. The attack against Estonian websites was conducted in the form of DDoS from a group of computers organized in botnet[233]. The targets of the attack were the websites of the government, parliament, banks, ministries which were disabled to function correctly for some days. This was the first case of a state attacking another state by means of cyber warfare[234]. However, no properties or critical infrastructures were destroyed, nor human beings killed because of the attack. Estonia

[230] The Pentagon is the symbol of the American military strength. It was built during the forties in Virginia. With its original shape and huge dimensions it hosts the US Department of Defence.

[231] The term hacktivist is a combination of the words hacker and activist and refers to a ideologically motivated person that uses malicious tools to attack a IT system for a demonstrative intent such as causing a temporary malfunctioning of the IT system attacked or damaging the image of the target. Examples of hacktivism are the DDoS attacks which are usually used by the hacktivist group Anonymous.

[232] The term ISIS stands for Islamic State of Iraq and al-Sham and is considered a terrorist organization . However experts argue that it is not a terrorist organization but it uses a terrorist tactic.

[233] A botnet is a collection of remote-controlled computers called bots that are connected to the Internet and infected by malware. These bots can be used by the person that control them remotely in a malicious way in order to launch cyber attacks.

[234] Collins A., *Contemporary security studies*, third edition, oxford university press, 2013, p. 370

suffered only economic loss. In fact scholars do not agree about the status of this attack: some argue that this was not an example of cyber war.

As regards the attribution of the attack to an author, Estonia accused Russia of being guilty because the attack was launched after the Estonian removal of a statue of a Second World War soviet soldier from the capital Tallinn to the periphery. However, due to the attribution problem typical of cyber attacks, a solid evidence for who was the attacker will not be achieved but only suspicion remains.

After the attack against Estonia, NATO[235] became more aware of the threats that could stem from the cyberspace and the necessity of improving the cyber defence of the countries members of the alliance. In fact, it signed an agreement of cooperation with Estonia aimed at helping it in case of future attacks[236]. In addition, it established the Cooperative Cyber Defence Center of Excellence (CCDCOE)[237] in Tallinn, Estonia. Exercises on cyber defence and courses on the law of cyberspace are hosted by the CCDCOE. As a result of the work of an international group of experts, the Tallinn Manual, a text on the law of cyberwarfare, was drafted in 2009 and published in 2013. Ninety five black letter rules governing cyber conflict which refer to topic such as sovereignty, state responsibility, the law of armed conflict, humanitarian law, are analyzed in the manual[238].

2.2 Georgia

In 2008, after the cyber attack against Estonian websites in 2007, Georgia too was targeted by a cyber attack conducted through the DDoS method against the government website and other websites. The Russian government was accused of being the author of

[235] The North Atlantic Treaty Organization is an alliance of countries from North America and Europe committed to achieve the goals of the North Atlantic Treaty signed on 4 April 1949.

[236] Even S. and Siman-Tov D., *Cyber warfare: concepts and strategic trends,* Memorandum No. 117, May 2012, consulted at http://mercury.ethz.ch/serviceengine/Files/ISN/152953/ipublicationdocument_singledocument/f3e19de1-bcf7-4d07-b088-f3d477b4329c/en/INSS+Memorandum_MAY2012_Nr117.pdf on 19/09/2015, p.36

[237] The Cooperative Cyber Defence Centre of Excellence is an International Military Organisation in charge of strengthening the cooperation and information sharing among NATO and its member nations and partners in the sector of cyber defence by means of research and development, consultation and education.

[238] Theohary C. and Rollins J., *Cyberwarfare and cyber terrorism: in brief*, Congressional research service, 2015, consulted at https://www.fas.org/sgp/crs/natsec/R43955.pdf on 08/10/2015, p. 5

the attack also in this case. However, the Georgian case differed from the Estonian one as the cyber attack against Georgia preempted a conventional war which consisted in the physical invasion of the country by Russian troops.

2.3 Anonymous attacked Israel

The DDoS method was used to conduct other cyber attacks such as that launched by a hacktivist group against Israel in 2012. A collective hacker called Anonymous attacked the Israeli government websites taking down some sites, deleting databases and revealing passwords and e-mail addresses[239]. The attack against Israel was a form of protest used by Anonymous in response to the brutal Israeli behavior against Palestinians of the Gaza strip. Israel in fact had hit Gaza with aerial strikes during the preceding weeks. The cyber campaign launched against Israel, called OpIsrael[240], was something more than a DDoS: in fact hackers penetrated any vulnerable targets[241], compromising private data of Israeli citizens and supporters. In addition, Anonymous posted on the web a new threat: it warned Israel that November 2012 would have been a month to remember because there would be a cyber war[242]. What emerged from those events was that Anonymous cyber capabilities were evolving and improving.

2.4 Arab-Israeli cyber war

The cyberspace, with respect to the ground, represents an additional domain of warfare where the historical series of Arab-Israeli conflicts is fought. In 2012 in fact a cyber war between these two countries took place. The reason of the mutual attacks, which appeared to be work of civilians rather than governments[243], was based on old hostilities

[239] Sutter J., *Anonymous declares 'cyberwar' on Israel*, CNN, consulted at http://edition.cnn.com/2012/11/19/tech/web/cyber-attack-israel-anonymous/ on 9/10/2015
[240] Ibidem
[241] Ibidem
[242] Ibidem
[243] Marquardt A., *Latest Arab-Israeli conflict is growing cyberwar*, ABC News, consulted at http://abcnews.go.com/blogs/headlines/2012/01/latest-arab-israeli-conflict-is-growing-cyberwar/ on 9/10/2015

related to the Arabian and Israeli claim of territories in the Arabian peninsula. On one hand, "pro-Palestinian hackers attacked the website of Israel's anti-drug authority"[244] redirecting users to a page were gunmen wearing masks and phrases such as "Death to Israel" and "Gaza hackers were here"[245] appeared. On the other hand, a Israeli hacker group called Israeli Defence Force (IDF)[246] launched a DDoS attack against the websites of the Arab Bank of Palestine, the Central Bank of the United Arab emirates, the websites of the Saudi Arabia and Abu Dhabi stock exchanges[247]. These events took place after that a hacker called "0xomar"[248] from Saudi Arabia published online the numbers of thousands of Israeli credit cards in protest against the Israeli killing of Palestinian people. In addition, the same hacker together with a group called "Nightmare"[249] hacked the websites of the Israeli national airline El Al and the Tel Aviv stock exchange[250].

2.5 Anonymous attacked Canada

The previously cited hacktivist group Anonymous launched a cyber attack against Canadian government websites using its typical DDoS method in 2015. It was not the first time Anonymous launched cyber attacks against Canada. In 2012 it hacked the Grand Prix's website stealing and distributing personal information of ticket buyers in response to the approval of the Bill 78[251] by the Quebec government[252]. In 2011 Anonymous threatened to release the names of the four boys accused of raping Rehteah Parsons[253] before she killed herself[254]. In 2015 the hacktivist group threatened to release

[244] Ibidem
[245] Ibidem
[246] Ibidem
[247] Ibidem
[248] Ibidem
[249] Ibidem
[250] Ibidem
[251] The Bill 78 officially entitled "An act to enable students to receive instruction from the postsecondary institutions they attend" was an emergency law approved in 2012 in response to students protests against tuition hikes.
[252] Armstrong J., *Canadian issue a hot topic for hacker group Anonymous*, Global news, consulted at http://globalnews.ca/news/2060420/canadian-issues-a-hot-topic-for-hacker-group-anonymous/ on 11/10/2015
[253] Rehteah parsons was a Canadian girl who killed herself at the age of 17 because her rapers put on the internet her photos and wrote brutal phrases against her.

the names of the boys involved in the "class of dds 2015 gentleman"[255] case. The latest cyber attack in 2015 was launched by the group against government websites of Canada taking them down for a period in protest against the approval of the bill c-51[256] because it represents a violation of human rights. Among the websites hacked the website of Foreign Affairs, Transport Canada, Citizenship and Immigration and Justice Canada can be remembered[257].

2.6 Stuxnet

As previously stated, the Stuxnet attack against Iran marked a new era in cyber war because it was the first time that a cyber attack conducted by means of the cyberspace had an effect on the physical world, damaging a physical target connected to the cyberspace. In 2010 the Symantec[258] reported that the Siemens SCADA systems[259] that controlled Iranian nuclear processes have been attacked by a computer worm that was inserted in 2009 exploiting at least four unknown zero-day vulnerabilities[260]. As a result, Iranian nuclear centrifuges were damaged and the production of Highly Enriched Uranium (HEU) was delayed.

The Stuxnet attack differed from other cyber attacks because it was based on the use of a highly sophisticated tool[261] against a specific target. On the contrary, the attacks

---

[254] Armstrong J., *Canadian issue a hot topic for hacker group Anonymous,* Global News, consulted at http://globalnews.ca/news/2060420/canadian-issues-a-hot-topic-for-hacker-group-anonymous/ on 11/10/2015

[255] The class of dds 2015 gentleman is the name of a facebook page in which male dentistry students of the Dalhousie university wrote sexually violent comment against female students of the Halifax university.

[256] The bill c-51 is an anti-terrorism bill whose title is: An Act to enact the Security of Canada Information Sharing Act and the Secure Air Travel Act, to amend the Criminal Code, the Canadian Security Intelligence Service Act and the Immigration and Refugee Protection Act and to make related and consequential amendments to other Acts.

[257] Minsky A., *'Anonymous' claims responsibility for cyber attack that shut down government websites*, Global News, consulted at http://globalnews.ca/news/2060036/government-of-canada-servers-suffer-cyber-attack/ on 11/10/2015

[258] The Symantec is a security company born in the eighties in the US involved in the production of software to protect the security of computers from cyber threats.

[259] The Siemens' supervisory control and data acquisition systems are used to control and monitor industrial processes.

[260] Brantly A., *Cyber actions by state actors: motivation and utility*, International journal of intelligence and counterintelligence, 27: 465-484, 2014, p. 479

[261] Even S. and Siman-Tov D., *Cyber warfare: concepts and strategic trends,* Memorandum No. 117, May 2012, consulted at

performed by Russia against Estonia and Georgia were based on less sophisticated tools and were not directed against a specific target.

In 2010 Israel and the US appeared to be the actors behind this attack. Furthermore, in 2012 it was discovered that the Stuxnet attack against Iranian nuclear facilities was part of a series of cyber attacks against Iran called Olympic games[262].

2.7 Israel's cyber attack against Syria's nuclear facility

Another example of cyber war was the Israel's cyber attack against Syria's nuclear facilities in 2007. Israeli cyber warriors sabotaged the Syrian air defence system and, as a consequence, Israeli air force bombers were able to fly in the Syrian sky with the aim of bombing the Syria's nuclear facility without being intercepted.

However, if on one hand some scholars argue that this type of cyber attack and the Stuxnet attack represent examples of cyber war because of the kinetic effect, on the other hand, Thomas Rid argues that, because of the absence of lethality, these types of cyber attacks do not constitute a cyber war.

2.8 Stuxnet-style cyber attack[263] against North Korea's nuclear program

At the same time Iranian nuclear program was being attacked by the Stuxnet virus in 2009, the US attacked North Korea's nuclear weapon program with a similar cyber attack based on the same virus. The US thought to implement a similar attack against North Korea as the centrifuges there, like those in Iran, were probably controlled by software developed by Siemens that runs on Microsoft operating system. The Stuxnet virus in fact took advantage of the vulnerabilities of both Siemens and Microsoft

---

http://mercury.ethz.ch/serviceengine/Files/ISN/152953/ipublicationdocument_singledocument/f3e19de1-bcf7-4d07-b088-f3d477b4329c/en/INSS+Memorandum_MAY2012_Nr117.pdf on 19/09/2015, p.38

[262] Brantly A., *Cyber actions by state actors: motivation and utility*, International journal of intelligence and counterintelligence, 27: 465-484, 2014, p. 479

[263] William M., *North Korea threatens cyber attacks on US*, PC world, consulted at http://www.pcworld.com/article/2933672/north-korea-threatens-cyber-attacks-on-us.html on 11/10/2015

programs. However, it was an unsuccessful[264] attack as the Stuxnet virus was not able to penetrate the North Korea's nuclear computer network. In addition, in North Korea there was not uranium but plutonium and this one did not require an enrichment process depending on the centrifuges that would have been an important target for Stuxnet. Therefore there were some differences between Iran and North Korean nuclear programs that caused the failure of the second attack.

2.9 North Korean cyber attack against the US

Five years after the Stuxnet-style attack against North Korea's nuclear program, in 2014 the company Sony Pictures received a cyber attack with devastating consequences: the IT system was disabled, workstations were destroyed and personal data and emails were released. The Federal Bureau of Investigation (FBI)[265] argued that North Korea was behind that attack. However, the latter denied any involvement in the attack praising a hacktivist group called "Guardians of peace" for the "righteous deed"[266]. That was not the first time North Korea attacked the US: it previously launched cyber attacks against the US government agencies. In response to the Sony hack, the US president Barack Obama announced that North Korea will continue to receive sanctions aimed at isolating ever more the country. More in specific, thirteen North Korean entities, ten individuals and three organizations[267] were sanctioned. This US policy against North Korea started some years before against its nuclear program. However, the sanction policy implemented by the Obama administration seems to be weak. The US should defend better the security of the cyberspace, take additional measures in order to punish North Korea and return it to the terrorism list as it represents a threat to the national security and economy of the US. If the US fails in its commitment to respond to threats

[264] Ibidem

[265] The Federal Bureau of Investigation is a national security organization with intelligence and law enforcement tasks. It is in charge of protecting the United States from terrorist and foreign intelligence threats, enhancing the criminal laws of the United States and providing criminal justice services to federal, state and international agencies.

[266] Theohary C. and Rollins J., *Cyberwarfare and cyber terrorism: in brief*, Congressional research service, 2015, consulted at https://www.fas.org/sgp/crs/natsec/R43955.pdf on 08/10/2015, p. 1

[267] *Klingner B., The U.S. Needs to Respond to North Korea's Latest Cyber Attack* , the Heritage foundation, consulted at http://www.heritage.org/research/reports/2015/03/the-us-needs-to-respond-to-north-koreas-latest-cyber-attack on 9/10/2015

and cyber attacks received, it will only encourage Pyongyang to continue its behavior[268].

In response to the sanctions received, North Korea threatened the US of a future Korean-style cyber war aimed at causing the US final ruin[269]. In addition, it warned that these sanctions would only make things worse as North Korea would improve its military force, including nuclear program[270].

President Obama referred to the Sony attack as an act of cyber vandalism while other used the term cyber war[271].

2.10 Cyber attacks against South Korea's nuclear program

Similar to the attack perpetrated by North Korea against Sony pictures, in 2014 North Korea attacked South Korea's nuclear facilities. These two attacks are similar because both are directed against civilian targets and both are accompanied by threats of violence and extortion of money[272]. The Korea Hydro and Nuclear Power Company[273] was the target of the attack and reported that its computer systems were violated and that information were revealed including blueprints of nuclear reactors. South Korea had already been attacked by North Korea with cyber attacks targeting websites of government agencies, banking sites, business, the presidential blue house but, as stated by the South Korean president Park Geun-hye, the attack against the nuclear facility represented an example of cyber terrorism since "nuclear power plants directly impact the safety of the people"[274] and the attack was accompanied by threats.

Like the US, South Korea too has to respond to the cyber attacks received in an appropriate manner. While the US reacted imposing sanctions against North Korea,

[268] Ibidem
[269] William M., *North Korea threatens cyber attacks on US,* PC world, consulted at http://www.pcworld.com/article/2933672/north-korea-threatens-cyber-attacks-on-us.html on 11/10/2015
[270] BBC News, *Sony cyber-attack: North Korea calls US sanctions hostile*, consulted at http://www.bbc.com/news/world-asia-30670884 on 9/10/2015
[271] Theohary C. and Rollins J., *Cyberwarfare and cyber terrorism: in brief*, Congressional research service, 2015, consulted at https://www.fas.org/sgp/crs/natsec/R43955.pdf on 08/10/2015, p. 1
[272] Klingner B., *The U.S. Needs to Respond to North Korea's Latest Cyber Attack* , the Heritage foundation, consulted at http://www.heritage.org/research/reports/2015/03/the-us-needs-to-respond-to-north-koreas-latest-cyber-attack on 9/10/2015
[273] Ibidem
[274] Ibidem

what South Korea should do is revoking the economic joint venture with North Korea as this one did not respect the contract. In addition, the main aim of the joint venture, which consisted in moderating the North Korean threatening behavior and reforming its politics and economy, failed.

The two examples of cyber attacks perpetrated by North Korea against the US and South Korea are a demonstration of its advanced cyber capabilities. Experts argue that it is surpassed only by the US and Russia in the cyber field.

2.11 Russian cyber attack against the White House

Russia is one of the countries that, in addition to North Korea, launched some cyber attacks against the US. In 2015 Russian hackers were able to penetrate the White House computer systems and access the president's schedule[275]. Experts argue that the cyber intrusion began when hackers entered into the State Department networks and from a State Department account sent a phishing email[276] to the White House computer systems[277]. Therefore "hackers had access to sensitive information such as non-public details of the president's schedule"[278]. As stated by Ben Rhodes, president Obama deputy national security adviser, intruders did not compromise the classified system.

2.12 Russian cyber attack against the Pentagon

Another important target of Russian cyber attacks was the Pentagon computer system. In 2015 Russian hackers hacked the Pentagon's Joint Staff unclassified email system with a "sophisticated cyber attack"[279]. Officials claimed that the attack was so

[275] Perez E. and Prokupecz S. *How the U.S. thinks Russians hacked the White House*, CNN politics, consulted at http://edition.cnn.com/2015/04/07/politics/how-russians-hacked-the-wh/ on 8/10/2015

[276] A phishing attack consists in manipulating victims to open a file attachment or clicking on a link embedded in an email in order to give access to the phisher to sensitive data and personal information or credentials and entering deeper into an organization website. The attack is distributed en masse.

[277] Perez E. and Prokupecz S. *How the U.S. thinks Russians hacked the White House*, CNN politics, consulted at http://edition.cnn.com/2015/04/07/politics/how-russians-hacked-the-wh/ on 8/10/2015

[278] Ibidem

[279] Paganini P., *Another computer system at the Pentagon has been hacked*, Security Affairs, consulted at http://securityaffairs.co/wordpress/40039/cyber-crime/pentagon-hacked-again.html on 7/10/2015

sophisticated that it was clearly work of a nation state. The method used to conduct the attack was the spear-phishing method[280], similar to the phishing one used to access the White House computer networks. The cyber intrusion affected personal data of about 4000 military and civilian personnel working at the Joint Staff[281]. The classified system was not hit. After the attack, the Pentagon decided to take the unclassified email system down for several days.

2.13 Chinese cyber attack against the OPM

In 2014 the White House was targeted by cyber attacks not only from Russian but also Chinese hackers. In specific, the Office of Personnel Management (OPM) of the White House was hacked. The intrusion compromised personal information of about 20 million people including 4 million federal employees who had to give these type of information to the agency so as to obtain security clearances[282]. Authorities suspected that Chinese hackers were able to obtain electronic credentials of an employee at private firm KeyPoint Government Solutions[283] and used them to access legitimately the OPM computer system[284]. China denied any involvement in this cyber attack arguing that it has been a victim of cyber attacks in its turn.

China and Russia are considered by the US intelligence community the "nation states with highly sophisticated cyber programs"[285]. The cyber attacks against the White House and the Pentagon launched by the two countries make clear the fact that hackers are increasingly able to penetrate the highest levels of the US government. The latter is

[280] The spear phishing attack is the advanced version of the phishing one and it is more sophisticated and elaborated. The goal and the method are the same but it is implemented toward specific individuals within an organization

[281] Paganini P., *Another computer system at the Pentagon has been hacked*, Security Affairs, consulted at http://securityaffairs.co/wordpress/40039/cyber-crime/pentagon-hacked-again.html on 7/10/2015

[282] Shinkman P., *Reported Russian Cyber Attack Shuts Down Pentagon Network*, US News, consulted at http://www.usnews.com/news/articles/2015/08/06/reported-russian-cyber-attack-shuts-down-pentagon-network on 12/10/2015

[283] The Keypoint government solutions is a US private company which provides investigative services to different US federal government organizations regarding civilian, defence and intelligence field.

[284] Levine M., *OPM Hack: Top Lawmaker Says US 'Under Attack'* , ABC News, consulted at http://abcnews.go.com/Politics/opm-hack-top-lawmaker-us-attack/story?id=31797366 on 12/10/2015

[285] Martinez L., *Russia is main suspect in cyber attack on joint staff's emails, US official says*, ABC news, consulted at http://abcnews.go.com/Politics/russia-main-suspect-cyber-attack-joint-staffs-emails/story?id=32939784 on 12/10/2015

not the only target of cyber threats since several reports state that cyber attacks are growing in number and frequency against financial sector, health-care and IT industries[286].

2.14 Cyber terrorism

As with cyber warfare, a definition for the term cyber terrorism is difficult to find because there is not a consensus of what constitute cyber terrorism[287]. However, it can be said that cyber terrorism is "an act of terrorism that occurs in or through cyberspace"[288]. Therefore, once the meaning of terrorism is clear, then it can be included in the cyber field. According to the United Kingdom legislation, in the Terrorism Act 2000 a definition of terrorism is given: terrorism refers to an action or threat of action aimed at affecting or intimidating the population or a part of it. In addition terrorism refers to an action or threat of action performed in furtherance of political, religious or ideological objectives. The action should entail serious violence against a person, serious damage to properties or serious risk for health and safety of the population or a part of it[289]. Since computers play a crucial role in cyber terrorism, this one could be defined as: "Unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyber terrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, plane crashes, water contamination, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyber

[286] Moises N., *Cyber war puts democracies on the defensive,* Defesanet, consulted at http://www.defesanet.com.br/en/e_ciber/noticia/19585/Cyber-War-Puts-Democracies-on-the-Defensive/ on 12/10/2015

[287] Theohary C. and Rollins J., *Cyberwarfare and cyber terrorism: in brief*, congressional research service, 2015, consulted at https://www.fas.org/sgp/crs/natsec/R43955.pdf on 08/10/2015, p. 9

[288] Even S. and Siman-Tov D., *Cyber warfare: concepts and strategic trends,* Memorandum No. 117, May 2012, consulted at http://mercury.ethz.ch/serviceengine/Files/ISN/152953/ipublicationdocument_singledocument/f3e19de1-bcf7-4d07-b088-f3d477b4329c/en/INSS+Memorandum_MAY2012_Nr117.pdf on 19/09/2015, p.43

[289] Centro studi per la pace, *La definizione di terrorismo internazionale e gli strumenti giuridici per contrastarlo,* consulted at http://www.studiperlapace.it/view_news_html?news_id=20050219140025 on 13/10/2015

terrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not"[290]. From this perspective, it seems that an act of cyber terrorism attributable to non-state actors has never taken place but it could be a hypothesis for the future. In fact, terrorist organizations such as Al-Qaeda[291] use the cyberspace only for propaganda or communicate with the members of the organization or with other terrorist organizations[292]. These types of organization do not conduct attacks through the cyberspace for different reasons. For example, they do not possess sufficient cyber capabilities to cause huge damage; in addition, terrorists prefer real and not virtual terrorism[293]. Finally, terrorists avoid acting within the cyberspace because of the possibility of a change of its rules.

However, as previously stated, the North Korean attack against nuclear plants in South Korea in 2014 was considered by the President Park Geun-hye an act of cyber terrorism since hackers threatened of violence South Korean people whose safety was endangered as a result of the attack.

Another possible example of cyber terrorism could be the hack of the Malaysia airlines website in 2015 by a group called Lizard Squad which self-describes as "Cyber Caliphate" and seems to be linked to ISIS[294]. Visitors of the website were redirected to a page where the words "404-plane not found. Hacked by Lizard Squad"[295] appeared. At the beginning in the browser tab the words "ISIS will prevail" also appeared[296]. The Malaysia airlines affirmed that its website was compromised but customers data and booking were not. This event should be a demonstration of the fact that terrorists are increasingly using cyber technologies to attack adversaries.

In 2015 ISIS, and in particular the Islamic State hacking Division, was involved in another hack, that of the US government websites. The hacking group linked to the

---

[290] Gordon S. and Ford R., *Cyberterrorism?*, Symantec, consulted at https://www.symantec.com/avcenter/reference/cyberterrorism.pdf on 13/10/2015, p . 4

[291] Al-Qaeda is a terrorist organization of extremist Muslims organized by Osama bin Laden with the aim of spreading Western ideas to influence the Muslim countries.

[292] Even S. and Siman-Tov D., *Cyber warfare: concepts and strategic trends,* Memorandum No. 117, May 2012, consulted at http://mercury.ethz.ch/serviceengine/Files/ISN/152953/ipublicationdocument_singledocument/f3e19de1-bcf7-4d07-b088-f3d477b4329c/en/INSS+Memorandum_MAY2012_Nr117.pdf on 19/09/2015, p.43

[293] Ibidem

[294] BBC News, *Malaysian airline websites compromised by hackers*, consulted at http://www.bbc.com/news/world-asia-30978299 on 14/10/2015

[295] Ibidem

[296] Harjani A., *Malaysia airline says website not hacked*, CNBC, consulted at http://www.cnbc.com/2015/01/25/malaysia-airlines-site-hacked-by-cyber-caliphate.html on 14/10/2015

terrorist organization ISIS released on the web a "chilling hit list"[297] which contained personal data of more than one thousand military and government personnel, including credit card numbers, phone numbers, computer passwords, e mail. Furthermore, personal information of Australian people like Australian defence force employees, a Victorian MP, Australian National Audit office employees[298] were released. People whose personal information have been published fear for the safety of their families. However, it seemed that the Islamic State Hacking Division received the personal information of the US military and federal employees contained in the hit list from a terrorist hacker member of the Kosova Hacker Security (KHS)[299]. Ardit Ferizi is the young man who, together with the other members of the Kosovar hacking group, hacked the US government network and then shared with the Islamic hacking group the information stolen, contacting the leader of the group named Junaid Hussein[300]. Consequently, Hussein was killed in Raqqa by the US military in a drone strike as part of a campaign aimed at taking down the terrorist group leadership. According to a US official, this event represented a "great intelligence success"[301]. On the contrary, Ferizi was arrested in Malaysia where he went to study computer science.

2.15 Summary of the cases

The following table represents an attempt to categorize the examples of cyber attack just described in order to help the reader finding a link between what has been stated in the first theoretical chapter and what has been stated in this practical chapter. However, if the term cyber war is used to refer to "any type of conflict with a cyber component"[302],

[297] Mail online, *Islamic State's chilling hit list: Terror group hacks personal details of hundreds of military, political and diplomatic personnel and posts them online urging local extremists to kill them… including EIGHT Australians*, consulted at http://www.dailymail.co.uk/news/article-3195139/The-chilling-ISIS-hitlist-Terror-group-hacks-publish-personal-details-hundreds-military-political-diplomatic-personnel-urges-local-extremists-kill-including-EIGHT-Australians.html on 15/10/2015

[298] Ibidem

[299] RT question more, *'Terrorist hacker' from Kosovo faces charges for giving US troops' IDs to ISIS*, consulted at https://www.rt.com/news/318825-terrorist-hacker-kosovo-arrested/ on 14/10/2015

[300] Junaid Hussein, also known as Abu hussain al-britani, is a british hacker who works for ISIS.

[301] Bennet J., *ISIS Hacker That Exposed US Troops In US Killed By Drone Strike* , the Daily caller, consulted at http://dailycaller.com/2015/08/27/isis-hacker-that-exposed-us-troops-in-us-killed-by-drone-strike/ on 15/10/2015

[302] Collins A., *Contemporary security studies*, third edition, oxford university press, 2013, p. 372

all the examples of cyber attacks described here are a demonstration of the fact that the cyberspace represents a new domain of war, therefore could be categorized under the category of cyber war.

Table of cases

Cyber terrorism	• North Korean attack against the South Korean nuclear plant "Korea Hydro and Nuclear Power Company" in 2014, which was considered an act of cyber terrorism by the South Korean President Park Geun-hye ; • North Korean attack against the Sony Pictures company in 2014 (however, it was considered an act of cyber vandalism by the US President Barack Obama); • Hack of the Malaysia airlines website in 2015 by the group Lizard Squad linked to ISIS; • Hack of the US government websites by the Islamic State hacking Division.
Hacktivism	• Anonymous attack against Israeli government websites in 2012; • Anonymous attack against Canadian government websites in 2015.
Cyber crime (cyber intrusion aimed at compromising personal data)	• Chinese attack against the computer systems of the OPM at the White House in 2014; • Russian attack against the computer systems of the White House in 2015; • Russian attack against the Pentagon computer system in 2015.
Cyber crime (cyber attacks conducted against computer networks in order	• Russian attack against Estonian websites in 2007, considered the first case of a state hitting another using cyber-warfare; • Russian attack against Georgian websites in 2008;

to disable their functioning)	• Arab-Israeli mutual cyber attacks against their websites in 2012.
Cyber attacks performed through the cyberspace in order to damage a physical objective	• Stuxnet attack against Iranian nuclear program launched by the US and Israel in 2010, signed a new era in cyber war as it was the first case of cyber attack aimed at destroying a physical objective; • Israeli attack against Syria's nuclear facility in 2007; • Stuxnet-style attack perpetrated by the US against North Korean nuclear facility in 2009.

CHAPTER THREE

CYBERSECURITY IN THE EUROPEAN UNION

3.0 Introduction

As emerged from the previous chapters, the modern era is characterized by nations that are increasingly dependent on ICT and the Internet from the economic and social perspectives. Everything, from the health sector to schools, transportations, energy and water supply, industries, military sector is controlled by IT systems. People every day access the Internet in order to enjoy the services offered such as on-line payments, booking or simply consult their Facebook profile. However, if on one hand benefits like growth and competitiveness derive from the introduction of new technologies into economies and the daily lives of individuals, on the other hand this trend make societies increasingly vulnerable as the more they rely on ICT the more they are exposed to the risk of cyber attacks. Therefore, a more secure cyberspace is needed in order to protect societies and economies, allowing them to grow and remain competitive, but also private citizens' data and privacy. States emerge as the main actors responsible for the creation and maintenance of a secure cyberspace.

The concept of cybersecurity, and in particular the European Union's (EU) vision about it, will be the focus of this chapter. The main aspects that characterize the EU and member states' policies in the cybersecurity field are the fight against the cyber crime and the protection of critical infrastructures[303]. From a European perspective, the first strategic and global document on cybersecurity ever realized by the EU was the "Cyber security Strategy of the European Union: An Open, Safe and Secure Cyberspace"[304], proposed by the EU Commission and the High Representative of the Union for Foreign Affairs and Security Policy Catherine Ashton the 7th February 2013. This document

[303] The fight against cyber crime and the protection of critical infrastructures are the two priorities in the cybersecurity field discussed in the Communication on cyber crime elaborated by the EU Commission in 2000.

[304] European Union, Joint communication to the European parliament, the council, the European economic and social committee and the committee of the regions, *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, consulted at http://eeas.europa.eu/policies/eu-cyber-security/ on 16/10/2015

represented only the last part of a path on the topic of cybersecurity started at the beginning of the Twenty-First Century by the EU. However, despite the presence of a definition of cybersecurity[305] in the EU strategy of 2013, it can be said that once analyzed the different strategic documents on cybersecurity at a national, European and international level a lack of shared definitions of the term emerges. In addition, a reference to the cyber war as distinct matter is absent in the European approach to cybersecurity. The term cyber war is never mentioned directly.

3.1 EU cybersecurity strategy: an open, safe and secure cyberspace

From the EU cybersecurity strategy the EU's vision about the topic of cybersecurity, the actions required on the basis of a strong protection of citizen's fundamental rights and the roles and responsibilities of the main actors involved emerge in order to make the EU digital domain the safest in the world[306]. The strategic document is divided into three parts: the first part refers to the previous cited impact of the Internet on every aspects of societies and the increasing reliance on cyberspace and the principles which lay the foundations for the cybersecurity sector; the second part refers to the strategic priorities necessary in order to enhance the EU's performance in the cybersecurity area; the third part refers to the roles and responsibilities at a national and European level.

3.1.2 The cyberspace and the principles for cybersecurity

The cyberspace is depicted as open and free: people and communities can interact among each other and share information and ideas through the Internet as no barriers exist among countries. ICT and the Internet are necessary for a nation to be prosperous and competitive. However, a nation can maintain its prosperity if the cyberspace is not

[305] According to the EU cybersecurity strategy, the term cybersecurity refers to the actions undertaken to protect the digital domain, both in the civil and military areas, from the possible threats that could cause damage to the information infrastructures and interconnected networks, assuring their integrity and functionality together with the protection of the private information stored therein.

[306] European Union, Joint communication to the European parliament, the council, the European economic and social committee and the committee of the regions, *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, consulted at http://eeas.europa.eu/policies/eu-cyber-security/ on 16/10/2015, p. 3

only free and open but also secure. In fact different threats could stem from the cyberspace such as criminal, politically motivated, terrorist or state sponsored attacks. Therefore cyberspace has to be protected from malicious activities and governments play a key role in making this digital domain secure. The aim of the EU cybersecurity strategy is assuring an open, free and secure cyberspace on the basis of the application, in the digital domain, of the same norms and rules that are applied in the physical world such as fundamental rights, democracy and rule of law[307]. Only if the so called "core values"[308] are respected, the cybersecurity can be achieved. First, fundamental rights, personal data and privacy have to be respected in the digital domain together with the freedom of expression. Second, the access to the Internet should not be limited but everyone should have the possibility to access to it and to the huge flow of information. Third, the EU supports a democratic and multi-stakeholder governance of the Internet as there are several entities, commercial and non-governmental, involved in the management of it. Finally, making the cyberspace secure is a responsibility that all actors involved, from the public sector to the private one and citizens, should share, implementing actions to protect themselves or cooperate to enhance cybersecurity.

3.1.3 Strategic priorities

Five actions that derive from five strategic priorities[309] are described as necessary for the EU to enhance its performance in providing a free and secure digital environment. The five strategic priorities are: achieving cyber resilience, drastically reducing cyber crime, developing cyberdefence policy and capabilities related to the Common Security and Defence Policy (CSDP), develop the industrial and technological resources for cybersecurity, establish a coherent international cyberspace policy for the EU and promote core EU values[310].

- **Cyber resilience**: The EU suggests public and private sectors to cooperate effectively so as to achieve the cyber resilience, which is a concept that has been

[307] Ibidem, p. 2
[308] Ibidem, p. 3
[309] Ibidem, p. 4
[310] Ibidem, pp. 4-5

already analyzed in the first chapter. Both public and private sectors should strengthen their resources and capabilities to prevent, identify and manage cybersecurity incidents. Since there are some gaps in the EU as regards national capabilities, sharing of information in case of cyber incidents and the readiness and involvement of the private sector in the cybersecurity field, the strategy proposes a legislation aimed at: establishing common minimum requirements for Network and Information Security (NIS) at a national level[311] which means that Member States have to design NIS competent authorities and establish National Computer Emergency Response Teams (CERTs)[312]; fostering cooperation, mutual assistance and information sharing among the national NIS competent authorities; improving the readiness and involvement of private actors in the field of cybersecurity as the majority of IT systems and infrastructures are owned by them. The private sector should develop its cyber resilience capabilities and share best practices within the sector. However, private actors are not incentivized to invest on security nor to adopt a risk management culture or provide data about cybersecurity incidents. The legislation aims to assure that all these facts take place and focuses on the importance of the mechanism of the incident reporting[313], in which ENISA is deeply involved. The public-private cooperation and sharing of information and best practices is very important in the cybersecurity field. In fact in 2009 the European Public-Private Partnership for Resilience (EP3R)[314] was developed by the EU Commission. In addition, the cooperation could be stimulated by the establishment of cyber incident exercises, which will be described hereafter.

[311] Ibidem, p. 5

[312] CERTs are organizations established in order to give responses to IT emergencies , financed by universities, big companies, governmental entities and composed of experts of the IT sector involved in providing support in case of cybersecurity incidents and in activities of prevention, training and monitoring.

[313] Since 2012, ENISA publishes every year a report which provides an analysis of the security incidents which have been reported to ENISA and the Commission. Up to now, four report have been published entitled "annual incident report 2011,2012,2013,2014" that presented the security incidents that took place during the previous year and that caused interruptions of electronic communication networks, services and interruptions in the field of fixed and mobile telephony.

[314] The EP3R was established in 2009 by the EU Commission in the context of CIIP. It represented an attempt to address, at European level, the issue of the resilience of critical information infrastructures on the basis of the public-private partnership. In particular, it encourages the information sharing and the identification and adoption of standards for security and resilience in Europe. The Commission requires ENISA to support the EP3R system.

What emerges from the EU cybersecurity strategy is that the Commission: intends to continue its support for the development of resilient systems; would ask the European Network and Information Security Agency (ENISA) to help member states to develop their national cyber resilience capabilities[315] and to help member states and EU institutions to develop cyber incident exercises; would ask industry to share information and best practices at a sector level and with the public sector.

Finally, as previously stated, cybersecurity is a common responsibility[316] and end users are relevant actors for the provision of security to IT systems and network. Therefore end users should be made aware of the risk they can face on the Internet every day. In fact ENISA, Europol[317] and Eurojust[318] are active in raising awareness through the organization of workshops and the publication of reports. The Commission asks member states to organize every year a cybersecurity month[319] with the support of ENISA and the private sector and promote training on NIS in schools; asks industry to encourage cybersecurity awareness.

- **Reduction of cyber crime**: A strong legislation is required in order to allow the EU and the member states to fight cyber crime. The Budapest convention, which is a treaty on cyber crime, emerges as a model for the adoption of national legislation. The Commission encourages states that have not ratified the Budapest convention yet to swiftly do it. A legislation on cyber crime has been

[315] European Union, Joint communication to the European parliament, the council, the European economic and social committee and the committee of the regions, *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, consulted at http://eeas.europa.eu/policies/eu-cyber-security/ on 16/10/2015, p. 7

[316] Ibidem, p. 8

[317] Europol stands for European police office and is responsible for the creation of a safer Europe by helping EU member states in contrasting international crime and terrorism.

[318] Eurojust stands for European union's judicial cooperation unit, was established in 2002 and is involved in supporting the cooperation among judicial authorities of EU member states in fighting organized crime.

[319] At EU level, the European cyber security month (ECSM) takes place every October since 2012 when it took place as a pilot project through Europe. ENISA is one of the actors involved in the deployment of the EU campaign whose main aim is promoting the cybersecurity among citizens, the security of data, the information and good practices sharing in the cybersecurity field. Among the several objectives of the ECSM, raising the awareness about cybersecurity and in particular about NIS, promoting the use of the Internet in safety for all internet users and enhancing the interest of people about information security can be remembered.

already adopted by the EU, together with a law focused on the fight against child pornography. However, not all member states possess the capabilities to respond effectively to cyber attacks since cyber crime techniques are evolving and are becoming increasingly sophisticated. Therefore the Commission intends to support member states to enhance their operational capabilities to investigate and fight cyber crime. In addition, the EU can help member states to fight cyber crime favoring a cooperative approach among public and private stakeholders. The Commission argues that: it would support the European Cyber crime Centre (EC3) [320] which represents the reference point for the fight against cyber crime in Europe; it asks to the EC3 to help member states in fighting cyber crime in the field of sexual abuses, payment frauds and intrusion[321]; asks to Eurojust and EC3 to cooperate and share information so as to improve their efforts in fighting cyber crime; it would ask to the European police college (CEPOL)[322] to develop training courses to provide knowledge and expertise to law enforcement in order to better fight cyber crime.

- **Cyberdefence policy**: The cyber defence represents a dimension of the cybersecurity. In particular the cyber defence capabilities of detection, response and recovery[323] from cyber threats are necessary to increase the resilience of the communication and information systems that support the interests of national security and defence of the member states. Given that threats have different origins, there should be cooperation between the civilian and military field to

[320] The EC3 was established in 2013 within EUROPOL and it is responsible for promoting the share of information about cyber crime among member states and making assessment, monitoring the threats and analyzing trends and making predictions about the cyber crime issue. EC3 is mainly involved in three areas of investigation: crimes performed against EU critical infrastructures and information systems; crimes that cause serious damage to people such as child pornography on line and illegal activities performed by the organized criminality in order to make economic profit like on line fraud.

[321] European Union, Joint communication to the European parliament, the council, the European economic and social committee and the committee of the regions, *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, consulted at http://eeas.europa.eu/policies/eu-cyber-security/ on 16/10/2015, p. 11

[322] CEPOL stands for European police college and is a EU agency that was established in 2005 aimed to strengthen capabilities of law enforcement authorities in the security field, address threats like cyber crime, terrorism and drug trafficking at EU level.

[323] European Union, Joint communication to the European parliament, the council, the European economic and social committee and the committee of the regions, *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, consulted at http://eeas.europa.eu/policies/eu-cyber-security/ on 16/10/2015, p. 11

protect critical cyber assets but also between academia, public and private sectors on the basis of information sharing. In addition, to reduce time and costs and avoid double efforts, the EU highlights the importance of the cooperation with international partner like the NATO in order to enhance the resilience of critical infrastructures and ensure effective defence capabilities. The High Representative together with the member states and the European Defence Agency (EDA)[324] focus on all aspects of capability development such as doctrine, organization, personnel, training, infrastructure and logistics for an adequate and effective cyber defence[325].

- **Industrial and technological resources**: Many ICT products used in the EU are produced outside it. Therefore the EU risks to become not only more dependent on external markets but also on the security solutions that are present outside Europe. What is important is making the technological components used in critical infrastructures which are produced both in the EU and outside it more secure, reliable and that aim to protect private data. In addition, in order to achieve a high level of security, the whole value chain of ICT products in Europe should be based on security as a priority. However, since many actors do not consider security an important element, there should be more incentives, for the private sector for example, to apply more security solutions. This strategy in fact requires the establishment of platforms where public and private actors meet to discuss about the cybersecurity practices to apply to the value chain. In 2013 the Commission: launched a public-private platform on NIS solutions[326] which encourages the adoption of secure solutions and good cybersecurity performance in the ICT field; asked ENISA to realize "technical guidelines and recommendations for the adoption of NIS standards and good practices"[327]; it asked public and private stakeholders to adopt stronger security features and

[324] EDA was established in 2004 and is the main responsible for cyber defence at EU level. It supports member states in developing defence capabilities, it promotes collaboration and new initiatives to improve the EU defence.
[325] European Union, Joint communication to the European parliament, the council, the European economic and social committee and the committee of the regions, *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, consulted at http://eeas.europa.eu/policies/eu-cyber-security/ on 16/10/2015, p. 11
[326] Ibidem, p. 13
[327] Ibidem

apply them to new software and hardware and develop security labels[328] which are important for the cybersecurity performance of companies and make them more competitive. Research and development (R&D) plays a crucial role in supporting the creation of a reliable European ICT industry, supporting the internal market and reducing the EU reliance on foreign ICT products. The EU intends to use the Horizon 2020 Framework Programme for Research and Innovation[329] in order to support the security research in the field of ICT emerging technologies and develop tools to contrast criminal and terrorist activities in the cyber domain.

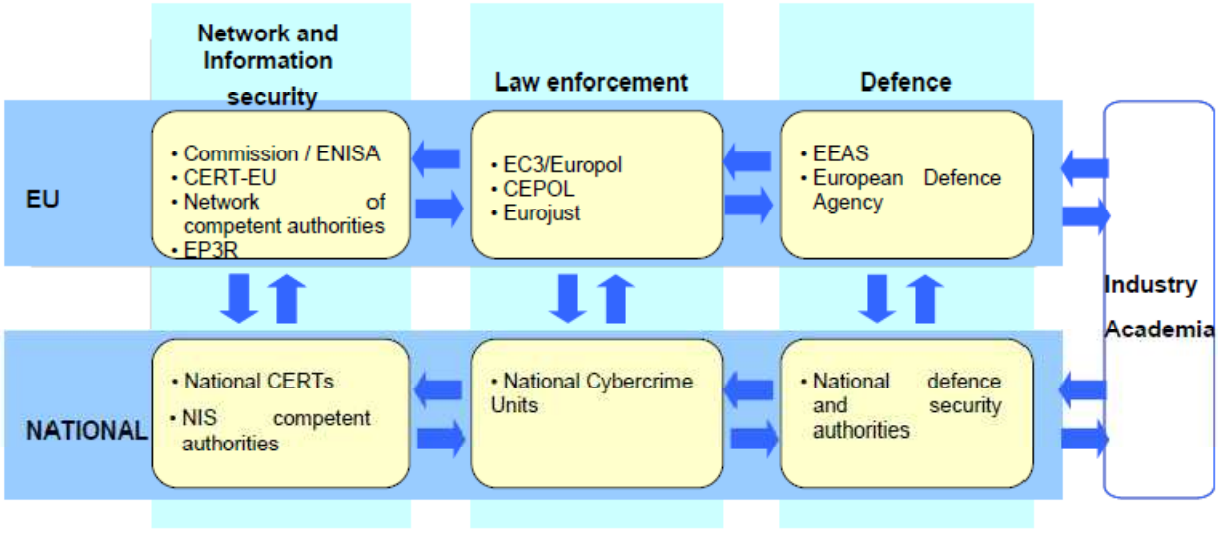
- **International cyberspace policy**: The aim of the EU cybersecurity strategy to assure an open, free and secure cyberspace can be achieved only if Europe and international partners and organizations work together. The Commission, the High Representative and the member states should elaborate the EU international cyberspace policy[330] in order to promote a stronger relationship with international partners and organizations and the private sector. The EU considers the cooperation and dialogue about cyber issues with like-minded countries and organizations like OECD, NATO, OSCE, UN, which are involved in the cyber issue, very important. The EU's core values of freedom, rule of law, democracy and human dignity[331] are at the basis of the EU international involvement in the cyber field. The EU in its international cyberspace policy puts emphasis on the fact that existing and not new international laws should be applied in the cyberspace, making a reference to the Budapest Convention as a legal instrument that could be used by third countries to contrast cyber crime and to the application of International Humanitarian Law and Human Rights law[332] when an armed conflict expands to the cyberspace. Here a reference to the cyber war seems to emerge but it is not explicit. The EU, together with international partners and organizations, supports the capacity building in third countries in order to improve the integrity and security of the Internet and fight cyber threats.

[328] Ibidem
[329] Ibidem
[330] Ibidem, p. 15
[331] Ibidem
[332] Ibidem, p. 16

As the international cooperation is of outmost importance for the good functioning of critical infrastructures, the EU is committed to strengthen the international cooperation on Critical Information Infrastructure Protection (CIIP).

3.1.4 Roles and responsibilities

The cybersecurity issue involves different actors who have to work together and take their different responsibilities at national and EU level to enhance cybersecurity. Given that a several number of actors is involved, each national government should take the responsibility to maintain a good level of cybersecurity and cooperate with the EU in case of cyber risks. The following scheme shows the organization of the structures involved in the maintenance of cybersecurity into three main areas: NIS, law enforcement, defence[333].



Source: Cybersecurity strategy of the European union: an open, safe and secure cyberspace[334]

[333] Ibidem, p. 17
[334] Ibidem

3.1.4.1 National level

At national level member states should have their national structures in each of the above mentioned areas. Each member state should establish, in its national cybersecurity strategy, the roles and responsibilities of national entities. Cooperation and information sharing at a national level and between national structures and the private sector is encouraged in order to have a better knowledge of the new trends and cyber techniques used to implement cyber attacks and respond quickly and adequately to the attacks.

3.1.4.2 EU level

At EU level, several organizations are involved in the cybersecurity issue. In the NIS area there are ENISA, established in 2004, the CERT-EU[335] and of outmost importance is the program launched by the Commission in 2009 called EP3R.
In the area of the law enforcement the EC3/Europol and Eurojust should cooperate to improve their capability in fighting cyber crime.
In the defence area the EDA is encouraged by the EU cybersecurity strategy to cooperate and share information with ENISA and Europol/EC3 and with their national counterparts.

3.1.4.3 International level

At international level the Commission, the High Representative and the member states focus on the dialogue with international partners and organizations like NATO, OECD, OSCE in the field of cybersecurity while promoting the EU's core values.

The strategy ends with a reference to major cyber attacks and invites the Commission and the member states to share information about cyber attacks. In case of an incident that seems to be linked to cyber crime, Europol/EC3 should be informed so as to start the investigation in order to identify the perpetrators. "If the incident seems to relate to

[335] The CERT-EU was established in 2012 by the EU, it is composed of experts in the IT sector and is responsible for the monitoring of threats in the cyberspace and for responding to cyber attacks against EU agencies and institutions.

cyber espionage or state sponsored attack"[336], national security and defence authorities should warn their counterparts of the fact they are under attack. In case of a serious incident, a member state can invoke the EU Solidarity Clause, notably Article 222 on the functioning of the EU[337]. If a cyber attack is directed toward personal data, national Data Protection Authorities[338] should be invoked.

In conclusion, the EU cybersecurity strategy has shown the EU's vision and the necessary actions to make the EU digital environment the safest in the world[339]. The aim can be achieved only if the EU core values are respected and only if all actors involved cooperate. The Council and the European parliament are invited to promote the strategy. Civil society and private sector are invited to give their support for the creation of a safe cyberspace.

3.2 The evolution of the European policies in the cybersecurity field

As previously stated, the EU cybersecurity strategy proposed by the Commission and the High representative in 2013 represented only the last part of a path started in 2000 by the EU on the cybersecurity issue. In the following paragraph an analysis of the relevant structures involved in the cybersecurity issue, some of which have been already cited in the previous paragraph, and the documents produced will be made.

The Commission has always played a crucial role in the evolution of the European policies on the cybersecurity issue since the beginning when it was involved in the elaboration of the first documents on this topic.

In 2001 the Commission elaborated a communication[340] focused on the NIS and its definition. The NIS is defined as "the ability of a network[341] or an information system[342]

[336] European Union, Joint communication to the European parliament, the council, the European economic and social committee and the committee of the regions, *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, consulted at http://eeas.europa.eu/policies/eu-cyber-security/ on 16/10/2015, p. 19

[337] Ibidem

[338] Ibidem

[339] Ibidem

[340] Eur-lex, *Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions - Network and Information Security: Proposal for A European Policy Approach* /* COM/2001/0298 final */, consulted at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52001DC0298 on 16/10/2015

to resist, at a given level of confidence, accidental events or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data and the related services offered by or accessible via these networks and systems"[343]. In addition to the definition of NIS, a list of threats that can have an impact on NIS is made. Six threats are described, together with the potential damage they cause and the potential solutions: interception of communication, unauthorized access to computer and computer network, network disruption, execution of malicious software that modify or destroy data, malicious misrepresentation, environmental and unintentional events[344].

- Interception of communication: it is necessary to distinguish between lawful and unlawful interception activities. The former refer to authorized interception for public security reasons. The latter refer to malicious activities intended to invade the privacy and exploit data of individuals such as credit card numbers or passwords[345].
- Unauthorized access to computer and computer network: the unauthorized access into computers is technically called intrusion. It aims to copy, modify or destroy data and can be performed in different ways[346].
- Network disruption: in the modern era it consists in disrupting attacks that exploit weaknesses and vulnerabilities of network components like routers or name servers while in the past network disruption was caused by failures in the computers that controlled the networks and attacks were directed against those computers[347].
- Execution of malicious software that modify or destroy data: software can be used in a malicious way to disable computers and modify or delete data.

[341] The term network refers to transmission systems that allow the transmission of signals by wire, radio, or other electromagnetic means, including satellite networks, terrestrial networks, electricity cable systems.
[342] The term information system includes not only computers and electronic communication networks, but also electronic data stored, processed, or transmitted by them.
[343] Eur-lex, *Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions - Network and Information Security: Proposal for A European Policy Approach* /* COM/2001/0298 final */, consulted at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52001DC0298 on 16/10/2015
[344] Ibidem
[345] Ibidem
[346] Ibidem
[347] Ibidem

Examples of malicious software are virus, that can have destructive consequences but also worms[348], logic bombs and Trojan horses[349].

- Malicious misrepresentation refers to the misrepresentation of identity which can induce people to download a malicious software from a website that appears reliable[350].
- Environmental and unintentional events: they are natural disasters that cause disruption to networks but also human errors[351].

In 2003 the European security strategy was elaborated by the Commission. Only in 2008 in the English version of the Relation on the implementation of the European security strategy the term cybersecurity emerged. In the document, the possibility that cyber attacks against private or governmental IT systems could become potential military, economic, political weapons is considered.

In 2004 the EU approved a regulation[352] that established the creation of the ad hoc structure ENISA which has its seat in Crete. Since communication networks and information systems have become crucial for the development of a nation from the economic and social perspectives, the security of those systems is increasingly important because, in case of attack, there could be negative consequences for physical infrastructures and, as a consequence, the well-being of the EU. ENISA has been established "for the purpose of ensuring a high and effective level of network and information security within the Community and in order to develop a culture of network and information security for the benefit of the citizens, consumers, enterprises and public sector organizations of the European Union, thus contributing to the smooth functioning of the internal market."[353] The Agency is a centre of expertise[354] at EU level

[348] A worm is a program that does not attack another program as virus does but makes copy of itself in order to swamp the system.
[349] A trojan horse is a program that seems benign but when opened releases a malicious attack.
[350] Eur-lex, Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions - *Network and Information Security: Proposal for A European Policy Approach* /* COM/2001/0298 final */, consulted at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52001DC0298 on 16/10/2015
[351] Ibidem
[352] Eur-lex, *Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency*, consulted at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:EN:HTML on 18/10/2015
[353] Ibidem
[354] ENISA, *Activities*, consulted at https://www.enisa.europa.eu/about-enisa/activities on 18/10/2015

which provides advice and assistance on network and information security issues to the Union institutions and the Member States[355]. The Agency intends to help the Commission, the business community and the member states to prevent, address and react to network and information security problems[356]. The Agency has other tasks such as:

- collecting information about those risks that provoke a negative impact on the resilience and availability of communication networks and on the authenticity and confidentiality of information stored and transmitted through them[357];
- supporting the cooperation among the different actors involved in the network and information security field by organizing meetings between the public and private sectors and industries[358];
- promoting information and best practices sharing and dialogue among member states and between them and UE institutions as well as between the public and private sectors[359];
- promoting of risk assessment activities and risk management solutions within the public and private sectors[360];
- developing technical guidelines for the adoption of NIS standards and good practices in the public and private sectors[361];
- contributing to the development of a culture of network and information security by supporting the EU community to cooperate with foreign countries and international organizations in order to promote a common global approach to network and information security[362].

In order to help EU member states to develop their national cybersecurity strategy the Agency published a guide entitled "National cyber security strategies. Practical guides

[355] Eur-lex, *Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency*, consulted at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:EN:HTML on 18/10/2015
[356] Ibidem
[357] Ibidem
[358] Ibidem
[359] Ibidem
[360] Ibidem
[361] Ibidem
[362] Ibidem

on development and execution"[363] in 2012. In particular, the manual provides useful recommendations to public and private stakeholders on the development, implementation and maintenance of a cybersecurity strategy[364]. The guide describes a lifecycle model for the development, evaluation and maintenance of a national cybersecurity strategy[365]. The model, which follows the Deming's Plan Do Check Act (PDCA) model for governing a cybersecurity strategy, is composed of two main phases which are deeply analyzed in the guide: one refers to the development and execution and the other to the evaluation and adjustment of the strategy[366].

Another significant effort performed by ENISA consisted in the organization of pan-European cyber crisis cooperation exercises aimed to enhance the cooperation among EU member states and gather the know-how and expertise of major experts at EU level by proposing simulations of cyber attacks in order to test their skills and give them the possibility to learn by doing. In specific, three exercises have been organized by the Agency: cyber Europe 2010, cyber Europe 2012 and cyber Europe 2014[367].

- Cyber Europe 2010 consisted in a simulation of cyber attacks that caused the loss of Internet connectivity among countries, forcing the participants to collaborate in order to avoid a complete crash[368].
- The second exercise was more complex and sophisticated with respect to the previous one and was based on recommendations and experience coming from cyber Europe 2010[369]. In addition to EU institutions and member states, it involved private actors from the industrial and information security field. The exercise consisted in a series of cyber attacks conducted in the form of DDoS attack against above all energy supply services. All participants had to cooperate using standard procedures in order to find a solution.

[363]ENISA, *National cybersecurity strategies: practical guide on development and execution*, December 2012, consulted at https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-an-implementation-guide on 18/10/2015
[364] Ibidem
[365] Ibidem
[366] Ibidem
[367] ENISA, *Cyber europe*, consulted at https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cce/cyber-europe on 19/10/2015
[368]ENISA, *Cyber Europe 2010*, consulted at https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cce/cyber-europe/ce2010 on 19/10/2015
[369] ENISA, *Cyber Europe 2012*, consulted at https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cce/cyber-europe/cyber-europe-2012 on 19/10/2015

- The third exercise took place in 2014 and for the first time the three levels of incident response were tested: technical, operational/tactical and strategic[370]. The aim of the exercise was contributing to the cooperation among participants in case of large scale cyber attacks against the security of vital infrastructures[371]. In particular, the exercise started with the proposal of a regulation on energy resources imports by EU member states which was followed by cyber attacks performed against member states and EU institutions in order to destabilize their energy market[372]. Other cyber attacks followed the first one, causing disruptions and impacting energy critical infrastructures with the aim of preventing member states to vote the regulation[373].

In general, at the end of each exercise, the best solution becomes automatically the model to address complex problems and it is made available to the other participants. In this way the expertise is shared among the participants to the exercise.

In addition the Agency is one of the actors involved in the incident reporting mechanism which is based on the fact that Internet and service providers report to competent authorities and EU institutions the attacks they received starting a mechanism of information sharing among all actors involved, aimed at providing the attacked entity with the solution. However, cyber incidents are not often made public as companies attacked fear for their imagine and reputation.

Finally, in 2013 a new regulation[374] that repealed the previous one was approved. With the new regulation the ENISA mandate is strengthened and extended until 2020 and its seat is confirmed to be in Crete. The new regulation confirmed the tasks of the Agency

[370] ENISA, *Cyber europe*, consulted at https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cce/cyber-europe on 19/10/2015

[371]ENISA, *Enisa cyber Europe 2014: after action report*, consulted at https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cce/cyber-europe/ce2014/ce2014-after-action-report on 19/10/2015 p.8

[372] Ibidem, p. 15

[373] Ibidem

[374]Official journal of the European Union, *Regulation (EU) No 526/2013 of the european parliament and of the council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004* , consulted at http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:JOL_2013_165_R_0041_01&qid=1397226946093&from=EN on 19/10/2015

described in the previous regulation and made the Agency the reference point for cybersecurity issue at EU level.

In the field of critical infrastructures, which is a topic already discussed in the first chapter, a universally definition of critical infrastructure (CI) is absent. However, this term usually refers to infrastructures whose malfunctioning produce negative effects on the well being of a nation, exposing people to security risks. At EU level, critical infrastructures are interdependent, as stated by the European Commission, therefore if a CI located in a member state is attacked, there could be a negative impact in another member state[375]. These interconnected infrastructures are thus called European critical infrastructures (ECI), defined as "critical infrastructure located in Member States the disruption or destruction of which would have a significant impact on at least two Member States"[376]. What emerges is that the protection of CI is very important and in fact in 2006 the Commission approved a communication on the European program for critical infrastructure protection (EPCIP)[377] aimed at improving the protection of ECI, following an all-hazards approach[378]. The document established the creation of the CIP contact group, that bring together national CIP contact points, which represents a centre of coordination and cooperation on general aspects of EPCIP[379]. In addition, experts groups on CIP[380] are required in order to provide their expertise on CIP and facilitate the dialogue and information sharing between the public and private sector on the CIP field. They can help identifying vulnerabilities and best practices and developing measures to reduce these vulnerabilities.

At national level, each member state should develop its own national CIP program in order to protect its national critical infrastructures. These programs should address the

[375]Sistema di Informazione per la Sicurezza della Repubblica, *2013 Italian cyber security report critical infrastructure and other sensitive sectors readiness*, consulted at http://www.sicurezzanazionale.gov.it/sisr.nsf/sicurezza-in-formazione/la-cyber-security-in-italia.html on 18/10/2015, p. 1

[376] Eur-lex, *Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection*, consulted at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32008L0114 on 20/10/2015

[377] Eur-lex, *Communication from the Commission on a European Programme for Critical Infrastructure Protection* /* COM/2006/0786 final */, consulted at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52006DC0786 on 20/10/2015

[378] Ibidem

[379] Ibidem

[380] Ibidem

identification and classification of national critical infrastructures on the basis of two main criteria: scope and severity[381].

- Scope refers to the disruption or destruction of a critical infrastructure measured on the basis of the dimension of the geographical area which could be damaged as a consequence of its malfunctioning[382].
- Severity means that the consequences of the disruption or destruction of the CI will be measured on the basis of economic, environmental, political, social consequences[383].

A relevant component of the EPCIP that allows the information and good practices sharing on the CIP issue among all actors involved is the Critical Infrastructure Warning Information Network (CIWIN)[384], which is an internet-based information and communication system.

On the same issue, that of critical infrastructures, in 2006 the European Commission elaborated the "Proposal for a directive of the council on the identification and designation of European critical infrastructure and the assessment of the need to improve their protection"[385] which represented the basis of the process of identification and designation of ECI. A list of critical sectors is made and it involves the food, water, health, energy, transport, financial, ICT sectors[386]. In 2008 a final version of the European Commission directive was approved: it was the "Council directive on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection"[387]. With respect to the 2006 directive, only the energy and transport critical sectors are considered while a reference is made to the possibility of a future inclusion of the ICT sector, which is fundamental for the

[381] Ibidem
[382] Ibidem
[383] Ibidem
[384] Ibidem
[385] Sistema di Informazione per la Sicurezza della Repubblica, *2013 Italian cyber security report critical infrastructure and other sensitive sectors readiness*, consulted at http://www.sicurezzanazionale.gov.it/sisr.nsf/sicurezza-in-formazione/la-cyber-security-in-italia.html on 18/10/2015, p. 61
[386] Ibidem, p. 6
[387] Eur-lex, *Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection*, consulted at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32008L0114 on 20/10/2015

functioning of modern societies. However, the directive has not been modified yet in that sense.

Since critical infrastructures are vital for the economic and societal growth of nations and the EU, in 2009 the European Commission proposed a communication on critical infrastructures protection named "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience"[388]. The document strengthens the role of ENISA on tactical and operational level and the activities outlined are performed in parallel and within the EPCIP[389]. In addition, the communication defines a plan of immediate action to strengthen the security and resilience of critical information infrastructures (CIIs)[390]. The plan is organized in five areas: preparedness and prevention, detection and response, mitigation and recovery, international cooperation, criteria for European critical infrastructure in the ICT sector[391].

- The preparedness and prevention will be achieved through the definition, with the support of ENISA, of a minimum level of capabilities for national CERTs and their key role for national preparedness, information sharing, coordination and response[392];
- Detection and response will be achieved thanks to the development of a European information sharing and alert system (EISAS)[393];
- Mitigation and recovery will be achieved through: the establishment of national contingency plans for the information sharing between member states, the organization of pan-European exercises on large-scale network security incidents, the cooperation among national CERTs with the support of ENISA;
- The international cooperation is achieved through principles and guidelines for the Internet resilience and stability developed by the Commission together with the member states at European and global level. At EU level the focus is on

[388] Eur-lex, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection - "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience"* {SEC(2009) 399} {SEC(2009) 400} /* COM/2009/0149 final */, consulted at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52009DC0149 on 21/10/2015
[389] Ibidem
[390] Ibidem
[391] Ibidem
[392] Ibidem
[393] Ibidem

agreements of mutual assistance and strategies for a coordinated recovery. At global level the focus is on the cooperation with foreign countries[394];

- Finally the Commission, with respect to the directive 114/2008, will continue to focus on the criteria used to identify ECI for the ICT sector[395].

In 2010 the Commission elaborated a communication for the establishment of a Digital Agenda for Europe[396]. It represents one of the seven pillars of the Europe 2020 strategy. The objective consists in the development of a digital single market based on fast Internet and interoperable applications in order to gain economic and social benefits[397]. It is composed of seven key points:

- The establishment of a digital single market without barriers in the EU is important in the modern era as people and businesses, which access the Internet everyday for many purposes, have the right to share their ideas, be protected and enjoy the highest quality of the services online[398];
- The enhancement of interoperability and standards refers to the fact that the EU, on the basis of standard policies and procedures, enhances the possibility for IT devices, applications and services to interact anywhere[399];
- The strengthening of trust and security on line is necessary in order to make Internet users feel safer when make on line transactions since cyber crime, child pornography and the theft of personal data are increasing. It was for this reason that in 2013 the Commission asked Europol to establish the EC3[400];
- The promotion of fast and ultra fast internet access for all is necessary in order to enjoy new services such as videoconferencing or high definition television. Therefore Europe has to be more competitive online, establishing next

[394] Ibidem
[395] Ibidem
[396] Eur-lex, *Communication from the commission to the European parliament, the council, the european economic and social committee and the committee of the regions, A Digital Agenda for Europe* /* COM/2010/0245 f/2 */ , consulted at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52010DC0245R(01) on 21/10/2015
[397] Ibidem
[398] European commission, *Digital Agenda for Europe*, consulted at http://ec.europa.eu/digital-agenda/digital-agenda-europe on 21/10/2015
[399] Ibidem
[400] Ibidem

generation access networks (NGA) in order to match South Korea and Japan online leaders[401];

- The investment in ICT research and innovation thanks to funding programs such as Horizon 2020 and the PPP is important for the economic growth of Europe and its competitiveness[402];
- The promotion of digital literacy, skills and inclusion is important in a context in which a part of the population is still excluded from the digital environment and therefore cannot benefit from the online services and cannot participate to societal mechanisms[403];
- The acquisition of benefit from ICT in the energy, environmental, health, transport and social sectors makes Europe more competitive[404].

Therefore, the creation of a single digital market entails social and economic advantages in the sense that with a single and secure market not only the safety of European people but also investments from abroad increase.

In the same year, an important document on cybersecurity was developed by the Commission named "EU internal security strategy in action: five steps towards a more secure Europe"[405]. In a context of increasing security threats in number and sophistication, the document identifies five strategic objectives in order to enhance the EU cybersecurity:

- disrupt international crime networks[406];
- prevent terrorism and address the radicalization and recruitment[407];
- increase the level of security for citizens and businesses in the cyberspace[408];
- enhance security through the management of borders[409];
- increase Europe's resilience to crises and disasters[410].

[401] Ibidem
[402] Ibidem
[403] Ibidem
[404] Ibidem
[405] Eur-lex, *Communication from the commission to the European parliament and the council, The EU Internal Security Strategy in Action: Five steps towards a more secure Europe* /* COM/2010/0673 final */, consulted at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52010DC0673 on 22/10/2015
[406] Ibidem
[407] Ibidem
[408] Ibidem
[409] Ibidem

Among the above cited strategic points, the third one requires a deeper analysis. Increasing the level of security for citizens and businesses refers to the fact that, due to new technologies, criminals activities are increasing in the cyber domain therefore IT network users need more protection from cyber threats. In particular, three main actions have to be implemented in order to make IT networks more secure. The first one refers to the establishment of the EC3 in order to fight cyber crime. The second one refers to the establishment of the incident reporting mechanism in order to allow people to make report of cyber attacks they received. Finally, the third action refers to the establishment of a relationship among national CERTs and the CERT-EU and the establishment of the EISAS.

[410] Ibidem

CHAPTER FOUR

ITALY AND CYBERSECURITY

4.0 Introduction

Due to the increasing number of cyber threats, which can take different shapes, can be performed by different actors and can possess different goals, Italy had to develop its national cybersecurity strategy in order to protect the economy and society from the negative impact of cyber attacks and ensure the well being of the nation and its citizens . 2013 was a significant year not only for the EU but also for Italy as regards the development of a strategy in the cybersecurity field. The Prime minister's decree (DPCM) of the 24th January 2013 "Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale"[411] defined the institutional architecture aimed at providing the security in the cyberspace but also established the creation of a National cybersecurity strategic Framework[412] and National Plan[413] which together represent the Italian National cybersecurity strategy, published in 2014. With respect to other EU member states and other nations across the world, Italy shows a delay in this field. However, 2013 represented an important year not only because, with the development of the national cybersecurity strategy, it signed the end of a long path started in the nineties in the cybersecurity field but also because it marked the starting point of another intense path toward the achievement of increasingly ambitious objectives, like the creation of the national CERT, in the cybersecurity field. Therefore the perspectives for the future are positive.

[411]Sistema di Informazione per la Sicurezza della Repubblica, *Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale*, consulted at http://www.sicurezzanazionale.gov.it/sisr.nsf/archivio-notizie/direttiva-sulla-sicurezza-cibernetica.html on 25/10/2015

[412] Sistema di Informazione per la Sicurezza della Repubblica, *National strategic Framework for cyberspace security*, consulted at http://www.sicurezzanazionale.gov.it/sisr.nsf/archivio-notizie/la-cyber-strategy-italiana.html on 15/09/2015

[413] Sistema di Informazione per la Sicurezza della Repubblica, *National Plan for cyberspace protection and ICT security*, consulted at http://www.sicurezzanazionale.gov.it/sisr.nsf/archivio-notizie/la-cyber-strategy-italiana.html on 25/10/2015

In this chapter an analysis of the DPCM and the National cybersecurity strategy of Italy will be made. Then a review of the Italian legislative landscape in the cybersecurity field, from the nineties when Italy started to be interested in cyber crime until the more recent developments in 2016, will be made.

4.1 DPCM of the 24th January 2013

In a context of increasing risks deriving from the cyber threats for the national security, the DPCM of the 24th January 2013 defines the institutional architecture which has to protect the national security with respect to material and immaterial critical infrastructures, with a particular reference to the national cyber protection and ICT security[414]. The tasks which have to be performed by the components of the architecture are described in the document, together with the mechanisms and procedures to follow in order to reduce vulnerabilities, prevent risks, swiftly respond to cyber attacks and restore the functionality of systems in case of crisis[415]. In art. 2 of the Directive some definitions are given. In particular:

- Cyberspace is defined as the set of IT infrastructures interconnected among them composed of hardware, software, data and users;
- Cybersecurity is defined as a condition in which the cyberspace is protected, by adopting different measures, from events which can be voluntary or accidental and that consists in the acquisition, destruction or modification of data, damage or destruction of IT systems and networks;
- Cyber threat consists in a set of conducts performed within or through the cyberspace by individuals or organizations in order to collect private data, destroy or modify them, and damage the functioning of IT systems and network;
- Warning consists in the communication of a cyber event;

[414]Sistema di Informazione per la Sicurezza della Repubblica, *2013 Italian cyber security report critical infrastructure and other sensitive sectors readiness*, consulted at http://www.sicurezzanazionale.gov.it/sisr.nsf/sicurezza-in-formazione/la-cyber-security-in-italia.html on 18/10/2015, p. 22
[415] Ibidem

- A situation of crisis takes place when a cyber event implies serious consequences for the national security and requires to take decisions at inter ministerial level.

The above cited institutional architecture has to be developed into three levels of intervention:

- The political and strategic level in charge of identifying operational objectives and ensure the national cyber protection and ICT security, considering the creation of a national plan for the cybersecurity;
- The operational level in charge of supporting and coordinating the actors involved;
- The management crisis level in charge of responding and restoring the functionality of systems.

In particular, from art. 3 to art. 10 the tasks assigned to each actor involved in the institutional architecture are described. The Prime minister is at the top of the architecture and, as stated in art. 3 of the decree, it has to adopt, on the basis of the proposal of the Inter ministerial committee for the security of the republic (CISR)[416], a strategic framework for the national cybersecurity and a national plan with the CISR deliberation. In addition, the decree assigns the Prime minister the task of giving directives to the Department for Intelligence and Security (DIS), the Intelligence Agency for the External Security (AISE) and the Intelligence Agency for the Internal Security (AISI).

CISR, in addition to the previously cited tasks, has to: monitor the implementation of the national plan; approve guidelines to promote the collaboration between public and private actors in the cybersecurity field but also the information sharing and adoption of best practices; it promotes the adoptions of initiatives to ensure the participation of Italy to forums (at bilateral or multilateral level, both EU and NATO) in order to adopt common strategies and policies of prevention and response in the cybersecurity field; it elaborates legislative proposals to empower the prevention and response measures in case of cyber threats and to manage crisis situations.

[416] As stated in the law 124/2007, CISR is chaired by the Prime minister and composed of the Ministry of foreign affairs, the Ministry of the Interior, the Ministry of Defence, the Ministry of Economy and Finance, the Ministry of Justice. It can make proposal and take decisions on guidelines and goals of the policy of information for the security. In addition it gives support in relation to the protection of critical infrastructures.

In order to support CISR in performing its previously cited tasks, the decree establishes the creation of the Collegial Coordinating body[417] chaired by the director of the DIS. The Collegial body, also known as technical CISR, is in charge of:

- developing preparatory activities to CISR's meetings;
- monitoring the implementation of the national plan and the effectiveness of the collaboration between public and private stakeholders;
- coordinating, with the support of CISR's guidelines and information provided by the public administration, the Scientific committee, Nucleus for cyberscurity, private stakeholders, the formulation of necessary information to identify cyber threats, vulnerabilities and to adopt best practices and security measures.

The previously cited Scientific Committee, established within the Intelligence System Training School[418], is composed of experts in the cybersecurity field coming from universities, public administrations, private sector with the task of developing mechanisms in order to improve security of IT systems and the security of the cyberspace.

In art. 7 a reference to DIS, AISE, AISI and their activities performed in the cybersecurity field, on the basis of tools and procedures defined by the law n.124/2007, is made. DIS is in charge of transmitting information linked to the cybersecurity to the Nucleus for the cybersecurity, public administrations and private sector. The two agencies elaborate information for the protection of the cyberspace and IT security.

Within the Military Adviser's Office the Nucleus for the cybersecurity is established permanently. It is headed by the military adviser and composed of members from DIS, AISE, AISI, Ministry of Internal and Foreign Affairs, Ministry of Defence, Ministry of Economy and Finance, Ministry of Economic Development, members of the digital agency. Its main aim consists in coordinating the different actors of the institutional architecture in the cybersecurity field. In addition, it encourages the planning of response to situations of crisis by private and public actors; it activates a 24/7 alarm and response unit; it assess and promotes information sharing involving private actors in order to spread warning in case of cyber incidents; it promotes the creation of inter

[417]Sistema di Informazione per la Sicurezza della Repubblica, *2013 Italian cyber security report critical infrastructure and other sensitive sectors readiness*, consulted at http://www.sicurezzanazionale.gov.it/sisr.nsf/sicurezza-in-formazione/la-cyber-security-in-italia.html on 18/10/2015, p. 23

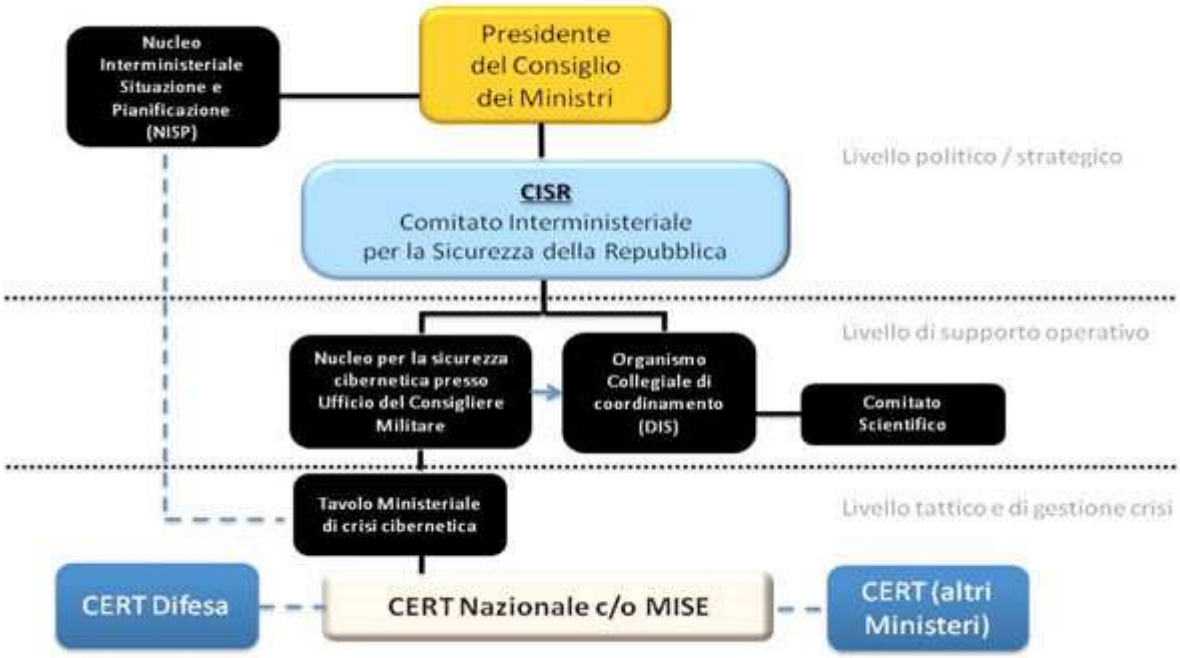
[418] Ibidem

ministerial exercises on cybersecurity and the participation of Italy to international exercises which simulate cyber attacks; it is a national reference point for maintaining contact with NATO, EU, ONU and other international organizations. In case of serious cyber attack that requires to take decisions at inter ministerial level, it declares the situation of crisis and activate the NISP as inter ministerial Table of cyber crisis.

NISP is headed by the military advisor and its main task is ensuring a correct and coordinated management of a situation of crisis in the cyber field. It can also collaborate with the national CERT, established within the Ministry for the Economic Development but which is not operative yet, in order to deal with technical aspects of the responses to crisis situation.

Art. 11 of the decree refers to the private sector, its duty and tasks. Private operators, which are those that provide "public networks of communication or electronic communication services to the public, operating national and european critical infrastructures depending on ICT systems"[419], have to communicate to the Nucleus for the cybersecurity the existence of violations of the security or integrity of IT systems; they have to adopt best practices and measures for the cybersecurity; they provide intelligence security organisms with information; they contribute to the management of cyber crisis by restoring the functionality of IT systems and networks. The strategic importance of the PPP in the cybersecurity field will emerge in the strategic framework and national plan.

[419] Sistema di Informazione per la Sicurezza della Repubblica, *National strategic Framework for cyberspace security*, consulted at http://www.sicurezzanazionale.gov.it/sisr.nsf/archivio-notizie/la-cyber-strategy-italiana.html on 15/09/2015, p. 26



Source: I principi strategici delle politiche di cyber security di Stefano Mele[420]

4.2 The National cybersecurity strategic framework and the National Plan

After the adoption of the DPCM of the 24th January 2013, the National cybersecurity strategic framework and the National Plan were both created by the Cybersecurity working group (CWG), established within the technical CISR the 3rd April 2013, chaired by the DIS and composed of all administrations that are represented within the CISR[421]. The two documents aim to strengthen the national preparedness to respond to cyber threats and focus on the importance of taking common solutions in the cybersecurity field. The strategic framework describes the nature and the evolving

[420] Mele S., *I principi strategici delle politiche di cyber security*, Sistema di Informazione per la Sicurezza della Repubblica, consulted at http://www.sicurezzanazionale.gov.it/sisr.nsf/approfondimenti/principi-strategici-delle-politiche-di-cyber-security.html on 26/10/2015

[421] Sistema di Informazione per la Sicurezza della Repubblica, *National strategic Framework for cyberspace security*, consulted at http://www.sicurezzanazionale.gov.it/sisr.nsf/archivio-notizie/la-cyber-strategy-italiana.html on 15/09/2015, p. 9

trends of cyber threats and the tools to address them[422]. In addition, it establishes strategic and operational guidelines to follow in order to enhance the national defence capabilities in the cyber field. The National Plan aims to give full implementation to the Framework by identifying lines of action and specific objectives. Italy, through these two documents, establishes its own national strategy in order to address threats that come from the cyberspace with more confidence.

The strategic framework is composed of two chapters and two annex. In chapter one, after making a reference to the cyberspace and its importance for the development of a modern nation, a deep analysis of the cyber threat is made. Cyber threat is defined as a set of conducts with malicious intent performed within or through the cyberspace by means of cyber attacks conducted by individuals or organizations in order to disrupt, damage and compromise the normal functioning of IT systems or compromise the confidentiality and integrity of data transmitted through IT networks[423].

A typical characteristic of the cyber threat is its asymmetric nature[424] as the attacker can perform the attack at distance given that he uses Internet to perform his attacks. In addition, he can hack sophisticated computer systems exploiting only one vulnerability and he is hardly identifiable as he hides itself behind the web, causing the attribution problem.

Then, four different categories of cyber threats are described: cyber crime, cyber espionage, cyber terrorism and cyber warfare[425]. As regards the category of cyber crime, a reference is made to its economic impact on societies and to the fact that the profit that derives from the illegal activity of cyber crime is often re-invested in the production of more advanced cyber weapons. States emerge as the main actors involved in the protection of the society from cyber threats, in particular they have to protect CII from cyber attacks, which can paralyze a nation, and the military command and control networks, ensuring also their resilience.

With regard to hacktivism, which consists in cyber attacks aimed at damaging the imagine of the target or causing the disruption of ICT systems for ideological reasons, a

[422] Ibidem, p. 7
[423] Ibidem, p. 12
[424] Ibidem
[425] Ibidem, p. 13

reference to DDoS attacks and web defacement, that consists in modifying a website in order to provoke disinformation[426], is made.

As regards cyber terrorism, the possibility that terrorists use cyber weapons in order to conduct attacks against civil or military targets is only an hypothesis for the future. Finally, as the cyberspace is characterized by evolving technologies and unexpected events can take place, a full knowledge of the number of threats that stem from this digital domain is impossible to achieve.

In conclusion, a focus on the types of vulnerabilities exploited by hackers when performing cyber attacks and the measures that should be implemented in order to avoid these vulnerabilities from being exploited is made. Organizational and procedural vulnerabilities are those caused by a "deficient implementation of protection against malware"[427], such as antivirus software, and by an inappropriate physical protection of critical infrastructures from natural events. Technical vulnerabilities depend on vulnerabilities of hardware and software[428].

Activities of risk assessment, mitigation and management should be taken into account, together with the promotion of training and education to raise the awareness of the personnel, in order to prevent vulnerabilities from being exploited[429]. In addition physical, logical, and procedural measures[430] are considered in order to ensure a high level of security. Physical measures consist in monitoring the access of the personnel to facilities and allowing only authorized personnel to enter; logical measures consist in ensuring the use of certified products; procedural measures refer to norms and procedures that govern the phases of the security procedure.

The second chapter is focused on the tools and procedures necessary for the enhancement of Italian cyber defence. In particular, six strategic guidelines and eleven operational guidelines are described. All the actors of the institutional architecture involved in ensuring the cybersecurity described by the DPCM of the 24th January 2013 have to follow the strategic guidelines which are:

[426] Ibidem, pp.15-16
[427] Ibidem, p. 17
[428] Ibidem
[429] Ibidem, p. 18
[430] Ibidem

- the strengthening of technical, operational and analytic capabilities[431] of the institutional actors involved in the cybersecurity issue;
- the enhancement of the capabilities to protect CI and strategic assets from cyber attacks[432];
- supporting the PPP[433];
- promoting and spreading the culture of the security in order to make Internet users aware of the cyber threats [434];
- the reinforcement of capabilities to address criminal activities online[435];
- the strengthening of the international cooperation[436] in the cybersecurity field.

In addition to these six strategic guidelines, eleven operational guidelines are analyzed:

- Strengthen the knowledge of Armed forces, the Police, the intelligence community, in order to prevent, identify, manage and react to cyber threats which hit IT systems[437];
- Identify a NIS authority in charge of sharing information at EU level about cybersecurity incidents, strengthen PPP by creating joint working groups, organizing national exercises which involve the participation of both public and private actors by obliging private operators to make incident reporting and establishing information sharing procedures[438];
- Develop a shared cyber taxonomy in order to make easier the communication on the topic at national and international level, raise the awareness of public and private actors about the risks that can stem from the cyberspace by organizing questionnaires, education campaign and promoting the culture of security[439];
- Promote the participation of Italy to international initiatives and forums on cybersecurity issue and to exercises organized by the NATO and ENISA[440]. It is

[431] Ibidem, p. 20
[432] Ibidem
[433] Ibidem
[434] Ibidem
[435] Ibidem
[436] Ibidem
[437] Ibidem, p. 21
[438] Ibidem
[439] Ibidem, p. 22
[440] Ibidem, pp. 22-23

important the cooperation with like-minded nations, allied countries and international organizations;

- Achieve the creation of a national CERT (CERT-N)[441] which has to communicate with other CERT's and act as an interface with the CERT-EU and the CERT's of other countries in order to enhance the national capabilities to react to cyber threats[442]. In addition, a reference is made to the creation of a Public Administration's Computer Emergency Response Team (CERT-PA) which acts as point of contact for public administrations and cooperate with the others CERT-PA at EU level[443];
- In order to make cybersecurity countermeasures efficient, it is necessary to adapt norms to the evolving trends of technology[444];
- Establishment of standards for the security of ICT products and the development of processes in order to confirm the compliance to these standards. Technical norms should be developed in order to protect the security of information (their integrity and privacy)[445];
- Cooperate with the industrial sector and develop services of assistance to small and medium enterprises[446];
- Use the cyberspace for the strategic communication, that is to say, to communicate national capabilities of deterrence in order to discourage cyber attacker[447];
- Assign to the Public Administration, financial, human and technological resources in order to achieve the objectives described by the framework[448];
- Implement a national system of information risk management in order to develop a structure for the prevention, identification and risk management[449].

The second chapter ends with a focus on the PPP and its crucial role in the cybersecurity field. The essential need of a cooperation between the public and private

[441] Ibidem, p. 23
[442] Ibidem, pp. 23-24
[443] Ibidem, p. 24
[444] Ibidem
[445] Ibidem
[446] Ibidem, p. 25
[447] Ibidem
[448] Ibidem
[449] Ibidem, p. 26

sector is mainly due to the fact that the majority of critical infrastructures which provide public strategic services are owned and managed by private operators. This topic has already emerged in the DPCM of the 24th January 2013, in particular in art. 11 where a reference was made to private operators and their key role in ensuring the protection of the cyberspace by contributing to the management of cyber crisis, communicating to the cybersecurity Nucleus eventual security violation of their IT systems and sharing information with intelligence and security agencies. Among the six strategic guidelines described in the Framework, the second, third and fourth make an explicit reference to the importance of involving the private sector in the cybersecurity field. The second strategic guideline focuses on the enhancement of defence capabilities of critical infrastructures and strategic assets (including also private actors); the third guideline refers to the cooperation between public and private actors; the fourth guideline refers to the promotion of a culture of security involving the expertise of universities in order to enhance the awareness among users, such as private users.

The topic of the PPP emerges also in two of the eleven operational guidelines which are described in the Strategic Framework and detailed in the National Plan. The two operational guidelines are: the second, which refers to the improvement of a PPP by, as stated in the Plan, developing working groups and cooperation activities involving public and private operators, enhancing the dialogue between institutions and the private sector, strengthening info-sharing systems and the third, which refers to the importance of spreading a culture of security for the achievement of the cooperation. The culture of security, as stated in the Plan, will be achieved by organizing initiatives for students, citizens, personnel of PA, organizing education and training programs on the cybersecurity topic, developing specific education programs for the personnel of PA and enterprises.

What emerges is that in the Italian strategic approach to the cybersecurity, the PPP fills an essential role. As stated by Stefano Mele in "I principi strategici delle politiche di cybersecurity"[450], the topic of the cooperation and info-sharing between the public and

[450] Mele S., *I principi strategici delle politiche di cyber security*, Sistema di Informazione per la Sicurezza della Repubblica, consulted at http://www.sicurezzanazionale.gov.it/sisr.nsf/approfondimenti/principi-strategici-delle-politiche-di-cyber-security.html on 26/10/2015

private sector in the cybersecurity field is one of the three strategic principles that, at a global level, all cyber strategies have in common, together with the goal of increasing security and resilience of IT systems and networks and developing diplomatic relationship and international partnerships. However, the EU cybersecurity strategy of February 2013, which has been analyzed in chapter three, makes a reference to the enhancement of the EP3R and to the need of improving the involvement of the private sector in the IT security but does not include, among the five strategic priorities, one specific on the topic of PPP. Stefano Mele in "La cooperazione tra pubblico e privato nella cyber-security"[451] concludes by stating three strong points and some weak points of the PPP. The strong points are:

- it is essential that private and public operators "facciano sistema"[452] since neither private nor public actors alone possess the whole vision and the information required in other to understand the problematic situation;
- private operators has to dialogue with public ones in order to achieve objectives which are impossible to achieve independently;
- the public sector alone is not able to obtain information about technologies, tools and procedures used by the actors which work in the cyberspace, therefore it has to start a relationship with the private one.

As regards the weak points, some obstacles to the PPP are: the need to protect more the privacy and the rights of citizens which are often unconsciously involved in cooperation processes; raise awareness not only of the big societies which manage critical infrastructures but also of the small and medium enterprises which represent the 99,8%[453] of the total amount of enterprises in Europe; maintain a simple structure in order to create trustworthy relationship among the subjects involved in the cooperation; identify, address and mitigate cyber attacks by creating a central system to promote the sharing of information between the public and private sector.

Finally, the author suggests some useful advices for an effective PPP: the public and the private sector should have a unique reference organism in order to communicate with

[451] Mele S., *La cooperazione tra pubblico e privato nella cyber security: punti di forza e criticità per la sicurezza nazionale*, Sistema di Informazione per la Sicurezza della Repubblica, consulted at http://www.sicurezzanazionale.gov.it/sisr.nsf/approfondimenti/la-cooperazione-pubblico-privato-nella-cyber-security.html on 26/10/2015

[452] Ibidem, p.12

[453] Ibidem, p.13

the other sectors; the relationship between public and private operators should be continuous and not occasional; the cooperation should be governed by specific norms; education programs financed by both the public and private sector should be developed.

The strategic framework ends with two annex. The Annex 1 focuses on the public stakeholders and their roles in the cybersecurity field. In addition to the actors involved in the institutional architecture described by the DPCM of the 24th January 2013, which were the Prime minister, CISR, DIS, AISE, AISI, NISP, Nucleus for the cyberecurity, other public actors emerge from the annex and they are: the Agency for Digital Italy, the Ministry of Foreign Affairs, Ministry of Interior, the Ministry of Defence, the Ministry of Economy and Finance, the Ministry of Economic Development. The Annex 2 includes a glossary of cybersecurity, where the most important terms used in this field are analyzed.

In order to give full implementation to the strategic Framework, the National Plan, which includes the lines of action and the goals to pursue, was elaborated by the CWG after the adoption of the DPCM as well as the Framework. In particular the Plan, in order to make the six strategic guidelines operative, describes the eleven operational guidelines and identifies the lines of action and the objectives to follow. Therefore the national Plan establishes a "roadmap for the adoption of priority measures for implementing the Framework"[454] through a process of dialogue among all the actors involved in the cybersecurity field. Private actors, which play a key role for the development of the PPP, are described as "indispensable"[455] for the development of cyber defence capabilities. Italy, adopting the Framework and the Plan, provides itself with a cybersecurity strategy which implies the involvement of both public and private stakeholders and that provides Italy with the possibility of preventing future cyber threats against the stability and competitiveness of the nation.

[454] Sistema di Informazione per la Sicurezza della Repubblica, *National Plan for cyberspace protection and ICT security*, consulted at http://www.sicurezzanazionale.gov.it/sisr.nsf/archivio-notizie/la-cyber-strategy-italiana.html on 25/10/2015, p. 7

[455] Sistema di Informazione per la Sicurezza della Repubblica, *National Plan for cyberspace protection and ICT security*, consulted at http://www.sicurezzanazionale.gov.it/sisr.nsf/archivio-notizie/la-cyber-strategy-italiana.html on 25/10/2015, p. 8

4.3 The Italian legislative landscape in the cybersecurity field

Italy started being interested in cybersecurity in the nineties. In particular, the law n. 547 of the 23th December 1993 "Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica"[456] and the law n. 269 of the 3rd August 1998 "Norme contro lo sfruttamento della prostituzione, della pedopornografia, del turismo sessuale in danno di minori"[457], whose art. 14 focuses on the task of the Ministry of the Interior to perform activities in order to contrast "i delitti commessi mediante l'impiego di sistemi informatici o mezzi di comunicazione telematica"[458], introduced in Italy a new type of criminality: the cyber crime.

With the advent of the 21st century Italian authorities became more aware of cyber threats and the risks for the security of the nation that derive from them, so they developed laws and organisms in order to make Italy a safer place from the cybersecurity point of view. The directive of the 16th January 2002 issued by the Ministry for Innovation and Technologies together with the Ministry of Communication "Direttiva sulla sicurezza informatica e delle telecomunicazioni nelle pubbliche amministrazioni"[459] represented the first law on the protection of information and data collected in the databases and managed by PA and the basis for future progress of PA on the cybersecurity topic. The directive establishes that the information managed by the PA possess a strategic value therefore has to be protected from possible modification. In addition, the directive invites PA to make a self-evaluation on the level of IT security of the systems they use and perform initiatives to place themselves on a "base minima di sicurezza"[460] in order to build the fundamentals of the security for PA.

In 2003 the Ministry of Communication together with the Ministry of Justice and the Ministry of the Interior issued a decree that established the Permanent Observatory for

[456] Interlex, Law n. 547 of the 23th December 1993, *Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica*, consulted at http://interlex.it/testi/l547_93.htm on 3/11/2015

[457] Parlamento italiano, Law n. 269 of the 3rd August 1998, *Norme contro lo sfruttamento della prostituzione, della pedopornografia, del turismo sessuale in danno di minori*, consulted at http://www.camera.it/parlam/leggi/98269l.htm on 3/11/2015

[458] Ibidem

[459] Presidenza del consiglio dei ministri, dipartimento per l'innovazione e la tecnologia, direttiva 16 gennaio 2002, *Sicurezza informatica e delle telecomunicazioni nelle pubbliche amministrazioni*, consulted at http://www.frareg.com/news/legislazione/privacy/direttiva_16012002.pdf on 4/11/2015

[460] Ibidem

communication and network security[461]. The observatory inherited the skills of the Working Group on network security and communication protection which was established with the inter ministerial decree of 21st September 1999[462]. The observatory acts within the Ministry of Economic Development and is composed of representatives of the Ministry of Communication, the Ministry of Justice, Ministry of Defence, Prime minister, Department of innovation and technology. Among the several tasks, the observatory has to develop norms and rules on NIS, monitor the fulfillment of the obligations of telecommunication organisms on NIS topic, provide assistance on the topic of network security and CIP, promote the culture of security. Another organism which acts within the Ministry for the Economic Development is the Superior Institute of ICT (Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione ISCOM)[463]. It was established with the law n. 111 of the 24th March 1907 on the improvement and expansion of postal, telegraphic, telephonic services. It experimented some changes because of the evolution of ICT. Today it is a technical-scientific organism whose activity, directed toward PA, ICT companies and users, consists in providing services to companies, producing norms, experimentation and research, education and training in the ICT field. The institute, which represents the national contact with ENISA, plays an important role with regards to the planning of national cybersecurity exercises such as CybIt 2013 which took place the 5th December 2013 within ISCOM and follows the first National cybersecurity exercise that took place the 19th June 2012. CybIt 2013, which consisted in the simulation of a cyber attack against companies involved in the energetic field and Public Institutions, obliged the different participants, both public and private actors, to cooperate and share information in order to ensure an adequate response in case of cyber incidents. Among the several actors that took part to the exercise, the Nucleus for the cybersecurity, the Intelligence department, the Agency for digital Italy, the companies ENEL and TERNA can be remembered.

[461] Ministero dello sviluppo economico, decreto interministeriale 14 gennaio 2003, *Istituzione osservatorio permanente per la sicurezza e la tutela delle reti e delle telecomunicazioni*, consulted at http://www.sviluppoeconomico.gov.it/index.php/it/normativa/decreti-interministeriali/2017545-decreto-interministeriale-14-gennaio-2003-istituzione-osservatorio-permanente-per-la-sicurezza-e-la-tutela-delle-reti-e-delle-telecomunicazioni on 5/11/2015

[462] Sistema di Informazione per la Sicurezza della Repubblica, *2013 Italian cyber security report critical infrastructure and other sensitive sectors readiness*, consulted at http://www.sicurezzanazionale.gov.it/sisr.nsf/sicurezza-in-formazione/la-cyber-security-in-italia.html on 18/10/2015, p. 17

[463] ISCOM, consulted at http://www.isticom.it/ on 5/11/2015

In 2003 two codes on the protection of personal data and electronic communication have been developed: the decree n. 196 of the 30th June 2003 "Codice in materia di protezione dei dati personali"[464] and the decree n. 259 of the 1st August 2003 "Codice delle comunicazioni elettroniche"[465]. The first one regulates the treatment of personal data implemented by anyone who finds itself in the territory of the state or in whatever place under its jurisdiction and by anyone who uses, for the treatment of data, tools located within the state. The code is important for the obligations it imposes on public actors such as PA. The second one defines norms in relation to communication through electronic means, defining principles, objectives and obligations for public sector and companies that provide communication services. As regards general principles, art. 3 establishes the freedom of people in using electronic communication means but also the right of economic initiative in the communication sector. As regards general objectives, art. 4 states that the regulation of electronic communication is aimed to the protection of the rights of privacy, freedom of communication, freedom of economic initiative. Art. 16-bis is important as it identifies a national CERT within the Ministry of Economic Development aimed to give technical assistance to users in case of cyber incidents. The national CERT is not operative yet. In 2012 the decree n. 70 of the 28th May modified the decree n. 259 of 2003 on electronic communication.

In March 2003 the Working Group on CIIP was established by the Ministry for Innovation and Technology. The Group was composed of representatives of the Ministry of Interior, Ministry of Infrastructures, Ministry of Communication, and the major private providers such as Telecom Italia and Wind. In March 2004 the Group issued a report named "Critical information infrastructure protection: the Italian situation"[466]. The report focuses on the increasing necessity of protecting critical information infrastructures which are interconnected in the cyberspace. In addition,

[464] Garante per la protezione dei dati personali, decreto legislativo 30 giugno 2003 n. 196, *Codice in materia di protezione dei dati personali*, consulted at http://garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1311248 on 6/11/2015

[465] Parlamento italiano, decreto legislativo 1 agosto 2003 n. 259, *Codice delle comunicazioni elettroniche*, consulted at http://www.parlamento.it/parlam/leggi/deleghe/03259dl.htm on 6/11/2015

[466]Sistema di Informazione per la Sicurezza della Repubblica, *2013 Italian cyber security report critical infrastructure and other sensitive sectors readiness*, consulted at http://www.sicurezzanazionale.gov.it/sisr.nsf/sicurezza-in-formazione/la-cyber-security-in-italia.html on 18/10/2015, p. 18

examples of interruptions of energy supply in Italy and across the world are made, together with a list of critical information infrastructures. These are: the electric infrastructure, IT and telecommunication networks, gas infrastructure, railway, streets, bank and financial circuits, hospitals, nuclear facilities, satellite navigation system, monitor system like SCADA. In the document a reference to the creation of a CERT-PA with an early warning function 24/7 is made[467]. The CERT-PA has to assist PA in order to guarantee the continuity of their service in case of cyber attacks and provides them with some advices in relation to the prevention, management, response and recover from cyber incidents. The CERT-PA became operative only in 2014.

In 2005 the decree n. 82 of the 7th March "Codice dell'amministrazione digitale" was issued and signed an important step in the process of digitalization of PA but focused also on the importance of the protection of personal data. Thanks to the digitalization of PA, public services are provided on-line making easier for companies and citizens to communicate with PA. Among the new services provided there are the online payment and the certified e-mail. Art 51. is focused on the security, availability, integrity, confidentiality of data, infrastructures and systems of PA and on the fact that the digital documents of PA have to be controlled in order to reduce to the minimum the level of destruction, loss and unauthorized access to information.

In the same year, the decree n. 155 of the 31st of July, "Conversione in legge, con modificazioni, del decreto-legge 27 luglio 2005, n. 144, recante misure urgenti per il contrasto del terrorismo internazionale"[468], also known as legge Pisanu as it takes the name from the Ministry of the Interior at that time, focused, in art. 7-bis, on the telecommunication security[469]. More specifically, the article gives jurisdiction to the Ministry of the Interior for what concern the protection of critical information infrastructures of national interest and identifies the Postal Policy as responsible for the law enforcement in case of cyber attack against national critical infrastructures.

---

[467] Dipartimento dei vigili del fuoco, del soccorso pubblico e della difesa civile, *Protezione delle infrastrutture critiche informatizzate, la realtà italiana*, consulted at http://www.vigilfuoco.it/aspx/page.aspx?IdPage=3857 on 7/11/2015, p. 43

[468] Parlamento italiano, legge 31 luglio 2005 n. 155, *Conversione in legge, con modificazioni, del decreto-legge 27 luglio 2005, n. 144, recante misure urgenti per il contrasto del terrorismo internazionale*, consulted at http://www.camera.it/parlam/leggi/05155l.htm on 8/11/2015

[469] Cencetti C., *Cybersecurity: Unione Europea e Italia prospettive a confronto*, 2014, edizioni nuova cultura, Roma, consulted at www.iai.it/sites/default/files/iaiq_12.pdf on 15/09/2015, p. 69

In January 2008 in the field of CIP a decree on "the identification of critical IT infrastructure of national interest"[470] was issued by the Ministry of the Interior. In art. 1 critical infrastructures are described as those systems and computer services that support the institutional functions of: ministries and agencies which operate in the sector of security, communication, defence, international relations, justice, transports, health, energy, environment, finance; Bank of Italy; state-owned societies which operate in the field of energy, health and water; other institutions, administration, public or private actor whose activity is of national interest[471].

As regards the CIIP, in the same year the Ministry of the Interior established the "National anti cyber crime center for the protection of critical infrastructures" (Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche CNAIPC)[472] within the Postal Police. CNAIPC is in charge of prevention, repression and contrast of criminal activities conducted against CII of national interest[473]. Its added value derives from the establishment of exclusive telecommunication links with critical infrastructures in order to share data and information useful for the assessment, repression and prevention of cyber threats. CNAPIC is composed of an Operational Sector and a Technical Sector[474]. The first one supports the function of: Operational Room, for the management of the contact point 24/7 specialized on the share of information with CII and companies involved in their protection; Intelligence, for the gathering of data and information useful for the prevention at national and international level; Analysis, in order to analyze data and information collected, develop report on the future evolution of threats, give responses in case of cyber attacks against CII. The second one is responsible for the management and functioning of the CNAIPC technical infrastructure and telecommunication links with CII, identification of resources and planning of training courses for the personnel.

In May 2010 the Prime minister established the "National organization for crisis management" in order to revise, on the basis of principles of prevention, management

[470] Sistema di Informazione per la Sicurezza della Repubblica, *2013 Italian cyber security report critical infrastructure and other sensitive sectors readiness*, consulted at http://www.sicurezzanazionale.gov.it/sisr.nsf/sicurezza-in-formazione/la-cyber-security-in-italia.html on 18/10/2015, p. 8
[471] Ibidem
[472] Ibidem, p. 19
[473] Ibidem
[474] Ibidem

and response to crisis elaborated by the NATO and EU, the "National manual for crisis management" published in 1994. In particular, art. 4 of the decree defines the structure of the Political strategic committee (Comitato Politico-Strategico COPS)[475] which was already described in the 1994 manual. It is chaired by the Prime minister and composed of the Ministry of Defence, Foreign Affairs, Interior, Economic Development. It has a role of guidance during a situation of crisis. In addition, it elaborates provisions and authorize the adoption of countermeasures. Art. 5 introduces a new body, the Inter ministerial Unit for situation and planning (Nucleo Interministeriale di Situazione e Pianificazione NISP)[476] as a permanent body in charge of constantly monitoring the level of national and international security, supporting COPS and coordinating inter ministerial cyber exercises.

In July of the same year, the Parliamentary Committee for the security of the republic (Comitato Parlamentare per la Sicurezza della Repubblica COPASIR) issued the "Relazione sulle possibili implicazioni e minacce per la sicurezza nazionale derivanti dall'utilizzo dello spazio cibernetico"[477]. This relation is important because it focuses on the increasing vulnerability of societies to cyber threats that can stem from the cyberspace and produces negative consequences for the competitiveness of a nation by impacting critical infrastructures. In order to simplify the complex issue of cyber threats, these are divided into four main categories: cyber-crime, cyber terrorism, cyber espionage, cyber war[478]. However, in Annex 2 a list of the main types of cyber threats is made and it includes cyber-espionage, propaganda, DDoS attacks, attacks against CII[479]. As regards the authors of cyber attacks, in Annex 1 a list of the main source of cyber attacks is made, including criminal groups, hacker, phishers, terrorists, spammers[480]. Annex 3 describes some concrete examples of cyber crime across the world.

The Relation considers the best systemic approach in order to defend the nation from cyber threats. A defence policy of this type involves all sectors of the society, implying

[475] Ibidem, p. 20
[476] Ibidem
[477] Cencetti C., *Cybersecurity: Unione Europea e Italia prospettive a confronto*, 2014, edizioni nuova cultura, Roma, consulted at www.iai.it/sites/default/files/iaiq_12.pdf on 15/09/2015, p. 73
[478] Comitato parlamentare per la sicurezza della repubblica, *Relazione sulle possibili implicazioni e minacce per la sicurezza nazionale derivanti dall'utilizzo dello spazio cibernetico*, consulted at http://www.parlamento.it/documenti/repository/commissioni/bicamerali/COMITATO%20SICUREZZA/Doc_XXXIV_n_4.pdf on 10/11/2015, p. 17
[479] Ibidem, p. 56
[480] Ibidem, pp. 54-55

collaboration among different subjects from institutional agencies to companies that manage CI and private citizens. Therefore, the essential role of the PPP in the cybersecurity field emerges. In addition, the Relation analyzes the importance of preventing cyber threats in the international landscape and focuses on the fight against cyber crime in Italy through a strategy composed of five points among which emerge the key role of PPP, the empowerment of the role of the intelligence, the development of training campaigns, the crucial role of the Postal Policy in contrasting cyber crime and ensuring the protection of national CI. As regards the role of the Italian intelligence in the cybersecurity field, a reference is made to the "Intelligence System for the security of the republic" established by the law n. 124/2007 which reformed the Italian intelligence on the basis of three structures: DIS, AISE and AISI. In the final section of the Relation, the Italian government is recommended to establish an organizing-strategic structure in order to ensure an adequate leadership and plan clear guidelines to contrast cyber threats and coordinate all actors involved. Therefore a coordinating structure focused on the cybersecurity issue should be established within the Prime minister.

More recently, in 2011 the President of the Republic issued the decree n. 61 of the 11th April "Attuazione della direttiva 2008/114/CE recante l'individuazione e la designazione delle infrastrutture critiche europee e la valutazione della necessità di migliorarne la protezione"[481] which transferred the European directive on critical infrastructures in the Italian legislation. The decree establishes the procedures to identify ECI in the energy and transport sectors but also the assessment method of the level of security of the infrastructures and the regulations for the protection from threats. A definition of CI is given in art. 2 on the basis of that given in the European decree. In addition, in art. 4 the NISP is defined as responsible for the identification of ECI, supported by the representatives of the Ministry of the Economic Development and the Ministry of Infrastructures and Transportation. In art. 6 the assessment criteria for the identification of CI are described and they involve:

- the possible victims, in terms of injured and dead people;

[481] Cencetti C., *Cybersecurity: Unione Europea e Italia prospettive a confronto*, 2014, edizioni nuova cultura, Roma, consulted at www.iai.it/sites/default/files/iaiq_12.pdf on 15/09/2015, p 77

- the possible economic consequences, in term of financial loss, deterioration of the service;
- the possible consequences for the population, in term of trust for the institutions, physic suffering.

The Decree makes a reference to a structure responsible for supporting the NISP with technical and scientific activities for the identification of ECI and for the relationship with the European Commission. This structure is the "Secretariat for critical infrastructure (Segreteria Infrastrutture Critiche SIC)"[482] established within the Office of the military adviser of the Prime minister with the DPCM of the 22th December 2010.

In March 2012 the Ministry of the Economic Development issued a decree which established the Italian Digital Agenda (Agenda Digitale Italiana ADI)[483]. It represents a set of actions and norms for the development of technologies, innovation and digital economy. It is one of the seven initiatives of the Europe strategy 2020, which establishes the objectives to achieve by 2020 for the growth of the EU in five areas: employment, innovation, education, social inclusion and climate[484]. According to ADI, the Italian cybersecurity strategy should focus on some areas such as: promotion of the education for citizens and businesses; raising awareness about risks that come from the web; development of tools to detect and contrast cyber threats; enhancement of the PPP; creation of mechanisms for incident response; enhancement of international cooperation[485].

In June 2012 with the decree n. 83, converted by law n. 134 of the 7th August 2012, the Agency for Digital Italy (Agenzia per l'Italia Digitale AGID)[486] was established. It is in charge of implementing the objectives of the Italian Digital Agenda. In addition, the Agency is in charge of: spreading the use of ICT in order to promote innovation and

[482] Sistema di Informazione per la Sicurezza della Repubblica, *2013 Italian cyber security report critical infrastructure and other sensitive sectors readiness*, consulted at http://www.sicurezzanazionale.gov.it/sisr.nsf/sicurezza-in-formazione/la-cyber-security-in-italia.html on 18/10/2015, p. 20

[483] Ibidem, p. 21

[484] European commission, *Europe 2020*, consulted at http://ec.europa.eu/europe2020/index_en.htm on 11/11/2015

[485] Sistema di Informazione per la Sicurezza della Repubblica, *2013 Italian cyber security report critical infrastructure and other sensitive sectors readiness*, consulted at http://www.sicurezzanazionale.gov.it/sisr.nsf/sicurezza-in-formazione/la-cyber-security-in-italia.html on 18/10/2015, p. 21

[486] Ibidem

economic growth; promoting initiatives of digital alphabetization; monitoring the quality of the services provided online by the PA; elaborating guidelines and rules in order to make IT systems used by PA uniform. The Agency inherited the skills of the DigitPA, a body responsible for the digitalization of PA established with the decree n. 177 of December 2009.

In 2013 the Intelligence System for the security of the republic issued the "Relazione sulla politica dell'informazione per la sicurezza"[487] concerning the year 2012. The Relation, in the second chapter, focuses on the impact of new technologies on the security of the nation and defines the cyber threat as asymmetric and transversal. This definition implies a strategy of response to the cyber threat based on the model of the "sicurezza partecipata"[488] which is based on the importance of the cooperation between public and private actors in the cybersecurity field. In the final section of the Relation, a reference to the increasing use of the web by terrorist organizations for propagandist reasons is made.

The following year the same Relation, concerning the year 2013, was published and focused, in part 1, on the cyber threat too, defining it as pervasive, sophisticated and asymmetric. A reference is made to the increasing number of cyber intrusions, on the basis of the results of monitoring activities of the intelligence, aimed to gain sensitive information and strategic know-how, damaging governmental and military bodies and research centers. Then, a focus on cyber crime and its huge economic impact on the society is made. In addition, an analysis of hacktivism, mainly attributable to Anonymous, and its evolution in term of motivation and offensive potential emerges. As regards the essential role of the PPP in order to improve the cybersecurity of a nation, in the Annex a reference is made to the establishment of the "Tavolo Imprese"[489] which gathered in 2013 and to which participated 10 Italian strategic companies.

In 2013 the research center "Cyber intelligence and information security (CIS)" of the University Sapienza in Rome issued, in collaboration with DIS, an important document entitled "2013 Italian Report on Cyber Security: critical infrastructure and other

[487] Cencetti C., *Cybersecurity: Unione Europea e Italia prospettive a confronto*, 2014, edizioni nuova cultura, Roma, consulted at www.iai.it/sites/default/files/iaiq_12.pdf on 15/09/2015, p. 81

[488] Ibidem

[489] Sistema di Informazione per la Sicureza della Repubblica, *Relazione sulla politica dell'informazione per la sicurezza 2013*, consulted at http://www.sicurezzanazionale.gov.it/sisr.nsf/relazione-annuale/relazione-al-parlamento-2013.html on 28/12/2015, p. 94

sensitive sectors readiness"[490] in order to provide an academic contribution for a better understanding of one of the most important topic at global level, that of the protection of critical infrastructures and other sensitive sectors from cyber threats. The document is composed of five chapters:

- The first chapter focuses on the topic of critical infrastructures and the importance of their protection, providing the definitions that United States, European Union and Italy give of them. In addition, the Italian definitions of cyberspace and cybersecurity are described. Finally, the topic of cyber threat is analyzed, providing data relative to cyber attacks against Italy, the sectors mainly impacted (according to Clusit data, by 2012 the Italian government sector was the most attacked, followed by industry and political organizations)[491], the most widespread methods of attack (according to Clusit data, in 2012 in Italy hacktivism was the most popular)[492], and the cost of cyber crime;
- The second chapter provides an analysis of the legislative landscape in the Italian cybersecurity field since the nineties until 2013, ending with a focus on CERTs and national CERTs, describing their tasks. Although the Italian national CERT has been identified by the decree n. 259 of the 1st August 2003, it is not operative yet. However, in 2014 the CERT-PA became operative and the CERT DIFESA is operative too and responsible for providing assistance and response methods to Defence users and providing the "Bollettino di sicurezza informatica"[493] to Armed Forces;
- The third chapter analyses the cybersecurity situation in the EU and other countries such as France, Germany, United Kingdom and the US;
- The fourth chapter is the most interesting one because it provides the result of the research made by the CIS through an anonymous questionnaire submitted to more than sixty Italian organizations sensitive to attacks coming from the

[490] Sistema di Informazione per la Sicurezza della Repubblica, *2013 Italian cyber security report critical infrastructure and other sensitive sectors readiness*, consulted at http://www.sicurezzanazionale.gov.it/sisr.nsf/sicurezza-in-formazione/la-cyber-security-in-italia.html on 18/10/2015
[491] Ibidem, p. 10
[492] Ibidem
[493] Ministero della difesa, *CERT difesa*, consulted at http://www.difesa.it/SMD_/Staff/Reparti/II/CERT/Pagine/Chi_Siamo.aspx on 13/11/2015

cyberspace[494]. These have been divided into four groups: PA, public utilities, financial sector and industrial sector[495]. The result is that these sectors are not fully aware of being objective sensitive to cyber attacks which could cause economic and technological damages. In addition, a "cybersecurity readiness index"[496] is provided at the end of the chapter in order to better understand the national cybersecurity situation. The readiness index is composed of four indexes: the awareness index, the defence index, the policy index and the external independency index[497]. What emerges is that public utilities are the readiest sector with respect to other sectors, while PA are the less ready one;

- The last chapter provides some recommendations for the implementation of a national cybersecurity strategy. In particular, it describes a risk management process, composed of risk assessment and risk treatment, which is necessary for the development of an effective national cybersecurity strategy.

In 2014 CIS, in collaboration with AgID, issued the "2014 Italian cybersecurity report: consapevolezza della minaccia e capacità difensiva della pubblica amministrazione italiana"[498]. In order to have a better understanding of the level of awareness of PA about the risks that derive from cyber threats and their defensive capabilities, CIS and AgID made a research, submitting a questionnaire to more than four thousand PA. The results of the research demonstrate that only the most important PA with bigger dimensions and with adequate means and budget are better organized and readier than little PA. The document is composed of five chapters. The first one is dedicated to the introduction. The second chapter describes the assessment method of questionnaires based on three key performance indicators: organization, defence and awareness[499]. The third chapter provides the results of the research. In the fourth chapter three case studies are described: INPS, Corte dei Conti and Regione Friuli Venezia Giulia. Finally, the

[494] Sistema di Informazione per la Sicurezza della Repubblica, *2013 Italian cyber security report critical infrastructure and other sensitive sectors readiness*, consulted at http://www.sicurezzanazionale.gov.it/sisr.nsf/sicurezza-in-formazione/la-cyber-security-in-italia.html on 18/10/2015 , p. 37
[495] Ibidem
[496] Ibidem, p. 51
[497] Ibidem
[498] Agenzia per l'Italia digitale, *Italian cyber security report 2014*, consulted at http://www.agid.gov.it/notizie/2015/01/14/italian-cyber-security-report-2014 on 13/11/2015
[499] Ibidem, p. 5

report provides some recommendations and advices in order to improve the level of security of PA.

In 2015, in particular the 1st August 2015, the Prime Minister Matteo Renzi issued a directive in which the lines of actions to follow in order to guarantee a secure cyberspace through which people can share ideas and communicate are stated. More in specific, in the first section of the directive Public Administrations are asked to enhance their capacity of reaction and response to cyber events by adopting coordinated procedures among administrations and acting in an integrated way with the other institutions and public organisms involved in the cybersecurity issue. Then, a focus is made on the importance of the partnership between public organisms and the private sector in order to increase the level of cybersecurity, given that the majority of critical infrastructures are managed and owned by private entities. Finally, the last two parts of the directive are dedicated to the fundamental role played by the research and development sector in the cybersecurity field, in particular in discovering new methods of cyber intrusion and the way to contrast it and to the international cooperation and its importance.

At the end of the year 2015, the Prime minister Renzi announced, during an event named "Italia, Europa: una risposta al terrore" which took place in the room Orazi and Curiazi in Rome, the financial measures stated in the Legge di stabilità approved in December 2015 aimed at establishing the budgetary policy of the following year. Among the news, the decision to invest two billion euro in the sector of culture and security, in particular 150 million euro will be invested to enhance the cybersecurity sector. This decision has been taken as a response to the threat of terrorism which menaces our security, especially after the Paris attacks.

More recently, at the beginning of 2016 the Prime minister Renzi has charged his friend Marco Carrai with a technical task in the cybersecurity field, more in specific, he should work as technical consultant at the Cybersecurity Nucleus at Palazzo Chigi. However, this decision caused a political debate among those that are not convinced about this designation as they fear the creation of a cybersecurity private structure since Carrai owns a firm involved in the cybersecurity issue. Renzi guaranteed that this will not happen and that the political authority in charge of managing security service will remain Marco Minniti.

CONCLUSIONS

In conclusion, the aim of this work was to demonstrate the importance of ICT in the Twenty-First Century by examining especially the negative changes the information revolution produced in modern societies, without forgetting the fact that with the spread of ICTs the world became more interconnected as people could share ideas, information and communicate at the speed of light, overcoming geographical and temporal boundaries, through the use of computers and the Internet. In addition, everything from the health sector to transportations and finance started base its functioning on IT networks, consequently increasing our dependence on ICTs. Therefore, from a positive point of view, societies and economies benefited from the introduction of ICT as it introduced increasing possibilities of growth and competitiveness for nations which became more digitalized.

However, the negative side of the spread of ICT consisted in the rise of a new type of threat, called cyber threat, which is different from traditional threats as it stems from a digital domain, named cyberspace. The latter has been described as a new dimension composed of the Internet, computers and IT networks where conflicts are fought, taking advantage of the intrinsic characteristics of the cyberspace that allow a cyber attacker to hit the adversary easily, anonymously and at low cost, with the aim of destroying its information and communication system while protecting his one. Therefore, with the introduction of ICTs the nature of conflicts has changed in the sense that means, place and objectives of war have changed, leading scholars to talk about cyber war when referring to this new way of making war.

All these elements have been deeply analyzed in the first chapter where the reader has been introduced to the cyber topic by providing some general aspects linked to the cyberspace and cyber threats. What emerges from this first section is that the more we depend on the cyberspace and the more societies and their services are digitalized the more vulnerable we are to cyber attacks as, being the main sectors of societies based on computer network and technologies for their functioning, we become possible targets for a potential cyber attacker. As a consequence, after a description of the cyberspace and the different types of cyber attacks that could stem from it, also taking into consideration the example of the relationship between China and the US on the cyber

topic, their mutual accuses of cyber espionage and their different ideas about the governance of the Internet and the cyberspace, the cyber war issue emerged. The reader clearly realizes that the topic of cyber war is a very complex one, being it very recent and in a continuous evolution, leading scholars not to agree on a single definition of it. In fact, while some of them argue that cyber war has never taken place and will never take place, being it not linked with the element of lethality and blood, others state the contrary arguing that wars have already embraced the cyber element and will do it more and more in the future, becoming inevitable. What emerges is that the difficulty one could encounter in defining cyber war derives from the fact that today it is difficult to understand what war is, what it means, being so different from traditional ones in means and scope and in continuous evolution therefore difficult to grasp. However, despite contrasting opinions of scholars about cyber war and the general complexity that permeates this issue, what is clear is the fact that the cyber threat is real and exists as potential menace in our daily lives.

This theoretical framework introduced the reader to the following chapter of my work in which a demonstration of the concreteness and the effectiveness of the cyber threat has been given. Through an analysis of different cyber attacks launched against both physical objectives and computer networks, a threatening framework emerges in the sense that, by describing in a detailed way when cyber attacks took place, in what they consisted and what were their dangerous and destructive consequences not only for the specific target but for the society and its economy in general, the reader can realize that the cyber threat is not a remote possibility, is not something that could take place in the future but is real and concrete. The famous Stuxnet attack launched by the US against the Iranian nuclear programs in 2009, the attack launched by Russia against Estonian websites in 2007, the more recent attacks launched by China and Russia against the websites of the Pentagon and the White house and the other attacks described in chapter two are only some of many cyber attacks that took place in the past and continue to occur. However, they are sufficient to demonstrate, on one hand, the ease with which an attack can be launched against an enemy and, on the other hand, the fact that with the spread of ICT the nature of conflicts has changed as they are fought through non-traditional means and in a non-traditional battlefield and the fact that the seriousness of

the consequences and the damages produced by the cyber weapon are similar to those that could be caused in a traditional war, avoiding death and blood.

After having dealt with a theoretical framework, in which a general overview of the cyber issue has been given in order to demonstrate our vulnerability to cyber attacks but at the same time the complexity that characterizes this issue and a practical framework, in which examples of real cyber attacks have been described in order to give concreteness to the first section, the topic of cybersecurity has been deeply analyzed. More in specific, in chapter three a focus on the EU legislative landscape in the cybersecurity field has been made, starting from 2000 until 2013 when the EU cybersecurity strategy was issued. In addition, the main documents, laws and directives linked to the cyber topic has been analyzed together with the organisms and institutions involved in this issue among which the Commission and ENISA emerged as the most important ones. In the same way, in the fourth chapter the legislative approach to the cybersecurity topic of a member state of the EU, that is to say, Italy, has been analyzed. In particular, a focus has been made on the most significant organisms involved and documents produced in this field starting from the nineties until 2014 when, as established by the Prime minister's decree in 2013, the Italian cybersecurity strategy has been issued, but also the latest developments in the cybersecurity field in 2016 have been considered.

Through these two chapters I tried to demonstrate what I have already stated in the introduction of my work, that is to say, the fact that with the spread of ICT and the rise of cyber threats states had to change their strategy of response in order to tackle with new threats which menace the security of their citizens and territory. In fact, both at EU and Italian level, when ICTs started developing and threats from cyberspace started stemming, it became clear that strategies aimed at protecting the cyberspace where needed, therefore shifting the focus from a traditional concept of security to the emerging concept of cybersecurity. What emerges from the last two chapters, in addition to a demonstration of the fact that investing in cybersecurity, making research in this field and producing norms in order to regulate the cyberspace are necessary in a threatening environment pervaded by ICTs, is that in the cybersecurity field the cooperation among states at international level but also the partnership between the public and private sectors, between universities and institutions together with the

cooperation between states and international organizations are fundamental. The whole society, not the state as single entity, is responsible for the provision of security, by sharing ideas and experiences in the cyber field.

After all these considerations, the aim of my work was awareness. In particular, make people aware that not only benefits and positive consequences derived from the spread of ICTs but, on the contrary, an environment of uncertainty, insecurity and in continuous evolution derived from the information revolution, making difficult finding suitable responses and strategies of defence. People should be aware of the fact that the cyber threat is real and that cyber attacks against IT systems, personal computers or physical objectives are increasing in number and frequency. Indeed, what has changed with the spread of ICT is the meaning of security, being threats coming from a non-traditional domain called cyberspace. As a consequence, focusing on cybersecurity represents the essential task not only of the government and specialized organisms but also of the whole society, together with the commitment to raise the level of cybersecurity, in particular after the Paris attack performed by ISIS the 13th November 2015. As stated by journalistic sources, ISIS terrorists use ICTs in order to communicate among them and the web as an instrument to spread terror. In particular, it seems that they planned the Paris attack by using the blinded chat of the PlayStation 4. However, if on one side terrorists used the web to communicate, on the other side they did not use it in order to launch cyber attacks. In fact, the terrorist threat, which is the most dangerous and spread across the world currently, is still physical, in the sense that it is based on the use of violence in order to cause the death of hundreds of people and bloodshed.

Finally, the purpose of my work was, above all, helping a disoriented outsider finding the right path in the complex, recent, risky and threatening cyber world.

BIBLIOGRAPHY

American foreign policy interests, *Cyberpower and national security*, 35:45-48, 2013

Arquilla J. and Ronfeldt D., *Cyberwar is coming!*, In Athena's camp: preparing for conflict in the information age, chapter 2, pp. 23-60, 1997

Brantly A., *Cyber actions by state actors: motivation and utility*, International journal of intelligence and counterintelligence, 27: 465-484, 2014

Collins A., *Contemporary security studies*, third edition, oxford university press, 2013

Eberle C., *Just war and Cyberwar*, Journal of military ethics, Vol. 12, No. 1, 54-67, 2013

Fjader C., *The nation-state, national security and resilience in the age of globalization*, Resilience, Vol. 2, No. 2, 114-129, 2014

Junio T., *How probable is cyber war? Bringing IR theory back in to the cyber conflict debate*, the Journal of strategic studies, Vol. 36, No.1, 125-133, 2013

McGraw G., *Cyber war is inevitable (unless we build security in),* The Journal of strategic studies, Vol. 36, No.1, 109-119, 2013

Rapetto U. e Di Nunzio R., *Le nuove guerre: dalla cyber war ai black bloc, dal sabotaggio mediatico a Bin Laden*, RCS libri, Milano, 2001

Segal A., *Cyberspace: the new strategic realm in US-China relations*, Strategic analysis, Vol. 38, No. 4, 577-581, 2014

Stone J., *Cyber war will take place*, The Journal of strategic studies, Vol. 36, No. 1, 101-108, 2013

WEBSITES

ABC News, *White House, Pentagon among targets of cyberattack*, consulted at http://abcnews.go.com/Technology/story?id=8034979&page=1 on 15/10/2015

Agenzia per l'Italia digitale, *Agenda digitale italiana*, consulted at http://www.agid.gov.it/agenda-digitale/agenda-digitale-italiana on 11/11/2015

Agenzia per l'Italia Digitale, *Italian cyber security report 2014*, consulted at http://www.agid.gov.it/notizie/2015/01/14/italian-cyber-security-report-2014 on 13/11/2015

Agenzia per l'Italia digitale, *Quadro normativo AGID*, consulted at http://www.agid.gov.it/agid/quadro-normativo on 11/11/2015

Allen N., *Russian hackers 'attacked Pentagon*, The Telegraph, consulted at 'http://www.telegraph.co.uk/news/worldnews/northamerica/usa/11788904/Russian-hackers-attacked-Pentagon.html on 11/10/2015

Armstrong J., *Canadian issue a hot topic for hacker group Anonymous*, Global news, consulted at http://globalnews.ca/news/2060420/canadian-issues-a-hot-topic-for-hacker-group-anonymous/ on 11/10/2015

Arnese M. e Pierri M., *Cyber security, ecco i fondi a disposizione di Renzi e Carrai*, Formiche, consulted at http://formiche.net/2016/01/20/cyber-renzi-carrai-legge-stabilita/ on 23/01/2016

Assinform, consulted at http://www.assinform.it/ on 19/12/2015

Assinform, *Security & Cybersecurity*, consulted at http://www.rapportoassinform.it/Sintesi/Segmenti_mercato/Security--Cybersecurity.kl on 19/12/2015

Auld A., *Dalhousie University Students' Facebook Page 'Deeply Disturbing,' Says School President*, The Huffington Post, consulted at http://www.huffingtonpost.ca/2014/12/16/dalhousie-university-students-facebook_n_6333200.html on 09/10/2015

BBC News, *Malaysia airlines website compromised by hackers*, consulted at http://www.bbc.com/news/world-asia-30978299 on 14/10/2015

BBC News, *Sony cyber-attack: North Korea calls US sanctions hostile*, consulted at http://www.bbc.com/news/world-asia-30670884 on 9/10/2015

Bennet J., *ISIS Hacker That Exposed US Troops In US Killed By Drone Strike* , the Daily caller, consulted at http://dailycaller.com/2015/08/27/isis-hacker-that-exposed-us-troops-in-us-killed-by-drone-strike/ on 15/10/2015

Biagio S., *L' isis utilizza internet. Ma forse è meno forte di quanto si creda*, Il sole 24 ore, consulted at http://www.ilsole24ore.com/art/mondo/2015-11-19/l-isis-utilizza-internet-ma-forse-e-meno-forte-quanto-si-creda-143247.shtml?uuid=AC6UwVdB&refresh_ce=1 on 22/01/2016

Cencetti C., *Cybersecurity: Unione Europea e Italia prospettive a confronto*, edizioni nuova cultura, Roma, 2014, consulted at www.iai.it/sites/default/files/iaiq_12.pdf on 15/09/2015

Central intelligence agency, consulted at https://www.cia.gov/about-cia/history-of-the-cia on 7/10/2015

Centro studi per la pace, *La definizione di terrorismo internazionale e gli strumenti giuridici per contrastarlo*, consulted at http://www.studiperlapace.it/view_news_html?news_id=20050219140025 on 13/10/2015

CERT di poste italiane, consulted at https://www.picert.it/ on 19/12/2015

China abc, *I rapporti sino-americani,* consulted at http://italian.cri.cn/chinaabc/chapter4/chapter40301.htm on 11/12/2015

China today, *China-taiwan issue,* consulted at http://www.chinatoday.com/city/china_taiwan_issue.htm on 12/12/2015

China.org, *The one-china principle and the Taiwan issue,* consulted at http://www.china.org.cn/english/taiwan/7956.htm on 12/12/2015

Clarke R., *War from cyberspace,* pp. 31-36, 2009, consulted at http://users.clas.ufl.edu/zselden/coursereading2011/Clarkecyber.pdf on 18/09/2015

Comitato parlamentare per la sicurezza della repubblica, *Relazione sulle possibili implicazioni e minacce per la sicurezza nazionale derivanti dall'utilizzo dello spazio cibernetico,* consulted at http://www.parlamento.it/documenti/repository/commissioni/bicamerali/COMITATO%20SICUREZZA/Doc_XXXIV_n_4.pdf on 10/11 /2015

Confesercenti, *Legge di stabilità, Renzi: "due miliardi di euro per sicurezza e cultura, taglio Ires rimandato al 2017",* consulted at http://www.confesercenti.it/blog/legge-di-stabilita-renzi-due-miliardi-di-euro-per-sicurezza-e-cultura-taglio-ires-rimandato-al-2017/ on 23/01/2016

Consulate- general of the people's republic of china in Toronto, *the Taiwan issue,* consulted at http://toronto.china-consulate.org/eng/topics/taiwan/t40572.htm on 12/12/2015

Cooperative Cyber Defence Center of Excellence (CCDCOE), consulted at https://ccdcoe.org/ on 7/10/2015

Corriere comunicazioni, *Cyber security, Renzi:"Investiremo 150 milioni",* consulted at http://www.corrierecomunicazioni.it/digital/38140_cybersecurity-renzi-investiremo-150-milioni.htm on 23/01/2016

Costanzo B., *La protezione del segreto industriale*, Sistema di Informazione per la Sicurezza della Repubblica, consulted at http://www.sicurezzanazionale.gov.it/sisr.nsf/aziende-e-sicurezza/la-protezione-del-segreto-industriale.html on 18/12/2015

Cronin A., *ISIS Is Not a Terrorist Group. Why Counterterrorism Won't Stop the Latest Jihadist Threat*, Foreign affairs, consulted at https://www.foreignaffairs.com/articles/middle-east/2015-02-16/isis-not-terrorist-group 10/10/2015

DigitPA, *Codice dell'amministrazione digitale, decreto legislativo 7 marzo 2005 n. 82*, consulted at http://archivio.digitpa.gov.it/amministrazione-digitale/CAD-testo-vigente on 7/11/2015

Dipartimento dei vigili del fuoco, del soccorso pubblico e della difesa civile, *Protezione delle infrastrutture critiche informatizzate, la realtà italiana*, consulted at http://www.vigilfuoco.it/aspx/page.aspx?IdPage=3857 on 7/11/2015

Ellyatt H., *Cyberterrorists to target critical infrastructure*, CNBC, consulted at http://www.cnbc.com/2015/01/27/cyberterrorists-to-target-critical-infrastructure.html on 13/10/2015

Enciclopedia britannica, consulted at www.britannica.com on 14/09/2015

Encyclopedia Virginia, *The pentagon*, consulted at http://www.encyclopediavirginia.org/Pentagon_The on 04/01/2016

ENISA, *Activities*, consulted at https://www.enisa.europa.eu/about-enisa/activities on 18/10/2015

ENISA, *Annual reports*, consulted at https://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/annual-reports on 18/10/2015

ENISA, *Cyber Europe 2010*, consulted at https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cce/cyber-europe/ce2010 on 19/10/2015

ENISA, *Cyber Europe 2012*, consulted at https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cce/cyber-europe/cyber-europe-2012 on 19/10/2015

ENISA, *Cyber europe*, consulted at https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cce/cyber-europe on 19/10/2015

ENISA, *Enisa cyber Europe 2014: after action report*, consulted at https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cce/cyber-europe/ce2014/ce2014-after-action-report on 19/10/2015

ENISA, *European public private partnership for resilience*, consulted at https://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/european-public-private-partnership-for-resilience-ep3r on 22/10/2015

ENISA, *National cybersecurity strategies: practical guide on development and execution*, December 2012, consulted at https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-an-implementation-guide on 18/10/2015

ENISA, *New regulation for eu cybersecurity agency enisa, with new duties*, consulted at https://www.enisa.europa.eu/media/press-releases/new-regulation-for-eu-cybersecurity-agency-enisa-with-new-duties on 20/10/2015

Eur-lex, *Communication from the Commission on a European Programme for Critical Infrastructure Protection* /***** COM/2006/0786 final */, consulted at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52006DC0786 on 20/10/2015

Eur-lex, *Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions - Network and Information Security: Proposal for A European Policy Approach* **/*** COM/2001/0298 final */, consulted at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52001DC0298 on 16/10/2015

Eur-lex, *Communication from the commission to the European parliament, the council, the european economic and social committee and the committee of the regions, A Digital Agenda for Europe* /* COM/2010/0245 f/2 */ , consulted at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52010DC0245R(01) on 21/10/2015

Eur-lex, Communication from the commission *to the European parliament and the council, The EU Internal Security Strategy in Action: Five steps towards a more secure Europe* /* COM/2010/0673 final */, consulted at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52010DC0673 on 22/10/2015

Eur-lex, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection - "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience"* {SEC(2009) 399} {SEC(2009) 400} **/*** COM/2009/0149 final */, consulted at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52009DC0149 on 21/10/2015

Eur-lex, *Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection*, consulted at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32008L0114 on 20/10/2015

Eur-lex, *Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency*, consulted at http://eur-

lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:EN:HTML on 18/10/2015

Eurojust, consulted at http://www.eurojust.europa.eu/about/background/Pages/History.aspx on 25/10/2015

European commission, *Digital Agenda for Europe*, consulted at http://ec.europa.eu/digital-agenda/digital-agenda-europe on 21/10/2015

European commission, *Europe 2020*, consulted at http://ec.europa.eu/europe2020/index_en.htm on 11/11/2015

European cyber security month, consulted at https://cybersecuritymonth.eu/about-ecsm/whats-ecsm on 25/10/2015

European Defence Agency, consulted at http://www.eda.europa.eu/Aboutus/Missionandfunctions on 22/10/2015

European Union, Joint communication to the European parliament, the council, the European economic and social committee and the committee of the regions, *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, consulted at http://eeas.europa.eu/policies/eu-cyber-security/ on 16/10/2015

EUROPOL, consulted at https://www.europol.europa.eu/content/page/about-us on 22/10/2015

Even S. and Siman-Tov D., *Cyber warfare: concepts and strategic trends*, Memorandum No.117, May 2012, consulted at http://mercury.ethz.ch/serviceengine/Files/ISN/152953/ipublicationdocument_singledocument/f3e19de1-bcf7-4d07-b088-f3d477b4329c/en/INSS+Memorandum_MAY2012_Nr117.pdf on 19/09/2015

Gagliano G., *Economia e Intelligence*, Sistema di Informazione per la Sicurezza della Repubblica, consulted at http://www.sicurezzanazionale.gov.it/sisr.nsf/approfondimenti/economia-e-intelligence.html on 17/12/2015

Garante per la protezione dei dati personali, decreto legislativo 30 giugno 2003 n. 196, *codice in materia di protezione dei dati personali*, consulted at http://garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1311248 on 6/11/2015

Gordon S. and Ford R., *Cyberterrorism?*, Symantec, consulted at https://www.symantec.com/avcenter/reference/cyberterrorism.pdf on 13/10/2015

Greco E., *Cyber war e cyber security, diritto internazionale dei conflitti informatici, contesto strategico e strumenti di prevenzione e contrasto*, Istituto di ricerche internazionali archivio disarmo (IRIAD) SIS-11/2014, consulted at http://www.archiviodisarmo.it/index.php/en/publications/magazine/magazine/finish/87/1020 on 14/09/2015

Harjani A., *Malaysia airlines says website not hacked*, CNBC, consulted at http://www.cnbc.com/2015/01/25/malaysia-airlines-site-hacked-by-cyber-caliphate.html on 14/10/2015

Helsel P., *ISIS Group Claims to Have Hacked Information on U.S. Military Personnel*, NBC News, consulted at http://www.nbcnews.com/storyline/isis-terror/isis-group-claims-have-hacked-information-military-personnel-n408236 on 14/10/2015

Hirschfeld J. and Sanger *D., Obama and Xi Jinping of China Agree to Steps on Cybertheft*, the New York times, consulted at http://www.nytimes.com/2015/09/26/world/asia/xi-jinping-white-house.html?ribbon-ad-idx=9&rref=world/asia&module=Ribbon&version=context&region=Header&action=click&contentCollection=Asia%20Pacific&pgtype=article&_r=1 on 11/10/2015

Homeland security, *National infrastructure advisory council*, consulted at http://www.dhs.gov/national-infrastructure-advisory-council on 15/09/2015

Il cyber bullismo, *La storia di Rheate Parson*, consulted at http://www.ilcyberbullismo.it/storia-rehtaeh-parsons/ on 10/10/2015

Instoria, *Stati Uniti e Cina*: *dal silenzio diplomatico al viaggio di Nixon in Cina*, consulted at http://www.instoria.it/home/stati_uniti_cina.htm on 11/12/2015

Interlex, Law n. 547 of the 23th December 1993, *Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica*, consulted at http://interlex.it/testi/l547_93.htm on 3/11/2015

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione (ISCOM), consulted at http://www.isticom.it/ on 5/11/2015

Klingner B., The U.S. Needs to Respond to North Korea's Latest Cyber Attack , the Heritage foundation, consulted at http://www.heritage.org/research/reports/2015/03/the-us-needs-to-respond-to-north-koreas-latest-cyber-attack on 9/10/2015

La Stampa, *Renzi:" Rafforzeremo la cyber security"*, consulted at http://www.lastampa.it/2015/11/28/italia/cronache/renzi-cybersecurity-contro-il-terrorismo-lKwzk6SjSw277rQaAtGquM/pagina.html on 23/01/2016

Levine M., *OPM Hack: Top Lawmaker Says US 'Under Attack'* , ABC News, consulted at http://abcnews.go.com/Politics/opm-hack-top-lawmaker-us-attack/story?id=31797366 on 12/10/2015

Linkedin, *Keypoint government solutions*, consulted at https://www.linkedin.com/company/keypoint-government-solutions on 12/10/2015

Mail online, *Islamic State's chilling hit list: Terror group hacks personal details of hundreds of military, political and diplomatic personnel and posts them online urging local extremists to kill them… including EIGHT Australians*, consulted at

http://www.dailymail.co.uk/news/article-3195139/The-chilling-ISIS-hitlist-Terror-group-hacks-publish-personal-details-hundreds-military-political-diplomatic-personnel-urges-local-extremists-kill-including-EIGHT-Australians.html on 15/10/2015

Mammoliti R., *Poste italiane impegno nella cybersecurity, sicurezza delle informazioni*, 2015, consulted at http://forges.forumpa.it/assets/Speeches/14416/07_co_04_mammoliti_rocco.pdf on 19/12/2015

Marquardt A., *Latest Arab-Israeli conflict is growing cyberwar*, ABC News, consulted at http://abcnews.go.com/blogs/headlines/2012/01/latest-arab-israeli-conflict-is-growing-cyberwar/ on 9/10/2015

Martinez L., *Russia is main suspect in cyber attack on joint staff's emails, US official says*, ABC news, consulted at http://abcnews.go.com/Politics/russia-main-suspect-cyber-attack-joint-staffs-emails/story?id=32939784 on 12/10/2015

Matteucci N., *Stato*, Treccani enciclopedia, consulted at http://www.treccani.it/enciclopedia/stato_(Enciclopedia-del-Novecento)/ on 18/12/2015

Mele S., *I principi strategici delle politiche di cyber security*, Sistema di Informazione per la Sicurezza della Repubblica, consulted at http://www.sicurezzanazionale.gov.it/sisr.nsf/approfondimenti/principi-strategici-delle-politiche-di-cyber-security.html on 26/10/2015

Mele S., *La cooperazione tra pubblico e privato nella cyber security: punti di forza e criticità per la sicurezza nazionale*, Sistema di Informazione per la Sicurezza della Repubblica, consulted at http://www.sicurezzanazionale.gov.it/sisr.nsf/approfondimenti/la-cooperazione-pubblico-privato-nella-cyber-security.html on 26/10/2015

Ministero dell'economia e delle finanze, *Legge di stabilità 2016*, consulted at http://www.mef.gov.it/focus/article_0014.html on 23/01/2016

Ministero della difesa, *CERT difesa*, consulted at http://www.difesa.it/SMD_/Staff/Reparti/II/CERT/Pagine/Chi_Siamo.aspx on 13/11/2015

Ministero dello sviluppo economico, decreto interministeriale 14 gennaio 2003, *Istituzione osservatorio permanente per la sicurezza e la tutela delle reti e delle telecomunicazioni*, consulted at http://www.sviluppoeconomico.gov.it/index.php/it/normativa/decreti-interministeriali/2017545-decreto-interministeriale-14-gennaio-2003-istituzione-osservatorio-permanente-per-la-sicurezza-e-la-tutela-delle-reti-e-delle-telecomunicazioni on 5/11/2015

Minsky A., *'Anonymous' claims responsibility for cyber attack that shut down government websites*, Global News, consulted at http://globalnews.ca/news/2060036/government-of-canada-servers-suffer-cyber-attack/ on 11/10/2015

Mohammed A., Spetalnick M., Hosenball M., *Exclusive: U.S. weighs sanctioning Russia as well as China in cyber attacks*, Reuters, consulted at http://www.reuters.com/article/2015/09/01/us-usa-cybersecurity-russia-exclusive-idUSKCN0R12FE20150901 on 13/10/2015

Moises N., *Cyber war puts democracies on the defensive*, Defesanet, consulted at http://www.defesanet.com.br/en/e_ciber/noticia/19585/Cyber-War-Puts-Democracies-on-the-Defensive/ on 12/10/2015

Moises N., *Why Cyber War Is Dangerous for Democracies*, The Atlantic, consulted at http://www.theatlantic.com/international/archive/2015/06/hackers-cyber-china-russia/396812/ on 13/10/2015

Morbidelli M., *Intelligence economica e competitività nazionale*, consulted at http://www.difesa.it/SMD_/CASD/IM/CeMiSS/Pubblicazioni/OsservatorioStrategico/Documents/31609_paper10_05.pdf on 20/11/2015

National assembly, Bill 78, *An act to enable students to receive instruction from the postsecondary institutions they attend*, 2012, consulted at http://www2.publicationsduquebec.gouv.qc.ca/dynamicSearch/telecharge.php?type=5&file=2012C12A.PDF on 10/10/2015

National security agency, consulted at www.nsa.gov on 15/09/2015

Nomisma società di studi economici, *29 settembre 2015 – Rapporto Industria Cyber Security – Nomisma/ITWay*, consulted at http://www.nomisma.it/index.php/it/press-area/comunicati-stampa/item/1007-29-settembre-2015-rapporto-industria-cyber-security-nomisma-itway/1007-29-settembre-2015-rapporto-industria-cyber-security-nomisma-itway on 19/12/2015

Normattiva, decreto legislativo 11 aprile 2011 n. 61, *Attuazione della Direttiva 2008/114/CE recante l'individuazione e la designazione delle infrastrutture critiche europee e la valutazione della necessita' di migliorarne la protezione*, consulted at http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2011;061 on 11/11/2015

North Atlantic Treaty Organization, consulted at http://www.nato.int/ on 7/10/2015

Official journal of the European Union, *Regulation (EU) No 526/2013 of the european parliament and of the council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004* , consulted at http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:JOL_2013_165_R_0041_01&qid=1397226946093&from=EN on 19/10/2015

Paganini P., *Another computer system at the Pentagon has been hacked*, Security Affairs, consulted at http://securityaffairs.co/wordpress/40039/cyber-crime/pentagon-hacked-again.html on 7/10/2015

Parlamento italiano, decreto legislativo 1 agosto 2003 n. 259, *Codice delle comunicazioni elettroniche*, consulted at http://www.parlamento.it/parlam/leggi/deleghe/03259dl.htm on 6/11/2015

Parlamento italiano, Law n. 269 of the 3rd august 1998, *Norme contro lo sfruttamento della prostituzione, della pedopornografia, del turismo sessuale in danno di minori*, consulted at http://www.camera.it/parlam/leggi/98269l.htm on 3/11/2015

Parlamento italiano, legge 31 luglio 2005 n. 155, *Conversione in legge, con modificazioni, del decreto-legge 27 luglio 2005, n. 144, recante misure urgenti per il contrasto del terrorismo internazionale*, consulted at http://www.camera.it/parlam/leggi/05155l.htm on 8/11/2015

Parliament of Canada, Bill c-51 , *An Act to enact the Security of Canada Information Sharing Act and the Secure Air Travel Act, to amend the Criminal Code, the Canadian Security Intelligence Service Act and the Immigration and Refugee Protection Act and to make related and consequential amendments to other Acts*, consulted at http://www.parl.gc.ca/HousePublications/Publication.aspx?DocId=6932136&Col=1&File=4 on 9/10/2015

Perez E. and Prokupecz S., *How the U.S. thinks Russians hacked the White House*, CNN politics, consulted at http://edition.cnn.com/2015/04/07/politics/how-russians-hacked-the-wh/ on 8/10/2015

Peterson A., *OPM says 5.6 million fingerprints stolen in cyberattack, five times as many as previously thought*, The Washington post, consulted at https://www.washingtonpost.com/news/the-switch/wp/2015/09/23/opm-now-says-more-than-five-million-fingerprints-compromised-in-breaches/ on 14/10/2015

Polizia di stato, Commissariato di P.S. online, CNAIPC, consulted at https://www.commissariatodips.it/profilo/cnaipic.html on 9/11/2015

Poste italiane, *Cybersecurity*, consulted at http://www.posteitaliane.it/it/innovazione/cyber_security/index.shtml on 19/12/2015

Presidenza del consiglio dei ministri, dipartimento per l'innovazione e la tecnologia, direttiva 16 gennaio 2002, *Sicurezza informatica e delle telecomunicazioni nelle pubbliche amministrazioni*, consulted at http://www.frareg.com/news/legislazione/privacy/direttiva_16012002.pdf on 4/11/2015

Primadanoi, *Carrai, l'amico di Renzi e il nuovo incarico alla cyber security,* consulted at http://www.primadanoi.it/news/italia/564244/Carrai--l-amico-di-Renzi.html on 23/01/2016

Ricerca giuridica, *Art. 16-bis sicurezza e integrità*, consulted at http://www.ricercagiuridica.com/codici/vis.php?art=16-bis&codice=comunicazioni%20elettroniche on 7/11/2015

Rizzini Cancarini P., *Cina, Stati Uniti e cyber security: anno nuovo, vita nuova?,* Il caffè geopolitico, consulted at http://www.ilcaffegeopolitico.org/15081/cina-stati-uniti-e-cyber-security-anno-nuovo-vita-nuova on 12/12/2015

Rizzini Cancarini P., *Cina, Stati Uniti e cyber security: anno nuovo vita nuova?,* Il caffè geopolitico, consulted at http://www.ilcaffegeopolitico.org/15139/cina-stati-uniti-e-cyber-security-anno-nuovo-vita-nuova-ii on 12/12/2015

RT question more, *ISIS releases 'hit list of US military personnel', claims hacking victory*, consulted at https://www.rt.com/news/312270-isis-hackers-us-military/ on 14/10/2015

RT question more, *'Terrorist hacker' from Kosovo faces charges for giving US troops' IDs to ISIS* , consulted at https://www.rt.com/news/318825-terrorist-hacker-kosovo-arrested/ on 14/10/2015

Salmon T., *Tip of the spear: phishing or spearphishing?*, Fishnet security, consulted at https://www.fishnetsecurity.com/6labs/blog/tip-spear-phishing-or-spearphishing on 10/10/2015

Sanger D., *Cyberthreat Posed by China and Iran Confounds White House*, the New York Times, consulted at http://www.nytimes.com/2015/09/16/world/asia/cyberthreat-posed-by-china-and-iran-confounds-white-house.html?ref=world&_r=1 on 11/10/2015

Shinkman P., *Reported Russian Cyber Attack Shuts Down Pentagon Network*, US News, consulted at http://www.usnews.com/news/articles/2015/08/06/reported-russian-cyber-attack-shuts-down-pentagon-network on 12/10/2015

Sistema di Informazione per la Sicurezza della Repubblica, *2013 Italian cyber security report critical infrastructure and other sensitive sectors readiness*, consulted at http://www.sicurezzanazionale.gov.it/sisr.nsf/sicurezza-in-formazione/la-cyber-security-in-italia.html on 18/10/2015

Sistema di Informazione per la Sicurezza della Repubblica, *Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale*, consulted at http://www.sicurezzanazionale.gov.it/sisr.nsf/archivio-notizie/direttiva-sulla-sicurezza-cibernetica.html on 25/10/2015

Sistema di informazione per la sicurezza della repubblica, *Direttiva 1 agosto 2015*, consulted at http://www.sicurezzanazionale.gov.it/sisr.nsf/documentazione/normativa-di-riferimento/direttiva-1-agosto-2015.html on 23/01/2016

Sistema di Informazione per la Sicurezza della Repubblica, *L'intelligence*, consulted at http://www.sicurezzanazionale.gov.it/sisr.nsf/cosa-facciamo/l-intelligence.html on 18/12/2015

Sistema di Informazione per la Sicurezza della Repubblica, *La legge 124/2007 in breve*, consulted at https://www.sicurezzanazionale.gov.it/sisr.nsf/documentazione/la-legge-1242007-in-breve.html on 25/10/2015

Sistema di Informazione per la Sicurezza della Repubblica, *National strategic Framework for cyberspace security*, consulted at http://www.sicurezzanazionale.gov.it/sisr.nsf/archivio-notizie/la-cyber-strategy-italiana.html on 15/09/2015

Sistema di Informazione per la Sicurezza della Repubblica, *National Plan for cyberspace protection and ICT security*, consulted at http://www.sicurezzanazionale.gov.it/sisr.nsf/archivio-notizie/la-cyber-strategy-italiana.html on 25/10/2015

Sistema di Informazione per la Sicurezza della Repubblica, *Relazione sulla politica dell'informazione per la sicurezza 2012*, consulted at http://www.sicurezzanazionale.gov.it/sisr.nsf/relazione-annuale/relazione-al-parlamento-2012.html on 28/12/2015

Sistema di Informazione per la Sicurezza della Repubblica, *Relazione sulla politica dell'informazione per la sicurezza 2013*, consulted at http://www.sicurezzanazionale.gov.it/sisr.nsf/relazione-annuale/relazione-al-parlamento-2013.html on 28/12/2015

Sutter J., *Anonymous declares 'cyberwar' on Israel*, CNN, consulted at http://edition.cnn.com/2012/11/19/tech/web/cyber-attack-israel-anonymous/ on 9/10/2015

The Federal Bureau of Investigation, consulted at https://www.fbi.gov/about-us/quick-facts on 12/10/2015

The Guardian, *NSA tried Stuxnet cyber-attack on North Korea five years ago but failed*, consulted at http://www.theguardian.com/world/2015/may/29/us-stuxnet-cyber-attack-north-korea-failure on 12/10/2015

Theohary C. and Rollins J., *Cyberwarfare and cyber terrorism: in brief*, Congressional research service, 2015, consulted at https://www.fas.org/sgp/crs/natsec/R43955.pdf on 8/10/2015

Thielamn S., *Chinese hack of US national security details revealed days after Russian hack*, The Guardian, consulted at http://www.theguardian.com/world/2015/aug/10/chinese-national-security-officials-hack on 13/10/2015

Treccani la cultura italiana, *Guerra asimmetrica*, consulted at http://www.treccani.it/vocabolario/guerra-asimmetrica_(Neologismi)/ on 16/12/2015

US department of state, office of the historian, *Cronology of us-china relations, 1784-2000*, consulted at https://history.state.gov/countries/issues/china-us-relations on 11/12/2015

Viebeck E., *Russian hackers got Obama's schedule in White House cyberattack*, The Hill, consulted at http://thehill.com/policy/cybersecurity/238127-white-house-state-dept-cyberattacks-linked on 8/10/2015

William M., *North Korea threatens cyber attacks on US*, PC world, consulted at http://www.pcworld.com/article/2933672/north-korea-threatens-cyber-attacks-on-us.html on 11/10/2015

Winter M. and Brook T., *Hackers penetrated Pentagon email* , USA today, consulted at http://www.usatoday.com/story/news/nation/2015/08/06/russia-reportedly-hacks-pentagon-email-system/31228625/ on 12/10/2015

Wordreference, consulted at http://www.wordreference.com/it/ on 28/01/2015