Università
Ca'Foscari
Venezia

—

Ca' Foscari
Dorsoduro 3246
30123 Venezia

Master's Degree programme – Second Cycle
(*D.M. 270/2004*)
in International Relations

Final Thesis

Concepts of International Relations applied to cyberspace: sovereignty, war and diplomacy in the digitized age

Supervisor
Ch. Prof. Matteo Legrenzi

Graduand
Luigi Ferdinando Treggiari
Matriculation Number 847628

Academic Year
2015 / 2016

Index

Abstract

L’idea di questa tesi nasce dalla constatazione che l’ambito della sicurezza internazionale si stia ampliando considerevolmente: lo spettro dei fenomeni destabilizzanti per il sistema internazionale sembra comprendere realtà sempre più ‘ibride’ e diverse rispetto ai parametri tradizionali delle relazioni internazionali. Mentre i conflitti inter-statali si fanno sempre più rari e il ricorso alla guerra sempre meno attraente, sono le più disparate entità non-statali (organizzazioni ‘orizzontali’ più o meno strutturate, ma anche singoli individui) a costituire la più grave minaccia alla sicurezza globale. In questo contesto, la sicurezza dello Stato è strettamente correlata a quella dei suoi cittadini: ogni attacco nei confronti di individui e, più in generale, delle società civili viene avvertito dai governi come minaccia alla sicurezza nazionale. Si pensi al fenomeno del terrorismo islamico, alle guerre seguite agli attacchi dell’11 settembre 2001 ed agli attentati compiuti da estremisti appartenenti allo Stato Islamico di Siria e Iraq in suolo europeo (Parigi e Bruxelles); ma si pensi anche ai conflitti interni, politici e religiosi, che coinvolgono i gruppi insurrezionalisti.

Ad essere colpita e indebolita da questi fenomeni di guerra ‘ibridi’ e asimmetrici è soprattutto la sovranità nazionale. L’intreccio delle risposte nazionali e globali a questo nuovo genere di aggressioni condiziona il panorama della sicurezza internazionale, rimettendo in discussione i tradizionali poteri attribuiti agli Stati. In questo contesto rilevano non poco anche le minacce provenienti dal cyberspazio. Esse rappresentano un pericolo concreto per le società moderne: l’avvento, nell’ultimo ventennio, delle tecnologie di informazione e comunicazione (ICTs, “information and

communication technologies") ha comportato importanti cambiamenti in ogni campo di attività delle società moderne. Interazioni di tipo economico, politico e sociale, che un tempo avvenivano solamente nella dimensione fisica, si svolgono oggi in larga misura nell'orizzonte digitale; di conseguenza, anche i governi hanno trasferito attività e servizi nel mondo virtuale. La natura intrinsecamente aperta e senza confini del cyberspazio non ha soltanto portato indubbi vantaggi alle attività economiche e alle società globali, ma ha anche ampliato il raggio d'influenza del processo globalizzante. Allo stesso modo, però, la diffusione di internet e la crescita del numero dei suoi utenti ha anche contribuito al moltiplicarsi dei pericoli provenienti dal web: il prolificare di malware (software dannoso per il sistema operativo) con scopi sia criminali che politici e militari, ha contribuito a inserire nelle politiche strategiche e di sicurezza (e talvolta anche in quelle militari) il tema della sicurezza informatica dei governi di quasi tutto il mondo. Una ricerca condotta nel 2012 dall'Istituto di ricerca delle Nazioni Unite sul disarmo (UNIDIR) ha infatti dimostrato che tra i 193 paesi membri delle Nazioni Unite, 114 avevano intrapreso programmi relativi alla sicurezza informatica. Tra questi, 47 avevano creato corpi all'interno delle forze armate dedicati ad operazioni nel cyberspazio; altri 67 invece avevano programmi di tipo prettamente civile. La stessa ricerca indica che 12 dei 15 maggiori investitori nell'apparato militare abbiano già, o stiano per acquisire capacità offensive derivate da mezzi informatici. In questo contesto, Stati Uniti, Regno Unito, Cina, Russia e Francia sono i paesi più avanzati in termini di potere e capacità informatiche con finalità strategiche e militari.

Il cyberspazio è dunque diventato il nuovo contesto strategico in cui nuove forme di potere e di interazione tra entità statali e non-statali si creano e si consumano, ridefinendo il panorama della sicurezza internazionale nel ventunesimo secolo.

Focus di questa tesi è appunto il fenomeno della 'cyberizzazione' delle relazioni internazionali: il termine si riferisce sia all'inclusione del tema della sicurezza informatica e più in generale, delle nuove tecnologie nelle politiche strategiche a livello internazionale, sia al processo stesso di cambiamento che il concetto di relazioni internazionali, storicamente collegabile solamente allo stato-nazione, subisce nel contesto virtuale. La tesi approfondisce l'analisi di questo processo, prendendo in esame quattro concetti di relazioni internazionali (sovranità, potere, guerra e diplomazia), esaminando la trasformazione che tali concetti subiscono una volta inseriti nel cyberspazio e identificando le sfide più rilevanti che impegnano oggi la comunità internazionale.

L'importanza strategica del cyberspazio si può dunque ricollegare alla più ampia questione della sicurezza internazionale contemporanea: il progressivo aumento di potere e di influenza da parte di entità non-statali. Il cyberspazio rappresenta la piattaforma d'eccellenza per queste entità: le possibilità di agire anonimamente, l'infinito spazio d'azione e l'azzeramento delle distanze conferiscono a soggetti e gruppi organizzati un potere non ottenibile nel mondo reale. Nella dimensione virtuale, lo stato sovrano si trova a competere con entità non-statali che approfittano dei mezzi offerti dall'architettura digitale di internet per promuovere i propri interessi e per compiere operazioni mirate allo spionaggio, al sabotaggio e alla destabilizzazione. Si pensi a questo proposito all'effetto causato nelle relazioni inter-statali dalle rivelazioni di WikiLeaks, oppure alle infiltrazioni in network contenenti informazioni riservate e sensibili da parte del gruppo Anonymous. Tutte queste circostanze contribuiscono all'apparente indebolimento dello Stato sovrano nella sua concezione Westphaliana: al cospetto del cyberspazio ed alle sue implicazioni, lo Stato si trova di fronte ad un paradosso. Da un lato, i benefici alle economie e alle società nazionali derivati dalla diffusione di internet sono capitalizzati dai governi che ne promuovono lo sviluppo; dall'altro, lo Stato percepisce la propria perdita di controllo nei confronti del flusso di informazioni e di idee trasmesse dai canali del cyberspazio. Questo è importante soprattutto relativamente al contenuto terrorista divulgato tramite internet. I terroristi, insieme ad altri soggetti, sono identificati come le principali categorie coinvolte strategicamente nel cyberspazio. Le altre identificate in questa tesi sono: gli hackers, le organizzazioni criminali, le imprese e infine i governi.

In origine, internet fu concepito nell'ambito di una ricerca per scopi militari col nome di *Agenzia per i progetti di ricerca avanzata sulle reti* (dalla sigla inglese ARPANET). Solo successivamente, dagli anni Ottanta, il progetto si rivelò essere uno dei più importanti progetti civili. L'elaborazione in forma embrionale di malware cominciò proprio in quel periodo, nonostante avesse come scopo esclusivamente quello di testare la resistenza dei sistemi operativi. Il perfezionamento del malware in termini di potenziale d'intrusione e di sofisticazione tecnologica ha tenuto lo stesso passo di quello dei sistemi operativi. Al giorno d'oggi, questo software dannoso è prevalentemente usato per attività criminali: nel 2011 Symantec (un'importante azienda informatica) ha stimato che le perdite economiche subite da individui vittime di forme di criminalità 'cyber' potrebbero ammontare a 388 miliardi di dollari ogni anno. Insieme ad attività criminali, il cyberspazio offre anche una piattaforma unica per individui politicamente motivati o con intento distruttivo, come nel caso di hackers e attivisti. La prima categoria, nonostante l'uso che ne viene spesso fatto nei media, non è da considerare necessariamente in una luce negativa: la comunità degli hacker è in realtà variegata e comprende anche informatici professionisti che offrono le loro abilità per testare i sistemi operativi e la loro resistenza a virus e ad intrusioni non autorizzate. Gli attivisti del web (come il gruppo Anonymous) fanno uso del web e dei suoi strumenti per attuare strategie d'infiltrazione e campagne politiche. Allo stesso modo, internet ha contribuito enormemente a strutturare organizzazioni terroristiche. Grazie ad esso infatti, gruppi geograficamente limitati come Al-Qaeda si sono potuti trasformare in network orizzontali, le cui modalità di reclutamento ed indottrinamento diventano disponibili ad utenti in tutto il mondo.

Gli Stati operano nel cyberspazio su livelli distinti. Da un lato, si cimentano nel cyberspazio per operazioni mirate alla lotta alla criminalità e per rimuovere contenuti ritenuti indesiderabili (di stampo terroristico o pedopornografico, per esempio); dall'altro, utilizzano l'ambito 'cyber' per compiere operazioni di tipo strategico come lo spionaggio, ma anche azioni militari con mezzi informatici. Quest'ultima dimensione è al giorno d'oggi realtà: il Dipartimento della Difesa statunitense (US DoD) ha definito il cyberspazio come il quinto ambito di guerra insieme a terra, mare, aria e spazio. Alla luce di questo, è molto probabile che le possibilità di conflitto inter-statali nella dimensione virtuale possano aumentare pericolosamente.

Il rapporto tra sovranità e cyberspazio è affrontato nel secondo capitolo. A questo riguardo, la questione più rilevante è ricollegabile al presunto processo di erosione della sovranità a causa dell'ampliamento del fenomeno della globalizzazione. Lo Stato si troverebbe incapace di controllare funzionalità sovrane a causa dell'interconnessione tra fenomeni politici, economici e sociali a livello globale. Questa interpretazione è applicabile al contesto cyber solo a metà: se da un lato la perdita di controllo esclusivo sui flussi di informazione e di idee trasmesse tramite il cyberspazio è un fenomeno concreto (si pensi, per esempio, non solo ai contenuti terroristici, ma anche ai messaggi religiosi e politici considerati dannosi da parte delle autorità), dall'altro lo Stato, nell'arena internazionale, continua a preservare il proprio status di unico soggetto titolare dei poteri sovrani nei confronti dei propri cittadini e nel relazionarsi con gli altri Stati nella comunità internazionale. I processi tecnologici, insieme al rafforzarsi dell'ideologia globalizzante, contribuiscono però a rendere il concetto di sovranità, intensa nella sua accezione tradizionale, particolarmente compromessa nell'ambito virtuale. Per lo Stato sovrano quindi, le sfide provenienti dal cyberspazio sono considerate urgenti, perché potenzialmente distruttive.

L'analisi su cyberspazio e sovranità include considerazioni di diritto internazionale; in particolare, l'ipotesi secondo cui intrusioni non autorizzate all'interno di network governativi con scopi offensivi o di spionaggio da parte di agenzie di intelligence e militari straniere o entità non-statali rappresentino violazioni della sovranità territoriale, come stabilito dalla Carta delle Nazioni Unite. A questo proposito, la conclusione a cui si perviene è che le intrusioni per mezzi informatici da parte di entità terze rispetto allo Stato non costituiscano violazioni vere e proprie, in quanto gli effetti di tali fenomeni non sono direttamente visibili. Inoltre, molto spesso è quasi impossibile risalire alla fonte dell'attacco o dell'operazione (grazie proprio agli strumenti tecnici offerti dall'architettura digitale per l'oscuramento dell'identità e della provenienza). Attribuire un'azione informatica ad un soggetto definito è dunque un processo tecnicamente complesso e politicamente rischioso: la questione dell'attribuzione rimane tutt'ora l'ostacolo più importante nella regolamentazione del comportamento statale nel cyberspazio. Il parametro prevalente in questi casi è dunque l'approccio basato sugli *effetti*: le azioni eseguite per mezzi informatici a danni di uno Stato sono riconosciute come violazioni della sovranità solo nel caso in cui queste producono effetti concreti, visibili e di lungo termine. Più in generale, la conclusione che viene raggiunta è che le violazioni di sovranità che avvengono nel cyberspazio, nonostante avvengano continuamente, siano riconducibili a violazioni di livello basso, ovvero sporadiche e con effetti di corto o medio termine. Nonostante ciò, l'esigenza da parte degli Stati di regolarizzare questi fenomeni è quanto mai urgente: il diritto internazionale attualmente vigente non fornisce risposte adeguate a circostanze moderne ed in evoluzione, come nel caso del cyberspazio.

Il concetto di potere associato agli Stati e le sue implicazioni nel cyberspazio è affrontato nel terzo capitolo. L'ambito virtuale, in questo caso, serve da piattaforma per la promozione e per la delegittimazione di idee politiche, o al consolidamento di altre già affermate. Anche qui, la questione più rilevante riguarda ancora le entità non-statali: nel cyberspazio gli Stati si trovano a competere con entità di altro tipo per influenza e capacità d'azione. La moltiplicazione di questi soggetti, prevalentemente hackers, attivisti ed estremisti, preoccupa particolarmente i governi: la diffusione di potere che caratterizza il sistema globale del ventunesimo secolo fa sì che nel cyberspazio il margine tra Stati ed entità non-statali in termini di potere si faccia sempre più piccolo. Inoltre, la dimensione globale del cyberspazio contribuisce alla crescente difficoltà per i governi di controllare i propri confini, sia fisici che politici, nella sfera digitale. Questo senso di preoccupazione si manifesta, per esempio, nel crescente intervento statale sulle attività che si svolgono su internet, spesso collaborando con gestori di servizi digitali per impedire che determinate categorie di persone o di contenuti possano trovare spazio nei domini del web nazionale. Inoltre, i mezzi offerti dal cyberspazio permettono ai governi di esercitare un sempre maggiore controllo su internet. Questo fenomeno è testimoniato, per esempio, dall'estensivo programma di sorveglianza di massa operata dalla National Security Agency (NSA) statunitense rivelata da Edward Snowden nel 2013, oppure dal rigido sistema di controllo operato dalle autorità cinesi sul traffico internet nazionale e su quello proveniente dall'estero. Tutte queste modalità rappresentano tentativi di ripristinare l'autorità sovrana nell'ambito virtuale e di imporre quindi il potere esclusivo dello Stato, spesso però a scapito delle libertà civili degli utenti.

Tutti gli attori impegnati strategicamente nel cyberspazio possiedono l'abilità di esercitare forme di 'hard' e 'soft' power, come categorizzato da Joseph Nye. Forme di *soft power* sono lo strumento prediletto per l'irradiazione del potere dello Stato nel cyberspazio, sia all'interno dello stesso ambito virtuale che in quello fisico attraverso la creazione di standard internazionali di sicurezza e comportamentali in internet; allo stesso tempo, però, esse sono sempre di più utilizzate da entità non-statali per la propagazione di messaggi anti-sistema (ad opera per esempio di estremisti). Le rivelazioni di WikiLeaks nel 2010, per fare un esempio famoso, rappresentano un'efficace forma di *soft power*, che ha contribuito in modo importante a destabilizzare le relazioni inter-statali. Allo stesso modo, nel futuro, entità non-statali potranno, alla stregua degli Stati, utilizzare forme coercitive di potere ('hard') ricorrendo a mezzi informatici offensivi. In questo stesso capitolo si evidenzia altresì come per gli Stati sia possibile fare uso di entità non-statali attive nel cyberspazio (come criminali e hackers) per rafforzare il proprio potere 'cyber'. È questo il caso della Cina, in cui gli hackers sono sospettati di essere diretti dal governo; e della Russia, che invece approfitterebbe dell'expertise di individui coinvolti in attività criminali sul web includendoli nelle proprie operazioni informatiche.

Il tema della guerra cibernetica è affrontato nel quarto capitolo. Questo fenomeno, nonostante venga notevolmente inflazionato dagli accademici e dagli strateghi, non rappresenta più solamente uno scenario ipotetico: negli ultimi vent'anni, azioni offensive derivate da mezzi informatici hanno avuto effetti rilevanti per le economie nazionali e hanno conseguentemente trovato ampi spazi di discussione nelle politiche di sicurezza di tutto il mondo. In ambito militare le operazioni informatiche vengono sempre più impiegate in coordinamento con quelle convenzionali: basti pensare all'estensivo uso nelle guerre al terrore dei droni, ovvero dispositivi elettronici manovrati manualmente a distanza. Nel dibattito sull'esistenza o meno della guerra cibernetica, l'approccio proposto in questa tesi è mediano: mentre una guerra cibernetica in quanto tale è improbabile, nel futuro i mezzi informatici verranno utilizzati sempre di più.

I fenomeni attuali riguardanti infiltrazioni in network militari e governativi, insieme all'estensivo uso di spionaggio e controspionaggio tramite mezzi informatici, servirebbero in questo senso a preparare il campo di battaglia a modalità di guerra inedite e con esiti potenzialmente distruttivi. La prima arma cibernetica di cui il mondo è venuto a conoscenza è chiamata Stuxnet: questo malware provocò nel 2007 l'arresto temporaneo del programma nucleare iraniano, infettando il sistema informatico che provvedeva al funzionamento delle centrifughe per l'arricchimento dell'uranio all'interno della stazione nucleare di Natanz, in Iran. La sofisticatezza di quest'arma informatica, insieme alla specificità della sua programmazione (ovvero quella di compromettere il sistema di controllo automatico computerizzato di processi industriali) e al suo fine strategico ha provocato allarme nella comunità internazionale: il sospetto che prodotti simili possano essere sviluppati non solo da entità statali, ma anche non-statali, contribuisce ad ampliare possibilità che i conflitti nel cyberspazio si intensifichino a tal punto da destabilizzare il sistema internazionale nel suo insieme. A ciò hanno anche contribuito numerosi casi di conflitti inter-statali tramite mezzi informatici avvenuti negli ultimi dieci anni, che sono elencati cronologicamente all'interno del capitolo. Tra questi, gli attacchi cibernetici contro i sistemi operativi delle istituzioni estoni nel 2007 e contro i siti governativi georgiani nel contesto della guerra contro la Russia nel 2008 rappresentano gli esempi più concreti di guerra cibernetica. È doveroso specificare però che fino ad adesso nessun attacco cibernetico ha avuto gli stessi effetti di uno convenzionale, ovvero danni concreti a beni ed infrastrutture critiche di uno Stato o alla sua popolazione. Il caso di Stuxnet è quello che si avvicina di più a questo scenario, ma ne rimane tuttavia ancora lontano. A complicare ulteriormente lo scenario è anche e soprattutto la già citata questione dell'attribuzione. Nonostante ciò, lo spettro di una guerra cibernetica affligge i governi e le comunità strategiche di tutto il mondo; anche la comunità internazionale ha intrapreso iniziative per regolare le capacità informatiche degli Stati con scopi offensivi e per adattare il diritto internazionale vigente a scenari di guerra cibernetica. A questo proposito, un gruppo di esperti appartenenti al Cooperative Cyber Defence Centre of Excellence, un organo della NATO con sede a Tallinn, ha elaborato uno studio accademico e non vincolante su come il diritto internazionale (in particolare lo *jus ad bellum* e il diritto umanitario internazionale) si possa applicare nel contesto di una guerra cibernetica: il Manuale di Tallinn, pubblicato nel 2013. Nonostante il carattere non vincolante e il fatto che non venga condiviso unanimemente, il Manale testimonia la direzione che una cospicua parte della comunità internazionale intende prendere nei confronti della guerra cibernetica. Il Manuale inoltre cerca di fare chiarezza su alcuni dei punti più controversi riguardanti questo tema, ovvero se un attacco cibernetico possa essere equiparato ad un attacco convenzionale, facendo scattare quindi il diritto di ogni Stato ad invocare l'autodifesa. Questo punto viene analizzato approfonditamente nel capitolo, non solo facendo riferimento alle varie implicazioni contenute nella Carta delle Nazioni Unite e alla giurisprudenza della Corte Internazionale di Giustizia, ma anche contestualizzando la guerra cibernetica col pensiero strategico classico sulla guerra, utilizzando in particolare la definizione fornita da Clausewitz.

Il compito di regolare le spinte conflittuali e di arginare le capacità offensive degli Stati sta dunque alla comunità internazionale: il negoziamento e la discussione di temi riguardanti l'ambito 'cyber' per la regolamentazione della sicurezza informatica prende il nome di 'cyber diplomacy', che è l'argomento affrontato nel quinto ed ultimo capitolo.

Questo filone della politica estera, nonostante non si sia stabilito definitivamente, è in continuo ampliamento e ha come primo obiettivo quello di colmare le lacune politiche e legali che caratterizzano il campo della sicurezza informatica a livello internazionale. Il tema della sicurezza informatica è stato introdotto per la prima volta nelle Nazioni Unite nel 1998 dalla Federazione Russa, ma da quel momento la formulazione di strategie nell'ambito di quell'istituzione ha visto la contrapposizione di blocchi opposti: piani condivisi per la definizione di regole riguardanti l'uso governativo di tecnologie d'informazione e comunicazione hanno spesso incontrato resistenze sia per ragioni politiche che per il contenuto che per la forma, in relazione, ad esempio, alla terminologia usata (gli Stati Uniti si riferiscono alla sicurezza informatica col termine "cybersecurity", mentre la Russia predilige quello di "information security"). La questione più rilevante in questo senso è infatti proprio l'assenza di un accordo universale condiviso da tutti i membri della comunità internazionale su norme di comportamento responsabile nel cyberspazio e sulla regolamentazione dello sviluppo di capacità offensive. Ciò è dovuto in gran parte alle ampie divergenze sulla direzione politica da dare al cyberspazio, in particolare sulle autorità che regolano il traffico globale di internet e su quali principi di diritto internazionale basare l'azione statale nella sfera virtuale. Questa situazione rende il cyberspazio un contesto in cui gli Stati sono lasciati al proprio giudizio, rendendo di conseguenza l'ambiente digitale anarchico e competitivo. Allo stesso tempo, però, gli Stati non sembrano volersi impegnare formalmente e sottostare a norme vincolanti riguardanti il comportamento da seguire nel cyberspazio: ciò infatti escluderebbe per loro le enormi e vantaggiose opportunità strategiche offerte dal mondo virtuale. Alla luce di questa situazione, nel capitolo viene evidenziato come gli Stati si rivolgano a mezzi alternativi e meno invasivi per sviluppare norme comportamentali non vincolanti che influenzino gli altri soggetti della comunità internazionale affinché si instauri un regime consuetudinario. Particolarmente efficaci in questo senso si sono rivelate quelle misure che contribuiscono ad instaurare fiducia reciproca tra parti in conflitto per scongiurare l'insorgere di conflitti armati, concepite all'epoca della Guerra Fredda e adattate per il contesto cibernetico. Queste misure ("Confidence and Security Building Measures") vengono sviluppate soprattutto all'interno di istituzioni multilaterali di tipo regionale: la convergenza di Stati con prospettive politiche ed economiche simili all'interno di organismi cooperativi fa sì che le norme comportamentali per il cyberspazio siano coerenti ed efficaci. Allo stesso tempo però, questo fenomeno contribuisce alla polarizzazione delle posizioni nei confronti della sicurezza informatica a livello internazionale, che riguarda in particolar modo il dibattito sull'internet governance. In ultima analisi, nel capitolo viene esposto un caso studio sulla Strategia Europea per la Cybersecurity del 2013 come esempio di una raccolta di norme e misure riguardanti la sicurezza informatica condivise da una moltitudine di paesi facenti parte un'entità influente come l'Unione Europea. La presentazione della Strategia è arricchita da informazioni e materiale reperito personalmente grazie all'esperienza di tirocinio fatta al Parlamento Europeo dal settembre 2015 al marzo 2016 nell'ufficio del Direttore Generale del Direttorato Generale ITEC (Innovation and Technological Support). In quel periodo venivano infatti discusse, in seno alle commissioni parlamentari e a workshop ed eventi specifici, questioni inerenti alla Strategia come la direttiva sulla sicurezza delle reti e dell'informazioni dell'UE e il Mercato Digitale Unico. Alla Strategia è dunque dedicato uno spazio importante e approfondito all'interno del capitolo sulla cyber diplomacy.

In conclusione, lo scopo ultimo di questa tesi è dimostrare come i fenomeni di potere e conflitto che si producono nel cyberspazio influenzino il mondo reale e in particolare il panorama della sicurezza internazionale. L'analisi procede esaminando le sfide che concetti consolidati di relazioni internazionali si trovano ad affrontare una volta contestualizzati nella sfera virtuale. La conclusione è che le sfide provenienti dal cyberspazio devono essere tenute in conto dalla comunità degli Stati, soprattutto alla luce delle implicazioni per la sicurezza a livello globale. Gli effetti di eventuali attacchi cibernetici, in un contesto privo di regole, possiedono lo stesso potenziale destabilizzante e distruttivo di quelli convenzionali; ciò è ancora più vero se si pensa a quanto le infrastrutture critiche di uno Stato (per il fornimento di energia ed acqua per esempio), i processi industriali e servizi fondamentali come la salute e le transazioni finanziare siano sempre di più digitalizzati e quindi vulnerabili ad attacchi e ad infiltrazioni non autorizzate. La minaccia di scenari catastrofici è dunque attuale, e la comunità internazionale ne risentirebbe considerevolmente. I conflitti inter-statali causati da incidenti occorsi nel cyberspazio e le tensioni derivanti dalla diffusione di potere a favore di entità non-statali potrebbero pericolosamente intensificarsi e destabilizzare il sistema nel suo insieme. Questo scenario è in qualche modo già presente: gli Stati Uniti hanno già annunciato che risponderanno ad attacchi cibernetici o spionistici con qualsiasi mezzo venga ritenuto adatto, includendo quindi anche i mezzi convenzionali. La situazione che ne risulterebbe sarebbe un mondo in cui il ricorso all'uso della forza è più facile e meno controllato. Per questo motivo, la comunità internazionale deve prendere atto del fatto che l'ambito virtuale è strettamente collegato a quello reale, e che le azioni intraprese in uno dei due contesti hanno inevitabilmente conseguenze immediate nell'altro.

Introduction

Concepts of International Relations as applied to cyberspace

The proliferation of ICTs (information and communication technologies) into every field of activity in modern societies has heightened the role of information in today's world politics, which is increasingly perceived by policy makers as the strategic power resource fit to deal with the interconnected and asymmetric nature of the political, economic and social trends of the actual global system. Furthermore, it is even more relevant in the context of the current political dimension of the world, composed by a multitude of horizontal networks in which the internet plays a fundamental and innovative role. For this reason, cybersecurity - defined both as the insecurity generating from cyberspace and as the technical and non-technical practices to make it more secure[1] - is being increasingly mainstreamed into political agendas. The use of ICTs for the functioning of essential services like energy supplies, financial transactions and their extension to the military, along with the rise of extensive networking has brought about rising concerns on the potential that threats generating from cyberspace have to alter established balances of power and resources in the international system. In this sense, the cyber domain represents a paradox of opportunities and vulnerabilities: the openness of modern societies within a networked world amplifies the impact of innovative and asymmetric threats, despite the absence of conventional ones[2].

[1] Alan Collins, Contemporary Security Studies, Oxford 2013

[2] *A Strong Britain in an Age of Uncertainty: The National Security Strategy*, the United Kingdom's National Security Strategy, The Stationery Office, 2010

Cyberspace is defined as an 'informational substrate' for economic and social activities, a man-made dimension comprising of both virtual and physical features. The internet is not to be confused with cyberspace, as the two terms are at the same time interrelated and independent from one another: the former relies for its functioning on physical infrastructure, namely optic cables and servers; conversely, the latter has a rather metaphorical dimension, encompassing all the interactions and flows of information channelled through its digital architecture[3]. The advantages to economies and to global societies generated by the spread of the internet has been considerable, considering especially interaction. In cyberspace, interacting actors are connected at a nearly light-speed, and spatial distance is reduced to zero[4]. This also entails important strategic implications: the contemporaneity of cause and effect in cyberspace has considerable consequences in the exercise of power. Forms of power whose access was previously restricted by physical and temporal limits, are available in cyberspace to any interest-driven subject[5]. Fundamental in this discourse is the advent of malware. The past decade can be regarded as the temporal dimension in which malware has been developed and perfected. Malware (abbreviation for malicious software) can be deployed against any target/device that is sufficiently networked, and considering the increased reliance of critical infrastructure, military instruments and industrial processes on ICTs, the effects of informational attacks hitting such entities can potentially be as severe as those resulting from conventional ones. For this reason, cyberspace has witnessed phenomena of militarization and securitization (through the use of restrictive measures such as censorship and surveillance, for example) with an increasing number of non-State and State actors engaging in forms of conflict, espionage and

[3] David J. Betz and Tim Stevens, *Cyberspace and the State: Toward a Strategy for Cyber-Power*, The International Institute for Strategic Studies (IISS), 2011

[4] Paul Virilio, *Speed and Politics: An Essay on Dromology*, Semiotext(e), 2006

[5] Betz and Stevens 2011

sabotage[6]; at the same time, policy makers and the strategic community have called for the development of national strategies dealing with the cyber domain[7]. An increasing number of States include offensive uses of informational means in their military doctrines[8], and cyber threats are in some cases even equated to threats concerning national security. The US Department of Defense for example regards cyberspace as the fifth domain of warfare along with land, sea, air and space[9]; cyberspace is increasingly viewed as the ultimate strategic context in which brand new instruments of war are developed, and where States not only compete with each other, but also face the challenging rise of super-empowered non-State actors[10].

The strategic advantages derived from cyberspace are unprecedented: techniques for anonymization and for source concealment allow any interest-driven and technically skilled subject to carry out cyberattacks and to intrude into one's IT system for purposes of espionage and intelligence gathering, as well as for criminal and political ones. For these reasons, non-State actors such as cybercriminals and the so-called 'hacktivists' (ideologically-driven hackers) have gained considerable power in cyberspace, challenging territorial sovereignty in its traditional assumption and key sectors of national economies.

Notable instances of inter-State cyber conflicts, thoroughly highlighted by the media, have managed to bring the topic of cybersecurity into the national security discourse and into military affairs. The events that paved the way for

[6] Cybersecurity in the European Union and Beyond: Exploring the Threats and Policy Responses, study commissioned by the European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs, European Parliament, October 2015

[7] A UNIDIR research from 2012 assessed that among the 193 States componing the United Nations, 114 had established national cybersecurity programmes

[8] The United States Cyber Command (USCYBERCOM) for example is an armed forces command subordinate to the United States Strategic Command and is focused on military operations in cyberspace, along with the protection of US military networks.

[9] US Department of Defense, *Strategy for Operating in Cyberspace*, 2011

[10] Joseph S. Nye, Jr., *Cyber Power*, Belfer Center for Science and International Affairs, 2010

discussions around the advent of cyber war were the cyberattacks against Estonia in 2007, where private and governmental institutions were hit by waves of cyberattacks for three weeks, and those against Georgia in 2008, in the context of the Russian-Georgian war[11]. This last instance of conflict demonstrated, for the first time, that informational means could be effectively used along conventional ones. Equally, the Israeli air-strike that disrupted a nuclear facility in Syria was found to be successful only by disabling the Syrian air defence system through sophisticated malware[12]. Additionally, the increase in scale and impact of espionage conducted through cyberspace and the numerous breaches of corporate data and confidential material by politically-driven, virtual entities such as Anonymous and WikiLeaks, have led many States and international organizations to implement strategies for cybersecurity as well as to develop defensive and offensive cyber capabilities. This has somewhat initiated an 'arms race' in cyberspace that increases the perception of the likelihood of a 'cyber-conflict', creating this way some sort of a 'cyber' security dilemma[13]. The cyber domain has thus become the field for competitiveness and for sporadic conflicts among States that are testing their capabilities, often carrying out their actions through the use of proxies and covertly enrolling hacktivists and criminals.

In this situation, the events and interactions taking place in cyberspace are likely to affect the international system and its components by altering the established balances of power in favour of non-States actors, the distinctions between peace and war and between technology, politics and economics. The analysis on the 'cyberization' of international relations is therefore the very topic of this thesis. The 'cyberization' of international relations[14] has a twofold

[11] Richard A. Clarke and Robert Knake, *Cyber War: The Next Threat to National Security and What to Do About It* (2010)

[12] Ibid.

[13] Nye Jr. 2010

[14] Jan-Frederik Kremer, Benedikt Müller, *Cyberspace and International Relations: Theory, Prospects and Challenges*, Springer 2014

implication: on one hand, it refers to the inclusion of informational security and more broadly, of ICTs into political discussions and strategies at international level; on the other, it refers to the shifting process that concepts, related historically exclusively to statehood, face when applied to cyberspace. Four concepts of international relations are considered: sovereignty, power, war and diplomacy.

The chapter on sovereignty examines how some of its constituent features such as exclusivity of jurisdiction and absence of external interference are affected in cyberspace. The issue of cyber espionage is highlighted, as its scale and impact is being growingly perceived as a threat to national security. Additionally, particular emphasis is given to the controversial relationship between domestic sovereignty and the flow of information allowed by the internet, with regards especially to terrorist content. The chapter on power displays the ways through which a State can project its power into cyberspace and the asymmetries in distribution of power in favour of non-State actors.

The chapter on war, taking into consideration the conflictual literature and the lively debate on the topic of cyber war, holds up the employment of informational means into current military strategies as an example representing how cyber warfare is already taking place in some form. A list of notable episodes of cyberattacks generally assumed as instances of cyber conflicts between State actors is presented, and an analysis on whether such acts can be equated to armed attacks (triggering the right to self-defence) is operated considering existing international law. Moreover, a comparison with strategic theories derived from the Cold War is presented, along with a focus on the proliferation of offensive cyber weapons, namely the Stuxnet worm. Finally, the chapter on diplomacy explains the debate over internet governance, focusing on the divergent Western/Eastern perspective on the regulation of cyberspace and on the development of behavioural norms to be followed in cyberspace. It then highlights the establishment of confidence-building measures for cyberspace as a result of cooperative mechanisms and convergence of like-minded States within international organizations. Further, cooperation on cybersecurity at regional level is analysed bringing the European Strategy for Cybersecurity as a case study for capacity-building and resilience-building effort at international level.

Before getting into the main discussion of the thesis a practical, non-technical introduction on the existing types of threats and on the categories of actors operating in cyberspace will be presented. Furthermore, particular attention will be given to the case study on the European Strategy for Cybersecurity. This is due to the research work done within the European Parliament as a trainee in the Directorate-General for Innovation and Technology (ITEC) in Brussels, where thanks to the precious collaboration of the Director General and of the traineeship's supervisor the idea for the thesis was conceived and developed.

Chapter One

Threats, Tools and Actors in Cyberspace

Preface

The peculiar techniques for anonymization and obscuration of location allowed from the physical architecture of cyberspace make it possible for any interest-driven subject to engage in cyber operations with malicious purposes. Any kind of stakeholder, ranging from governments, enterprises and organizations to individuals, are involved in cyberspace, all with different interests and security concerns. Over time, advancements in technology for the digital infrastructure implied also refinements in malicious expertise, which focuses on the exploitation of vulnerabilities of IT systems in order to gain access and to carry out actions aimed at acquiring, modifying or copying information or at disrupting the system itself. Terminologies and definitions concerning actions that involve malicious uses of computer systems differ according to the institution or country that formulates them. A comprehensive definition of cyberattack is however provided by NATO, describing it as an "action taken to disrupt, deny, degrade or destroy information resident in a computer and/or computer network, or the computer and/or computer network itself"[15]. In order to counteract that, IT operators have been strengthening the security of the systems, but malicious operations are so widespread and in constant evolution as to make it challenging for authorities to effectively grant the users' complete security. Malicious operations in cyberspace vary in technical features and in impact, ranging from email spamming to cyberattacks against critical infrastructure. This chapter will

[15] Cyber Definitions, NATO Cooperative Cyber Defence Centre of Excellence website (www.ccdcoe.org/cyber-definitions)

provide with a comprehensive framework for the categorization of actors involved in cyberspace, what threats originate from it and what are the means employed.

Actors engaged in cyberspace

A wide range of stakeholders are present in cyberspace, as the spread of the use of the internet in the past two decades resulted in every activity of modern societies being totally or partly adapted to ICT technologies. Existing frameworks for the categorization of actors operating in cyberspace mostly identify them according to the outcome or to the motivation of their action[16]. A State actor for example, might be identified as such for conducting espionage activities or for sabotaging military networks belonging to a foreign country, but those actions could be put in place by any other actor. Equally, activities such as the defacement of websites or data breaches of private companies can be seen as the operation of hacktivists or cybercriminals, but any other category could be responsible. Overlapping of interests and ambiguity of intentions, combined with anonymity and the problem of attributing the source of an attack is coherent with the very nature of cyberspace, which renders problematic the linking of actions to categories of actors. Despite this, I have tried to make an exhaustive list, taking into account every category of subjects that can be relevant in this context. The list includes: individuals, hacktivists and extremists, profit-driven criminals, organizations and enterprises, and States/ intergovernmental organizations.

[16] Klimburg, Alexander & Heli Tirmaa-Klaar, *Cybersecurity and Cyberpower: Concepts, Conditions and Capabilities for Cooperation for Action within the EU*, 2011. Found in 'Cybersecurity in the European Union and Beyond: Exploring the Threats and Policy Responses', Study Commissioned by the Committee on Civil Liberties, Justice and Home Affairs (LIBE), Directorate-General for Internal Policies, European Parliament, 2015

The category of **individuals** includes users with limited technologic expertise, such as private citizens, as well as trained IT operators, including Hackers. What defines this category is the absence of any link to loosely structured or to structured organizations, meaning autonomous action. Individuals can be equally targets and perpetrators of cyber operations. In the public eye, **hackers** are generally seen as lone operators with the aim of affecting IT systems with malicious purposes, often defined as criminals or even terrorists. In reality, hackers differ among them according to the nature of their operations, differing in particular from "white-hat" to "black-hat" hackers[17]. "White-hat" hackers are individuals tasked with the authorised intrusion into IT systems in order to detect possible security vulnerabilities of operating systems. They are often employed from IT companies and from Governments, and their performance is perfectly legal. "Black-hat" hackers on the other hand, make use of their technical knowledge in order to engage in politically-motivated or financially-driven operations for pleasure or personal gain, often resulting in sabotage and blackmailing. Such actions are definitely seen as a threat by public authorities, but generally result in annoyance. Some of these skilled individuals however, might be still tempted to join organized criminal organizations online[18]. There exists another category in between the two, the "grey-hat" hackers. These individuals contribute to the well-being of the internet, fighting malware developers and spammers. Although their actions are for the greater good of the online community, grey-hat hackers intrude into IT systems without the target's knowledge or consent, which is regarded as a criminal action.

Hacktivists are defined by the Dutch National Cyber Security Centre (NCSC) as "people who use cyberattacks to realise ideological aims or to bring such

[17] Christian Czosseck, *State Actors and Their Proxies in Cyberspace*, in Katharina Ziolkowski (ed.), Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy, NATO CCD COE Publication, Tallinn 2013

[18] Christian Czosseck, *State Actors and Their Proxies in Cyberspace*

aims closer. The aims vary amongst and within groups of hacktivists over time"[19]. What differentiates them from autonomous hackers is that they operate in informal groups often within loosely structured organizations, such as online platforms and forums[20]. Examples of such groups are the black-hat hacking group Lulzsec and Anonymous. Born inside 4Chan, an online forum, Anonymous acts cohesively in their ideologically-driven operations and follows a political agenda. These groups manage to amplify their political actions by enrolling both poorly and highly skilled 'followers' and by making a strategic use of social networks such as Twitter and Facebook. Another example of a Hacktivist group is WikiLeaks. WikiLeaks stands for the disclosure of confidential information to the public, and by doing so in 2010, with the release of 250,000 US embassy cables, has managed to compromise interstates relations, highly damaging the affected States' soft power. **Extremist groups** are organizations that have often existed independently from the Internet, but the category includes those born online as well. They refer to: international insurgents, jihadists and terrorist organizations, who use the Internet for purposes of recruitment, propaganda and communication[21].

Profit-driven criminals have as their primary goal financial gain and are generally regarded as the biggest threat to governments and businesses. Estimates account transnational cybercrime of damaging individuals globally for 388 billion USD annually[22]. Cyber criminals often target the financial services industry and the retail sector, and it has been proven that even individuals lacking technical skills can engage in cybercrime activities, if

[19] National Cyber Security Centre (NCSC), 2014. *Cyber Security Assessment Netherlands – CSBN 4*. In Cybersecurity in the European Union and Beyond: Exploring the Threats and Policy Responses, Study Commissioned by the Committee on Civil Liberties, Justice and Home Affairs (LIBE), European Parliament, 2015

[20] Czosseck 2013

[21] Ibidem

[22] Symantec, 2011

provided with the adequate tools[23]. They can act individually or can belong to an organization. Previously existing organized crime associations have been increasingly transferring their activities in cyberspace acquiring technical skills online. Digital platforms where information and expertise on cybercrime techniques are exchanged exist, and although some of them have been dismantled by law enforcement authorities, like the Darkode forum in 2015, they are still widespread all over the Internet and often in disguise[24].

Organizations and enterprises represent legal entities that engage in cyberspace as they rely heavily on ICTs for their business performance. Examples of such organizations are key players in the ICT industry, such as Microsoft, Cisco, and all the other relevant providers of IT security products. These private companies have been highly involved in the development of cybersecurity packages as they detain most of the global communication infrastructure, thus making them some of the most relevant stakeholders in the field of cybersecurity. Organizations and enterprises are at the same time targets of cyberattacks and developers of malware. By delivering IT security, these companies have been offering pen-testing services with the aim of discovering vulnerabilities in the operating systems and zero-day exploits, *de facto* employing the use of malware[25]. In doing so, this industry has developed a profitable legal market, as opposed to the illegal one created by the cybercrime network, that is essential for enterprises and governments in order to perform their ever increasing internet-based services.

Finally, **States** are involved in cyberspace on multiple levels. Firstly, States engage in cyber operations for law enforcement purposes, such as the fight against cybercrime and child pornography. Secondly, States have been adapting military activities to cyberspace, some of them even identifying the

[23] As it is the case with the DDOS attacks on Georgian governmental websites during the conflict with Russia in 2008. The topic is discussed in detail in Chapter Four.

[24] Joseph S. Nye, Jr., *Cyber Power*, Belfer Center for Science and International Affairs, 2010

[25] Czosseck 2013

cyber as the fifth domain of warfare, along with land, sea, air and space (US and Canada)[26]. Some events that anticipated the advent of "cyberwar", such as the cyberattacks on the Estonian government in 2007 and against Georgia in the war with Russia in 2008, have prompted States to develop military capabilities to operate in cyberspace. Clapper[27] identified in this regard:

- Nation States with highly sophisticated cyber programmes, such as Russia and China;
- Nation States with less sophisticated cyber programmes but potentially with more disruptive intent, such as Iran and North Korea.

In addition to this classification, a research conducted in 2013 by the United Nations Institute for Disarmament Research showed that 32 States have included cyber warfare in their military plans and structures[28]. The US, China and Russia appear to be the most developed in this field[29]. Thirdly, States have been transferring their intelligence services to the cyber domain, which provides governments with unprecedented advantages of anonymized access and global outreach for purposes of espionage and data gathering. More specifically, the dimension of digital espionage between States has increased dramatically, in terms of extension, numbers and influence[30]. Given the possibilities derived from cyberspace, nearly every intelligence agency has been investing in the development of espionage activities via the internet, making this ability no longer an exclusivity of powerful States. Espionage via digital means has a twofold direction: on one hand it is exercised for intelligence gathering from foreign countries' networks, on the other hand

[26] Lynn, William J. III., *Defending a New Domain: The Pentagon's Cyberstrategy*, Foreign Affairs, 2010

[27] Clapper, James R., *Worldwide Threat Assessment of the US Intelligence Community – Statement for the Record*. Found in 'Cybersecurity in the European Union and Beyond: Exploring the Threats and Policy Responses', European Parliament, 2015

[28] UNIDIR, 2013

[29] Klimburg, Alexander & Heli Tirmaa-Klaar, 2011

[30] NCSC, 2014

it is used for surveillance purposes aimed at national citizens. Although the aforementioned operations are rarely disclosed to the public, the revelations initiated by Edward Snowden in 2013 concerning the surveillance operations undertaken by the National Security Agency (NSA), shows how many resources States are willing to deploy in order to increase their soft power and strategic advantage through the cyber domain.

Threat Tools

This next session will display the technical tools used to conduct a cyberattack. Every cyberattack consists in intruding into an IT system without the user's authorisation in order "to extract or to modify data, to change the system configuration or to take down the entire system"[31]. There are multiple techniques that allow the intrusion into an IT system that can vary in expertise and complexity.

Malware stands as shorthand for 'malicious software' and refers to a variety of products that allow the intruders to gain access to a system. Malware is usually inserted into a system covertly or voluntarily by the users without their knowledge (through spam for example), and is aimed at "compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or of otherwise annoying or disrupting the victim"[32]. The proliferation of malware has been dangerously increasing in the past decade both in numbers and in complexity. The German Ministry of the Interior has stated that there were at least 1 million infections a month in Germany[33].

Developers of malware often mirror the technological advancement of legal commercial software companies, updating the malicious products with the

[31] Cybersecurity in the European Union and Beyond: Exploring the Threats and Policy Responses, European Parliament, 2015

[32] Ibidem

[33] Ibidem

introduction of variations that are difficult to be recognized by traditional anti-virus protection. The aim of the developers is to refine malware as to making it ever more hard to detect and to examine. Common forms of malware are: computer viruses, worms, ransomware, Trojans, Phishing, malvertisement.

A 'Botnet' is a special malware that works as a network of infected computers ('bots') that is remotely controlled via command-and-control servers maintained by the botnet's creator. Botnets can have impressive scales, with networks of millions of hijacked systems spread around multiple locations. Botnets are especially used for cybercriminal activities, including information theft and financial fraud. They are able to send massive quantities of spam, e-mails with malware attached and ransomware. Although the number of botnets has been decreasing due to law enforcement takedowns, their technical expertise has been oppositely increasing thanks to the use of peer-to-peer networks that allows the disguise of the perpetrators' identity[34].

According to Microsoft, "an Exploit takes advantage of weaknesses or 'vulnerabilities' in common software"[35]. It consists in a software or a series of commands that exploit an operating system's vulnerability, installing malware into the affected computer. Security professionals use exploits to test hardware vulnerabilities, in order to develop products to protect them. That is not the case with a 'zero-day exploit'. A zero-day exploit is the vulnerability of a software or a hardware that is exploited from an intruder that security developers had not recognized before. In that situation, a product able to fix the breach is not available yet. The Stuxnet worm that affected an Iranian nuclear facility in 2010 had these characteristics[36].

A Distributed Denial of Service (DDoS) attack is a type of malware aimed at preventing a computer's user from properly accessing online resources and

[34] Czosseck, 2013

[35] Microsoft, *The Exploit Malware Family*, Microsoft Malware Protection Center

[36] More on the Stuxnet worm will be discussed in Chapter Four.

services. This is commonly achieved through the use of botnets, sending huge amounts of web traffic to the victim so that the system is overwhelmed with information and is unable to operate. This type of cyberattack is usually used for blackmailing purposes by cybercriminals, but it is also used for achieving political goals by hacktivists. DDoS attacks have the potential to seriously affect societies. By overwhelming the servers of governmental websites for example, citizens can be faced with the unavailability of essential services like healthcare and financial transactions.

Threats in Cyberspace

Through the use of the techniques listed above, actors in cyberspace can carry out cyberattacks that result in real threats for individuals, States and organizations alike. Cyberattacks can have different outcomes depending on the target and on the motivation behind the attack.

Unauthorised access is the basis of a cyberattack, essential condition for carrying out any kind of action. This type of threat is especially affecting economic services that have been transferring their activities online, such as the retail and entertainment sector. E-commerce is also affected: through the use of Point of Sale malware (PoS), intruders can copy credit and debit card credentials from consumers through check-out systems used in retail[37]. Unauthorised access also paves the way for various forms of fraud, such as identity theft and banking account takeover. **Cyberespionage** represents a threat generating from unauthorised access as well, representing loss of control over sensitive information for States and of intellectual property for industries. Threats of **modification and destruction** can affect IT systems taking the form of "digital sabotage". The intent of the intruder might be that of erasing or editing certain data for political or strategic purposes, as well as

[37] Cybersecurity in the European Union and Beyond, 2015

for criminal ones. **Disclosure** affects users' privacy, and can be the result of extortion from cybercriminals. Many data breaches in recent times, such as the Ashley Madison[38] and the Sony Pictures Entertainment hack[39], show that these threats can be affiliated both with profit-driven criminals and hacktivists.

Disruption refers to the most dangerous actions undertaken via digital means that have the potential to cause physical damage. These include cyberattacks aimed at disrupting operating systems running energy, water and oil utilities, as well as military remotely controlled devices and networks. The most renowned event with these characteristics is the Stuxnet worm that was able to destruct an Iranian nuclear facility's centrifuges by infecting its operating system. The Stuxnet worm is often defined as the first cyber weapon[40].

Relevance of Threats

After having defined which are the actors operating in cyberspace, in relation to threat tools and outcomes, it is important to illustrate what consequences these threats entail for States and what actions are undertaken. Threats originating in the cyber domain can affect States directly and indirectly, and can have high or low relevance[41].

An **indirect threat** to the State is defined as any cyberattack directed against non-governmental actors located within national territory. Such threats underscore the State's economic performance, public safety and national security, even if the government's IT systems are not being attacked directly. Examples of such threats are represented by cyberattacks against the IT

[38] Brian Krebs, 'Online cheating site Ashley Madison hacked', KrebsonSecurity.com, July 2015

[39] Sanger, David E., Perlroth, Nicole, 'U.S. Links North Korea to Sony Hacking'. The New York Times, December 2014

[40] Joshua Alvarez, 'Stuxnet: the World's First Cyber Weapon', Center for International Security and Cooperation (CISAC), February 2015

[41] Jan-Frederik Kremer and Benedikt Müller, *SAM: A Framework to Understand Emerging Challenges to States in an Interconnected World*. In Cyberspace and International Relations: Theory, Prospects and Challenges, Springer 2011

infrastructure of private companies as well as power supplies, limited industrial espionage and stealing of corporate data, disruption of privately-owned communication networks. In this situation, the State's authority and space for action is present but limited. In fact, as mentioned before, most of the digital infrastructure is privately owned, so that law enforcement authorities can investigate and react only with the support of private IT security companies. These threats are categorized as 'indirect', but they still pose a certain risk to the State and are then considered of high relevance. Cases of indirect threats of low relevance for the State include attacks aimed against individuals, including credit card fraud, personal data breach and account hacks. Although these threats can be worrisome for private citizens, as they undermine fundamental rights like the right to privacy and freedom of speech, the State has no authority over the degree of protection of privately owned electronic devices.

Direct threats via digital means targeting the State instead have all high relevance. They can be defined as any cyberattack directed against the national institutions' IT systems. These include: attacks against the government's IT systems, disruption of military networks and stealing of sensitive or confidential information, systematic espionage of the State's strategic assets. Depending on the political nature of a State, manipulation of information and intromissions into governmental communications channels can be perceived as a high relevance threat as well. That is the case for totalitarian regimes and autocracies for example. In face of a direct threat, the State affected has every competence in persecuting the authors and to enforce countermeasures. Events of this relevance however have to be dealt with once again in coordination with the private sector, defining common responsibilities among representatives in order to properly respond to the threat.

Emerging Threats

Having assessed the current threat landscape, it can be interesting to illustrate the potential innovative threats that can arise from advancements in technology.

According to experts, cyberattacks against the Internet of Things could pose serious risks in the future[42]. The Internet of Things (IoT) is "the network of physical objects – devices, vehicles, buildings and other items – embedded with electronics, software, sensors and network connectivity that enable these objects to collect and exchange data"[43]. The risk for cyberattacks lies in the number of devices connected and in the amount of data exchanged enabled by this technology. Such data needs proper protection, and although the IoT is already employed, so far attacks against such technology have been limited. The reason for that might be the absence of lucrative ends for cybercriminals[44], but the situation is likely to change in the years to come.

Another emerging threat might be one affecting mobile devices. Up until now, mobile devices have not been the preferred targets for data breaches: Verizon accounts the amount of mobile devices affected by malware as being "an average of 0.03 per cent of smartphones per week – out of tens of millions of mobile devices on the Verizon network – infected with 'higher grade' malicious code"[45]. Europol however estimates that potential risks might derive from the installation of mobile banking applications with malicious code that could steal and replicate the user's credentials[46].

[42] John Pescatore, *2014 Trends That Will Reshape Organizational Security*, sans.org, 2014. Found in 'Cybersecurity in the European Union and Beyond', European Parliament, 2015

[43] International Telecommunications Union website (ww.itu.int), 'Internet of Things Global Standards Initiative', 2012

[44] James Lyne, *Security Threat Trends 2015*, Sophos.com, 2015. In 'Cybersecurity in the European Union and Beyond' 2015

[45] Verizon, *2015 Data Breach Investigations Report*, 2015. In 'Cybersecurity in the European Union and Beyond' 2015

[46] Europol, 'Payment Fraud' Report, 2015

Appendix: Threat Inflation and Securitization of Cyberspace

As it was previously mentioned, the threat landscape in cyberspace can vary in relevance and impact depending on the stakeholder's subjective perception. Some of the threats can be amplified and 'securitized' for strategic purposes through media coverage and political rhetoric. Professionals in the field like Eric Jardine confirm this trend. He states in particular:

"*Since cyberspace is, in a number of ways, expanding at an exponential rate, it is reasonable to expect that the absolute number of cyberattacks will also increase simply because the Internet ecosystem is getting bigger and not necessarily because the situation is getting worse*"[47].

In this perspective, the urgency of security measures in response to threats in cyberspace are inflated, because there exists a tendency on focusing on absolute numbers instead of normalizing such numbers taking into account other indicators such as the number of Internet users, web domains and web traffic volume. Once this is done, the cybersecurity landscape can be seen as improving rather than worsening. The reason behind this type of discourse on cybersecurity has political and economic explanations. On one hand, media coverage inflating cyber incidents and political rhetoric amplifying threats in the cyber domain manages to create commotion in the public so to justify action from policy makers. On the other hand, the business surrounding cybersecurity has become increasingly lucrative for IT security private companies, that can count on the sustained demand from enterprises and governments for the protection of their IT systems as a result of threat inflation.

[47] Eric Jardine, *Global Cyberspace Is Safer Than You Think: Real Trends in Cybercrime*, Global Commission on Internet Governance, Cigionline.org, 2015. Found in 'Cybersecurity in the European Union and Beyond' 2015

Threat inflation can be also explained in the light of the concept of the securitization process. Securitization of cyberspace refers to the ever increasing transformation of the domain into a matter of national security and can be witnessed with particular strength in the United States. The securitization process is a concept of international relations connected to the Copenhagen School of Thought on Security Studies[48]. This topic will be mentioned later in this thesis, but it is important to point it out in the context of this discussion as it affects the issue of cybersecurity as a whole. In this scenario, once shaped through the securitization process, the discourse on cybersecurity acquires a special relevance for national security thanks to media coverage and political rhetoric, which enables policy makers to adopt extraordinary means to use in the name of security, altering the real perception of the threat[49].

Conclusions

This chapter provided with a categorization of actors operating in cyberspace, of threats generating from its malicious use and of the tools utilized for that scope. As mentioned in the introduction, a shared concept of what a threat constitutes does not exist: threat perception rests solely upon the subjective perspective of the actor affected, and this manages to amplify the dimension of the risks related to cyberspace. What appears clear at this point is the potential that threats originating from cyberspace have to alter the normal conduct of the social, economic and political activities of networked societies. Moreover, sophisticated malware can be used for offensive purposes against governments or State-owned strategic assets, generating political implications that can potentially escalate into conflicts. For this reason, the following

[48] Alan Collins, *Contemporary Security Studies*, Oxford University Press, 3d ed., 2013

[49] Hanna Samir Kassab, *In Search of Cyber Stability: International Relations, Mutually Assured Destruction and the Age of Cyber Warfare*. In Cyberspace and International Relations: Theory, Prospects and Challenges, Springer 2011

chapters will display how threats stemmed from malicious uses of ICTs can affect international security and how historical concepts of international relations are transformed when applied to the cyber context. The framework of actors, threat tools and actions proposed in this section, although operated from a non-technical point of view, will result useful for the topics discussed hereafter.

Chapter Two

Sovereignty and Cyberspace

Preface

After the Cold War era and with the spread of the process of globalization, scholars and political thinkers have tended to declare the end of the sovereign State as we know it, said to be eroded by the global flux of information, people and capitals and by the relative loss of relevance of territorial borders and of the dimension of nation-States[50]. While some of these stances are true in part, the Sovereign State - standing as the only and rightful component of the international system - is far from decline and has still some power to exercise its authority over the borderless cyberspace. Nonetheless, cyberspace is regarded as a global space that reaches beyond traditional sovereignty, making the challenges for the application of sovereign power in that environment urgent and evident. Territorial sovereignty is considered in international jurisprudence as the fundamental feature of a State, which implies that a State is able to exercise its exclusive authority over a given portion of the globe[51]. The concept of integrity can be analysed on its own, as it refers to the obligation for States to refrain from interfering with the internal affairs of other States. This chapter will intend sovereignty as categorized by Stephen Krasner, adopting three of the four layers identified in his analysis of sovereignty applied to cyberspace: Westphalian sovereignty, domestic

[50] Jean-Marie Guéhenno, *The End of the Nation-State*, 1995; Saskia Sassen, *Losing Control? Sovereignty in an Age of Globalization*, 1996. Found in David J. Betz and Tim Stevens, *Cyberspace and the State: Toward a Strategy for Cyber-Power*, The International Institute for Strategic Studies, 2011

[51] Benedikt Pirker, *Territorial Sovereignty and Integrity and the Challenges of Cyberspace*, in Katharina Ziolkowski (ed.), Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy, NATO CCD COE Publication, Tallinn 2013

sovereignty and interdependence sovereignty. The fourth dimension, international legal sovereignty, will be kept out and briefly examined in the conclusion[52].

Westphalian, Domestic and Interdependence Sovereignty applied to Cyberspace

Westphalian sovereignty refers to the traditional assertion of the concept, meaning that a State's authority is the only legitimate source of power within a specific territory. Intervention in the internal affairs and changes in the political and physical structure of another State through the use of force thus constitute violations to this principle[53]. In the context of cyberspace, the most evident violations are represented by Computer Network Operations (CNOs)[54] and by cyber espionage, in the situation where such actions are undertaken by sources generating from a foreign country. The cyberattacks faced by the Estonian government in 2007 are said to have had these characteristics[55]. In April 2007, Estonian authorities agreed on the removal of the Bronze Soldier of Tallinn, a war memorial from World War Two representing a Soviet soldier, and of other war graves from the same period to be relocated on the

[52] Stephen D. Krasner, *Power, The State and Sovereignty: Essays on International Relations*, 2009. Found in Betz and Stevens, 2011

[53] Pirker 2013

[54] Computer Network Operations (CNOs) are described by the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) in its online portal for Cyber Definitions mentioning the definition operated by the US Department of Commerce. CNOs are defined as "comprised of computer network attack, computer network defense, and related computer network exploitation enabling operations". Similar and more used concepts are: Computer Network Exploitation (CNE) and Computer Network Attack. The latter is defined by NATO as an "action taken to disrupt, deny, degrade or destroy information resident in a computer and/or computer network, or the computer and/or computer network itself".

[55] Ian Traynor, 'Russia accused of unleashing cyberwar to disable Estonia', The Guardian, online article, May 2007

outskirts of the country's capital. Soon after this event, amid a dispute with Russia on the matter, a three-week series of cyberattacks targeted websites of Estonian organizations, of the national parliament, banks, ministries and newspapers. Most of the attacks were distributed denial of service type of attacks (see part one); spam distribution through armies of botnets and defacement of websites were also employed[56]. Although there exists still much speculation over who is responsible for these attacks, it is widely recognized that Russia was involved, allegedly enrolling and directing patriotic hackers for the prosecution of such actions[57]. The cyberattacks against Estonia, along with those faced by Georgia in 2008, are generally regarded as (if the allegations are correct) the first manifestation of a cyber conflict between two Nation-States.

In the Estonian case, Westphalian sovereignty is violated via cyber means, but the consequences according to international law are limited. In fact, the potentiality of such breaches to happen continuously is *de facto* legitimised by the presence of 'active defence systems' installed in most sensitive national networks[58]. In this sense, Computer Network Operations and intrusions into governmental IT systems would be 'institutionalised' as non-discriminatory activities, consequence of the implementation of active defence systems that are both tasked with the detection of unauthorised accesses and with the ability to respond with offensive counteractions, eliminating the threat at the source but normalising CNOs and unauthorised intrusions into foreign IT systems at the same time[59]. These types of breaches would formally constitute violations of Westphalian sovereignty, but just as much as espionage conducted in the physical world (which will be discussed later on) they would

[56] Betz and Stevens 2011

[57] Joseph S. Nye Jr., *Cyber Power*, Belfer Center for Science and International Affairs, 2010

[58] Salma Shaheen, Offense-Defense Balance in Cyber Warfare, in Kremer and Muller, Cyberspace and International Relations: Theory, Prospects and Challenges, 2011

[59] Pirker 2013

fall into an international law grey area, which means that they would not be considered either legal or illegal, but rather accepted as an unregulated and acknowledged international custom and a result of extensive State practice.

Domestic sovereignty refers to the ways in which the exercise of the State's exclusive authority within national borders is conducted[60]. Being cyberspace an unregulated global space, States have been struggling with the identification of spaces of action for the execution of authoritative rule. Indicative of this situation is the increasing number of States that have set up special forces tasked with the surveillance of national web traffic or that have implemented legislation directed at the regulation of the cyber domain. In addition to these provisions, most States have adopted national cybersecurity strategies that aim at targeting mostly internal phenomena such as digital sabotage and criminal activities[61]. A valid example that testifies this trend is the scale of the control exercised by States on information acquired online by national citizens in relation to terrorist propaganda for purposes of recruitment and radicalization, which is perceived as especially threatening in Western democracies[62]. Filtering techniques that preclude national users from accessing specific contents and services online are the preferred tools used in this regard, which are often supported by physical surveillance provided by law enforcement authorities. Such techniques can have different effects depending on the motive behind the preclusion of internet services: while in Western democracies the intent is to impede individuals to affiliate themselves with terrorist organizations and ideologies, that type of control can be used by authoritarian regimes to suffocate expression of political dissent. Information and Communication Technologies (especially social networks) as platforms for political dissent and uprisings have indeed gained importance in

[60] Betz and Stevens 2011

[61] *Cyber Defence in the EU: Preparing for Cyber Warfare?*, European Parliamentary Research Service, briefing by Carmen-Cristina Cirlig, European Parliament, October 2014

[62] Betz and Stevens 2011

international politics in recent times, as it is the case with the Arab Awakenings of 2010-2011, as well as with the Turkish and Iranian political contestations of the past few years. The importance of these instruments is testified by the scale of resources deployed by the affected governments in order to respond to these forms of revolts. At the same time, those very technologies can be used by authoritarian regimes to distort and to manipulate inflow of news from the world, denying their citizens of non-discriminatory access to information and exposing them to propaganda communication[63]. In the light of these trends, it can be noted how the flow of information channelled through cyberspace can compromise domestic sovereignty in terms of affecting the State as the exclusive regulator of internal affairs.

Interdependence sovereignty intends sovereignty as the State's ability to manage the external influences that can affect domestic power, such as the flows "of goods, persons, pollutants, diseases, and ideas across territorial boundaries" which have been enormously amplified in scale and impact by the globalizing process[64]. In the globalized era States struggle to ensure control over these flows and more so in cyberspace, which thrives on the unregulated and borderless free flow of information. As much as with issues affecting domestic sovereignty, interdependence sovereignty is thus concerned with the unceasing flow of information and content transmitted through the internet, which in certain cases can result undesirable for national interests: that is the case with terrorist material shared online. States attempt to filter such content by filtering web traffic and through specific agreements with service providers and web companies, but the very nature of cyberspace renders these actions limited. An example of this trend is represented by the numerous attempts by States to pressure Google to prevent national users from viewing specific videos containing terrorist messages posted on the

[63] Betz and Stevens 2011

[64] Krasner, *Power, The State and Sovereignty: Essays on International Relations*, 2009

video-sharing site YouTube by geo-blocking the content based on the source of the IP address[65]. Despite this however, that same content can be easily copied and transferred to another website or can be replicated in other platforms. These attempts have thus partially failed to strengthen interdependence sovereignty, and have instead increased the governments' reliance on web companies for the censorship of undesired material. This situation poses another paradox: while cyberspace is widely regarded by policy makers as the drive for economic growth and as the platform for the spread of democratic ideals and principles, it is also perceived at the same time as an environment where undesirable content can be shared and divulged freely, endangering national security. The paradox also lies in the political direction that needs to be assigned to cyberspace: if the concerns over national security were to be preferred, cyberspace would be regulated domestically as to reflect the normative standards comprised within territorial borders, seriously limiting freedom of expression and of exchange of information which are principles cherished and promoted globally by Western democracies. Following this perspective, cyberspace would assume the characteristics of the one ensured in China, which means a digital environment that is strictly regulated by authorities through the surveillance and censorship programme known as the 'Great Firewall of China'[66]. With the configuration of advanced technologies incorporated into national network gateways aimed at filtering contents according to their origin, the Chinese government manages to preserve its exercise of domestic sovereignty, excluding from the political discourse within civil society those ideas considered threatening for national security. Cyberspace is therefore utilised strategically by the Chinese as an environment where to enhance political influence and for economic advantages with the assurance of the absence of undesired external

[65] Betz and Stevens 2011

[66] Nye Jr. 2010

influences[67].

The conflict between control both over the advantages and the threats deriving from the digital domain is perhaps the most challenging and defining feature of the current discourse over cyberspace policy, which will be discussed further in the thesis[68].

The international legal sovereignty of States, as it is conceived according to the fourth dimension of sovereignty described by Krasner (that was not considered in this analysis) refers to States as the prominent political subjects of the international community that recognize each other as equal in international law[69]; in this sense, cyberspace does not pose a threat to this kind of sovereignty as long as it is guaranteed by international law. However, as seen with the analysis of sovereignty in the context of the three categories taken into examination, States are urged as to how to adapt to a shifting international system where the role of cyberspace is gaining more and more prominence in the global economy and in international affairs. Since a State can only exist in the presence of sovereignty, the relevance of the concept in cyberspace will depend both on the type of approach chosen by governments towards the regulation of the digital environment and on the adaptability of the international system as a whole.

Territorial Sovereignty and Integrity in cyberspace according to international law

As mentioned in the previous section, sovereignty is intended as the State's right to exercise its exclusive authority within a specific territory. Although the two principles are inherently correlated, the concept of integrity can be defined separately from the notion of sovereignty, and is generally intended as

[67] Betz and Stevens 2011

[68] The chapter on Cyber Diplomacy displays in detail the issues and developments concerning the debate over internet governance.

[69] Krasner 2009

the duty to not interfere with the territorial integrity of other States and, equally, as the State's right to be free from interference[70]. This section displays how the rules of international law concerning violations of sovereignty can be adapted in the cyber domain, addressing in particular the abstract characteristics of the digital environment where the complexity in attributing the source of Computer Network Operations can result in an increase in inter-State tensions and potential escalations involving retaliation through armed force. The *Tallinn Manual on the International Law Applicable to Cyber Warfare* represents the best theoretical support on the applicability of international law concerning territorial sovereignty and integrity[71], but while some of the prescriptions illustrated in the manual are considered entirely applicable to cyberspace, a more structured legal framework will only be available once new State practice and case law are established.

Lower-Level Violations of Territorial Sovereignty and Integrity in Cyberspace according to International Law

Territorial sovereignty and integrity are violated under international law in two cases: firstly, interventions involving the use of force as prescribed in Article 2(4) of the Charter of the United Nations[72]; secondly, territorial integrity of a State can be violated through coercion, which can amount to a violation under international law if it involves enough intensity as to concretely compromise the affected State's political, social and territorial configuration. The notion of coercion is deducted from Article 2(1) of the Charter of the United Nations which declares the principle of the sovereign equality of States. The peculiar characteristic of cyberspace renders the application of these principles somewhat complicated, as States practice is not

[70] Pirker 2013

[71] NATO Cooperative Cyber Defence Centre of Excellence, *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge University Press, 2013

[72] UN Charter, 1945

fully established yet and as a consequence of the secrecy that surrounds actions undertaken in this domain; but mostly what remains unclear at a legal level regards what level of intensity must a cyberattack reach in order to be identified as an ‘armed attack’ and thus treated accordingly as illustrated in Article 51 of the UN Charter. This particular issue, although representing a violation of territorial sovereignty and integrity under international law, will be kept aside in the analysis of this chapter as it will be taken up and will be discussed more thoroughly in the chapter on cyber war.

The focus is then put on the notion of **coercion**, which can be used to describe the predominant lower-level violations of sovereignty in cyberspace. As mentioned previously, coercion does not represent interference with territorial sovereignty and integrity as long as it is of a political and economic kind; only coercion that possesses enough intensity as to have serious effects on the fundamental characteristics of a State is considered a violation under international law. Keeping this in mind, the lower-level violations of sovereignty so widespread in cyberspace do not constitute formal transgressions against principles of international law but nonetheless affect the integrity of a State and its sovereign power. The tool utilised in the examination of cyber activities that can qualify as violations of sovereignty is thus the ‘coercive’ effect that these have on the targeted State[73].

As a first example, a State could take advantage of the availability of information in cyberspace to exercise **political influence** onto another one. That can be achieved through hosting blogs for foreign activists and journalists critical of their governments, as well as through communication campaigns targeting another State where a regime change is desired. In this case, the level of political influence would not be as intense as to reach the level of coercion; as demonstrated in the case law of the International Court of Justice in the

[73] Pirker 2013

Nicaragua case, coercion is reached only if it is demonstrated that an evident financial and logistic support to subversive groups was provided. In that case, a violation of territorial sovereignty is identified[74].

Cyber espionage, as it was demonstrated previously, theoretically constitutes a violation of territorial sovereignty through the intrusion into foreign IT systems[75].

But since espionage is not regulated at international level, the same applies to cyber espionage, which is universally regarded as a consolidated and acknowledged practice among States. Equally, **economic espionage** does not implicate that a violation of international law has taken place, despite the frictions that the alleged economic espionage conducted by the Chinese against the US has created in the countries' relations in recent times[76].

Cybercrime can also affect a State's territorial sovereignty and integrity but is generally tackled through national law enforcement, as opposed to having it treated as a breach of international law. **Cyberterrorism** and **digital sabotage** are dealt with in the same manner, although terrorist activities conducted via cyber means and actions of digital sabotage that are aimed at the disruption of critical infrastructure (as it is the case with the attacks against a water supply system in Haifa in 2013[77] and against an Ukrainian power grid in late 2015[78]) could be considered as acts violating territorial sovereignty and integrity[79].

As seen with these cases, **coercion** as the element identified with lower-level violations of territorial sovereignty and integrity in cyberspace depends on the

[74] *Case Concerning Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States)*, ICJ Reports 1986

[75] Tallinn Manual on the International Law Applicable to Cyber Warfare, *Sovereignty*

[76] The US-Chinese controversial debate on cyber issues is discussed thoroughly in Chapter Five.

[77] 'Haifa Tunnel Paralyzed by Cyberattack, Expert Reveals', haaretz.com, October 2013

[78] Alex Hern, 'Ukrainian blackout caused by hackers that attacked media company, researchers say', The Guardian, January 2016

[79] Tallinn Manual, *Sovereignty*

intensity of the coercion exercised, which must result in fundamental changes in a State's political and physical structure as a consequence of the interference generated from another State.

Cyber espionage as a violation of Territorial Sovereignty and as a threat to National Security

Espionage is an activity conducted since the dawn of mankind: the gathering of information has always been regarded as the strategic edge against political opponents and military adversaries. In the present age, the interconnectedness brought about by the spread of the use of the internet has dramatically increased the possibilities of espionage activities, thanks to the borderless dimension of the cyberspace, to source concealment and to infiltration potential. Intelligence agencies all over the world have invested in transferring their activities into the cyber domain: espionage conducted in cyberspace reduces risks, protects intelligence personnel, and most of all increases the amount of information collected at an almost instantaneous speed. The effectiveness of espionage conducted via cyber means is unprecedented in scale and influence, and economically-motivated espionage is especially employed[80]. As in the post-Cold War international system economic competitiveness and performance lies as the foundation of a State's power, economic espionage has turned out to play a strategic role for developing/industrialized countries to compensate their technologic inferiority by targeting industrial and intellectual property of developed/post-industrialized countries that are more vulnerable to this kind of threat and more proactive in counteracting this phenomenon.

[80] Katharina Ziolkowski, Peacetime Cyber Espionage – New Tendencies in Public International Law, in in Katharina Ziolkowski (ed.), Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy, NATO CCD COE Publication, Tallinn 2013

Economic espionage is at the top of the political agenda in the relationship between the US and China. During their latest meeting in September 2015, cyberattacks targeting intellectual property and strategic assets were the main concern on the American side. While Xi Jenping was quick to deny any involvement, he stated that the Chinese face the same problem internally and that the issue of cybersecurity should be tackled jointly with the American partner and with the international community as well[81].

Despite reassurances on the Chinese side, a new political discourse has risen in the US which links cyberattacks aimed at gathering industrial and technological information as threatening its national security, leading officials and scholars to consider foreign unauthorised intrusions into national computer networks as a violation of the territorial sovereignty of the State as well as armed attacks, or even as comparable to 'military occupation'[82]. This threat is considerably perceived as originating from China: some notable cyberattacks in recent times have proved that Chinese hackers are particularly active in the field of cyber espionage, although clear identification of the attacks is hardly reachable, due to the aforementioned issue of attribution.

The cyber incidents occurred between 2003 and 2007 called '*Titan Rain'*, were allegedly conducted by State-sponsored Chinese hackers that managed to infiltrate computer networks of the United States Department as well as of defence contractors in order to acquire confidential and strategic information regarding aviation and flight-planning software from the Redstone Arsenal of the US Army and Missile Command[83]; in 2009, the '*GhostNet*' operation was found to be consisting in unauthorised accesses into computer networks of

[81] Dan Roberts, 'Obama warns of 'weaponising the internet' ahead of Xi Jinping's US visit', The Guardian, September 2015

[82] Melnitzky in particular has stated "Chinese cyber espionage against the United States has reached such a massive scale that it more closely resembles an act of looting, which before the Internet could have only occurred coupled with military occupation, rather than series of criminal acts".

[83] Bradley Graham, 'Hackers Attack Via Chinese Web Sites', The Washington Post, 25 August 2008

embassies, foreign ministries, and other governments offices in more than 103 countries, including the Dalai Lama's Tibetan exile centres in India, London and New York[84]. Again, the political aim of the operation and the entity of the targets induced many to judge the Chinese were behind the attacks, even though only circumstantial evidence has since been collected. The one event that changed the US-Chinese debate over cyberattacks was the Google hack in 2010[85]. In January 2010, Google announced that hackers in China had infiltrated into the company's IT systems to gain access into Gmail accounts of human rights activists in China and in other parts of the world (Europe and North America), in addition to targeting and stealing intellectual property of US hi-tech and chemical companies, such as Yahoo, Adobe and Symantec. The operation, called '*Operation Aurora*' by security companies, is considered the incident that considerably shifted the US' perception of economic espionage via cyber means as threatening national security and its attitude towards China in the matter[86]. In the aftermath of the revelations, a few reports were published by the Obama administration that reflect the new approach on cyberattacks: the first to be divulged, the *Joint Strategic Plan on Intellectual Property Enforcement* of June 2010, is the first official statement where economic espionage is directly connected to national security. In May 2011, the *International Strategy for Cyberspace – Prosperity, Security and Openness in a Networked World* clearly states that the United States are willing to retaliate against cyberattacks through every mean they retained necessary and appropriate. As illustrated in the Strategy: "the US will take measures to identify and respond to such actions to help build an international

[84] The SecDev Group, *Tracking GhostNet: Investigating a Cyber Espionage Network*, Infowar Monitor Report, 29 March 2009

[85] Oliver Read, How the 2010 Attack on Google Changed the US Government's Threat Perception of Economic Cyber Espionage, in Kremer and Muller (ed.), Cyberspace and International Relations: Theory, Prospects and Challenges, Springer 2011

[86] Read 2011

environment that recognizes such acts as unlawful and impermissible, and hold such actors accountable"[87].

In the light of this situation, the shift in the approach towards cyberattacks in the US perspective is considerable. The political discourse around cybersecurity is now extremely militarized in actions and ideals[88]; the institution of the Cyber Command within the US armed forces (USCYBERCOM) and of similar institutions in the militaries of other countries could be the representation of a more offensive cyberspace, where unauthorised intrusions into national computer networks targeting information regarded as vital to national interests can be deemed as 'armed attacks' or as violating territorial sovereignty, justifying the resort to retaliation in self-defence.

Such stances do not reflect the prescriptions of international law and could only be established as shared rules once confirmed by States practice, which is still absent. Inter-State cyber espionage, meaning conducting unauthorised access into foreign IT systems, can constitute a violation of one's territorial sovereignty and integrity only if it results in causing a *physical* effect in said State. The effects-based interpretation of cyberattacks is the one to be preferred.

Under present international law, it is questionable whether a 'virtual trespass' into national computer networks would be comparable to physical entry into a foreign territory by a State agent, organ or representative[89]. A US Department of Defence legal memo from 1999 describes the situation: "An unauthorized electronic intrusion into another nation's computer system may very well end up being regarded as a violation of the victim's sovereignty. It may even be regarded as equivalent to a physical trespass into a nation's

[87] International Strategy for Cyberspace – Prosperity, Security and Openness in a Networked World, White House, 2011

[88] Read 2011

[89] Ziolkowski 2013

territory, but such issues have yet to be addressed in the international community”[90].

According to current international law, the effectiveness of the violation of territorial sovereignty and integrity relies on an *effects-based* approach, which means that the violation must result in physical damage caused in the other State’s territory or otherwise in medium or long-term serious consequences to the State’s critical infrastructure, otherwise the intrusion does not constitute a violation. In the case of cyber espionage, the physical absence of the infiltrator renders intrusions into IT systems for the purposes of intelligence/economic data gathering a lower-level violation of territorial sovereignty.

Given the secrecy of espionage activities, it is unrealistic that intelligence agencies would expose their actions by causing physical damage while conducting a covert operation via cyber means.

The current debate on cybersecurity at global level and the harsh dispute between the US, China and Russia over cyberattacks and the perception of cyber issues as affecting national security concerns has the potential to turn the cyber domain into a more aggressive and conflictual environment; in that situation, cyberattacks would have more disruptive features and violations would become more explicit. If this were to happen, new State practice and case law will be developed, which would recognize lower-level violations as proper violations of sovereignty; until then, State practice and case law is to be developed, and the technical issue of attribution is to be overcome.

[90] US Department of Defense, Office of General Counsel. Found in Ziolkowski, *Peacetime Espionage*

Appendix: Territorial status of Cyberspace

Cyberspace is a metaphorical dimension that comprises both abstract and physical features. The abstract ones refer to the data transmitted through the informational channels provided by cyberspace and to the interconnectedness generated by global networks; more broadly, they refer to the flow of information and content favoured by the spread of the internet. Conversely, the internet relies on technical physical infrastructure composed of hardware and software, as well as optic cables and servers[91]. Despite existing as the sole man-made domain, interactions happening in cyberspace have acquired strategic importance for States, and recent regulatory developments have declared that the territoriality vocabulary of international law applies in principle[92]. Consequently, it has been argued that cyberspace shall be granted a special status, drawing analogies with the way other domains are treated under international law (like outer space or the high seas), and in particular with the 'global commons' regime[93]. But the peculiarities of the cyber domain make the application of such an approach difficult. The identification of cyberspace as a 'global common' would not be feasible as a global commons regime implies the implementation of shared rules, which issues of identification and attribution in cyberspace would compromise. Secondly, the technical infrastructure underlying cyberspace is mostly privately-owned, and the application of the global commons regime would entail the expropriation of property rights belonging to companies. Further, considering the limitless dimension of cyberspace, sanctions condemning inappropriate behaviour would be hard to implement given the difficulties in identifying users. Thus, theoretically, cyberspace remains a domain where global interaction is subject

[91] Betz and Stevens 2011

[92] Benedikt Pirker, *Territorial Sovereignty and Integrity and the Challenges of Cyberspace*

[93] Katharina Ziolkowski, General Principles of International Law as Applicable to Cyberspace, in Katharina Ziolkowski (ed.), Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy, NATO CCD COE Publication, Tallinn 2013

to the existing norms of international law[94]. Given the specificities of the cyber domain, and mainly its borderless feature, cyberspace cannot be appropriated by one State. Under current international law, no special status is granted to cyberspace and States tend to regulate it in accordance with their national jurisdiction. This creates asymmetries in access to the internet and in the fruition of civil liberties online: increasingly, States tend to emphasize their role on the internet in order to regain sovereign control over the flow of information channelled through the informational substrate, and this impacts negatively with human rights.

[94] Pirker 2013

Chapter Three

Power and Cyberspace

Preface

Power is a debated concept: its meaning differs considerably according to the context in which it is applied. Commonly, power is assumed as the ability of an individual to exploit certain resources in order to achieve a desired goal. Crucial to this observation is the social component of power: it can only be created in the context of a social interaction, in the absence of which power does not show. This last stance leads us to affirm that power arises from a social relationship within a determined context: definitions of power always depend on context, and cyberspace is an emerging context where power is expressed[95].

The interdependence and interconnectedness of persons, devices and services brought about by the internet affects the dimension of power in cyberspace. Even though States remain the actors with the most resources deployable in this domain, as with regards to other features of traditional statehood they struggle to detain control over the cross-border flow of information channelled through the digital architecture of cyberspace. In addition to that, States find themselves competing for influence with a wide range of actors, who exploit the strategic advantages found online for the pursuit of their own interests.

Non-State actors have gained considerable power in the cyber domain, thanks to low and affordable barriers for entry, identity concealment and availability of technical means to conduct malicious operations[96]. These entities, ranging

[95] Joseph S. Nye, Jr., *Cyber Power*, Belfer Center for Science and International Affairs, 2010

[96] Ibid.

from a teenage hacker to a transnational enterprise, have the potential to cause considerable damage and to afflict changes to the status quo: the impact that actions undertaken by loosely structured groups such as Anonymous and WikiLeaks have had on the States' political reputation confirms this trend.

As a consequence, governments are growingly concerned with the multiplication of actors in cyberspace and of the differential of power that is narrowing between them; not only with regards to non-State actors, but also to developing nation-States such as North Korea, Iran and Brazil who have invested in technology to acquire influence in the cyber domain, this way compensating the gap in conventional resources with the most powerful States and obtaining advantages in the diffusion of soft power.

For these reasons, the prioritization of cybersecurity in the current international affairs comes as a result of the diffusion of power characterizing the global politics of the 21st century.

Cyber Power

Cyber power is not to be intended as a new form of power, but rather as the manifestation of power in the digital environment, where physical presence and identities are shifting[97]. Cyber power can be defined as "the ability to use cyberspace to create advantages and [to] influence events in other operational environments across the instruments of power"[98]. Cyberspace represents the most prominent emerging context for the application and the diffusion of power. States compete in this environment with other actors who are equally able to exercise hard and soft forms of power[99]: the flow of information and

[97] David J. Betz and Tim Stevens, *Cyberspace and the State: Toward a Strategy for Cyber-Power*, The International Institute for Strategic Studies (IISS), 2011

[98] Daniel T. Kuehl, *From Cyberspace to Cyberpower: Defining the Problem*, in Franklin D. Kramer, Stuart Starr and Larry K. Wentz, *Cyberpower and National Security*, 2009

[99] J.S. Nye, *Soft Power: The Means to Success in World Politics*, 2004. In 1990, Nye operated a distinction between hard and soft power. Hard power behaviour relies on coercion, whereas soft power behaviour relies on persuasion and on the formulation of agendas.

the instruments channelled through cyberspace that cannot be exclusively and fully controlled by States are used as a power resource that is deployed both for offensive and for defensive purposes. This is particularly threatening for post-industrialized countries that heavily rely on information and communication technologies for the functioning of essential assets in the military and economic field; forms of hard and soft power have the potential to cause disruptive effects on societies and to alter power differentials among States and non-State actors.

Cyber Hard Power

Power can assume its coercive dimension in cyberspace when the intention behind the action is to modify or to interrupt the behaviour of another actor through digital means and can occur both between States and non-State actors as well as between non-State actors[100]. Coercive power can be achieved through the unauthorised access or through the installation of malicious software into a computer network: by doing this, the intruder is able to utilize the device according to its will and to carry out any kind of action. In addition to that, the attacker can also preclude the original user from accessing content and services online and can force him to interrupt or to modify his course of action.

An example of this is represented by the hack conducted by Anonymous against the hi-tech security company HBGary Federal. After the CEO of the company had announced that the company had been able to infiltrate the Anonymous network and that the company was willing to expose the identities of the members of the organization, Anonymous retaliated attacking the

[100] Betz and Stevens 2011

company's servers, defacing its websites and sending messages to the CEO himself and other staff members threatening to publish the private e-mails and corporate data obtained with the hacking. In the end, the company had to surrender and had to come to terms with Anonymous for the corporate data not to be disclosed[101]. Remote control over privately owned or over governmental networks affects the conduction of an actor's actual behaviour online, excluding the range of actions available that enable an actor to have power over its own will. The HBGary Federal hack represents a highly successful cyberattack consisting of a non-State actor exercising cyber coercive power towards another one.

Informational resources can be used by States and non-State actors to deploy acts of hard power in cyberspace, for example by conducting Distributed Denial of Service attacks (DDOS) through the use of botnets and by defacing websites, as well as by introducing malicious software into IT systems or even by acquiring sensitive/confidential data through unauthorised access. The most disruptive tool available to actors online however is represented by cyberattacks against SCADA systems (Supervisory Control and Data Acquisition systems). The introduction of malware into the operating systems of these machines can have indeed a potentially disruptive effect on the critical infrastructure located within a State's territory, interrupting the distribution of essential services for societies like energy and water supplies. These type of actions have immediate physical effects and can be used as coercive tools for inducing another actor to comply with a desired outcome.

Another act of hard power is represented by the destruction of the physical infrastructure upon which the informational substrate relies for its functioning, meaning servers, routers and cables. This infrastructure can be potentially attacked both by States, during an armed conflict for example, and

[101] Charles Arthur, 'Anonymous attacks US security company', The Guardian (online article), February 2011

also by non-State actors in the form of sabotage, by terrorist or insurrectionist groups.

The deployment of hard power in cyberspace follows the definition of power as intended in its military and strategic dimension, which understands power as direct coercion; in this case, informational resources found in cyberspace can be deployed for the achievement of a desired goal. The largest and most technologically advanced States are the sole actors detaining the resources needed to carry out these types of offensive attacks[102]. Such actions are categorized as 'advanced persistent threats'[103] and require highly skilled personnel and impressive financial resources to be deployed; previous intelligence data on the target is also needed. A type of advanced threat is the so called 'zero day' attack, that is specifically aimed at affecting a previously undiscovered vulnerability of the operating system; this is the case with the Stuxnet worm, which was programmed to infect an undetected vulnerability of the Samsung software running the SCADA systems of a uranium enrichment facility in an Iranian nuclear plant. It is clear that non-State actors, such as hacktivists, and terrorist groups do not detain the amount of technical, logistic and financial resources for the successful conduction of these extreme examples of coercive power, also because these actors usually prefer to resort to forms of soft power[104].

[102] Nye Jr., 2010

[103] 'Advanced Persistent Threat' is defined by the CCDCOE list of various national cyber definitions as "an adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception). (Definition is provided by the Department of Homeland Security, United States of America).

[104] Robert K. Knake, *Cyberterrorism Hype v. Fact*, Council on Foreign Relations Expert Brief, February 2010. In Nye Jr., *Cyber Power*

Cyber Soft Power

Cyberspace is widely regarded as the prominent informational environment, and thus represents the perfect platform for the diffusion of forms of soft power. An instrument of soft power exclusively available to States is the promotion at international level of specific behavioural procedures and normative standards in cyberspace. States make use of this power through institutional intermediaries, most importantly the International Telecommunications Union (ITU) and the Internet Corporation for Assigned Names and Numbers (ICANN). This last institution has managed to remain under the unofficial supervision of the United States: despite acting as a non-governmental institution for the allocation of domains on the internet, it is based in the US and faces the influence of the US government, more specifically through the Department of Commerce. Through the ICANN, the US has been able to highlight its influence in shaping the Internet normatively and culturally, as well as for its economic interests[105]. In particular, thanks to its strong ties to the ICANN, the US is strategically exploiting these institutional intermediaries as to influence internet governance according to its political and economic priorities through some normative and regulative standards referred as 'rules of the road' for cyberspace included in the International Strategy for Cyberspace promoted by the Obama administration in 2011[106]. Despite the American perspective on internet governance appears to be widely shared by its allies, other influential countries disagree. China and Russia for example promote a different view on the regulation of cyberspace and detain a much more explicit cyber power; these powerful countries, along with their allies, find institutional channels for their policies in the

[105] Betz and Stevens 2011

[106] *International Strategy for Cyberspace: Prosperity, Security and Openness in a Networked World*, White House, May 2011

International Telecommunications Union as well as in the Shanghai Cooperation Organization (SCO).[107]

Cyberspace can be also used as a platform to launch informational campaigns aimed at promoting or at degrading certain political issues as a form of soft power.

In 2009 for example, in occasion of the political protests in Iran in the aftermath of the presidential elections, the US government managed to pressure Twitter to postpone a scheduled technical maintenance of the website so that the social network would be active during the days of the protests and so that it would be utilized by the protesters for the organization of gatherings and for the divulgation of political messages. Despite this however, a few months later the Iranian Cyber Army was able to deviate web traffic directed at Twitter to a website filled with anti-American propaganda, and in early 2010 the Iranian government managed to prevent access to Twitter from its citizens and to other social networks[108].

The informational channels offered by cyberspace can also serve as platforms for reinstating and legitimizing existing political discourses as well as to introduce new ones. An example of this trend is the transformation that certain issues face through the securitization process, with regards in particular to the identification of specific threat actors in cyberspace, such as hackers. This type of process is particularly relevant in the illustration of the issue of cybersecurity by policy makers to the public, and the media plays an instrumental role in this. Hackers are usually depicted in the media as technically skilled individuals that breach into computer systems of other people for stealing and destructing data, while in reality, as seen in the first chapter, the hacker community is very diverse and includes professionals that

[107] A more detailed overview on the diverging Western/Eastern stances on internet governance is presented in the Chapter on Cyber Diplomacy.

[108] Michael B. Farrell, 'Iranian Cyber Army Hack of Twitter Signals Cyberpolitics Era', The Christian Science Monitor (online article), December 2009

are legally employed by security firms and governments for the protection of their networks and for the development of more resilient operating systems. A bad moral status was also attributed by part of the media to Julian Assange of WikiLeaks in 2010, when his background as hacker was meticulously highlighted in a derogatory manner[109]. The WikiLeaks revelations of 2010 represent an informational conflict between a non-State actor and State actors resulting in a loss of soft power from the latter. With the release of more than 250,000 diplomatic cables, the group managed to compromise the affected States' political reputation and the official relationships between them, and most importantly to affect their soft power.

Cyberspace is also a potent medium for the diffusion and the promotion of terrorist propaganda. Terrorist groups reinforce their soft power predominantly through effective communication and cultural representations, and that happens mostly online. Terrorist web platforms, despite the various attempts of take-downs by national and international authorities, thrive on the internet for the amplified outreach of their messages. Terrorist content shared online has the direct objective of inducing individuals to change their initial preference and to adhere to their ideals, setting an agenda and thus exercising soft power. Terrorists use digital platform for the promotion of terrorist ideals, for the recruitment of followers, for fund raising and for the management of conventional operations. By using strategically the internet, some territorial and limited terrorist groups like Al Qaeda have managed to transform their organizations into horizontal global networks, instrumental for the irradiation of the terrorist ideology[110].

A form of soft power is also exercised by governments in the presence of a pressure originating from them on web companies and service providers to

[109] Luiza Ch. Savage, 'Julian Assange: The Man Who Exposed The World', Macleans (online article), December 2010

[110] Nye Jr. 2010

conform the content hosted on their servers to legal and moral standards of the State, by agreeing with these companies to block or to filter undesired material. For example, in China the Google search engine renders unavailable most of the content originating from the West and the government restricts access to online material linked with the Falun Gong religion; the government of Saudi Arabia blocks certain websites considered as against the religious moral; France and Germany prevent discussions on the Nazi ideology from taking place online[111]. Governmental control over behaviour on the internet is a form of soft power as it rests on the framing of a political agenda that influences the social conduct of the subjects affected.

State-use of non-State actors for the building of Cyber Power

The global nature of cyberspace and the scale of the resources needed for the building of effective cyber power has made it difficult for States to develop national approaches and capabilities. In the cyber domain, they are confronted with the empowerment of non-State actors that have acquired an influential amount of power through the exploitation of the potentialities of global outreach and anonymity provided by the internet[112]. The exponential rise of the internet as a cross-border and open resource has managed to distribute forms of power to its users, who in certain cases are capable of detaining a reasonable amount of soft power that can be used to influence states; in this context, it is important for states to preserve the historical access to power they have detained since the Westphalian system. It is then in cyberspace that States feel the need to master cyber power, especially in the form of hard power.

[111] Ibid.

[112] Katharina Ziolkowski, *Peacetime Espionage – New Tendencies in Public International Law*, 2013

Cyber power can be developed **directly**, which means that the State chooses to invest in ICTs for defensive and offensive purposes in order to enhance national capabilities. The most powerful and resourceful states have already done this, as it is the case with the United State, Western European countries (France, Germany), China and Russia, but some others might not dispone of the resources and might compete with other actors for the acquisition of those, especially with the industry[113]. In the absence of national capabilities, States can develop national cyber power **indirectly** through the use of proxies, more specifically through non-State actors such as hackers and criminal organizations for the conduction of cyber operations, exploiting the resources and the expertise that these actors have acquired in cyberspace. In this case, it is irrelevant whether governments openly recognize and acknowledge taking advantage from these entities within their societies. When components of civil society are incorporated into strategies aimed at building national cyber power, the term to be used is '*integrated national capability*' as identified by Klimburg. He states in particular:

"[The] 'whole of nation' approach to security policy – the joint integrated application of state (whole of government) and non-state (business and civil society) efforts to attain common objectives – has only recently begun to be applied in the US government circles. The West, and the United States in particular, has been relatively slow to realise the importance of integrated national capabilities in cyber power. Russia and China both have highly visible non-state cyber capabilities that interact with their governments"[114].

One reason for the resort to proxies in building cyber power might be that of testing the effectiveness of an offensive attack. While preserving for themselves the possibility of denying any involvement, States can direct and

[113] Christian Czosseck, *State Actors and Their Proxies in Cyberspace*, in Katharina Ziolkowski (ed.), Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy, NATO CCD COE Publication, Tallinn 2013

[114] Alexander Klimburg, *Mobilising Cyber Power*, 2011

support non-State actors (such as hackers or other technically skilled individuals) in the conduction of informational operations in the place of the State for testing the defence system of the target and its preparedness in responding; in addition to that, the government can also witness what the reaction at international level can be. The Conficker operation represents a good example of this eventuality. Deployed in late 2008, Conficker consisted of a complex combination of the most sophisticated malware and botnets technologies available at the time, that propagated at an impressive speed creating an army of ten million remotely controlled devices around the world. The surprising fact that was discovered during the multiple attempts at taking down the malware by joint national-international personnel, was that the Conficker operation was not criminally motivated, as the use of botnets would have implied, but rather seemed to be purposely set up to test the resilience of the malware and its prolonged resistance against take-downs[115]. In addition to that, the Conficker Working Group have put forward the hypothesis that the reaction of the international community was intended to be studied by the creators of the malware as well[116]. The take-down process of the Conficker malware engaged security experts and national law enforcement agencies for more than a year, and this testifies that although no precise authorship for the malware was directly available, resourceful State actors were probably behind the operation considering the sophistication and the resilience of Conficker.

A second reason for the resort to proxies in building cyber power can consist in governments taking advantage of the powerful potential of hacktivists and criminal groups to carry out inter-State offensive operations that might be perceived as hostile acts if undertaken by the State itself[117]. In this regard, governments can find particular advantages in exploiting groups of individuals

[115] Czosseck 2013

[116] Porras, P., Saidi, H., & Vinod, Y., *An Analysis of Conficker*, SRI International, 2009

[117] Czosseck 2013

whose actions in cyberspace reflect the political strategy of the state: these are the so-called '**patriotic hackers'**[118]. Russia is particularly taking advantage of these groups of hackers: its involvement is widely regarded as the source behind the cyberattacks against Estonia in 2007, when individuals were allegedly enrolled and supervised by Russian authorities in the conduction of the attacks against Estonian governmental websites. Evidence of this can be found in the attempts put forward by Estonian authorities to involve Russia in the prosecution of those deemed responsible, only to be denied by Russia itself[119]. Hard evidence of Russian involvement is still absent, made more difficult by the fact that the attacks were executed through the use of American servers, which further complicated the process of attribution. The DDOS attacks that targeted the Georgian governmental websites in the context of the Georgian-Russian conflict of 2008 are also considered as being the result of the action of patriotic hackers supervised by Russia. In these cases, groups of politically-motivated hackers might even carry out offensive actions independently and be supported logistically and financially by governments only in a second phase, but either way States deny involvement most of the times.

Existing national resources located within the State's territory can be used to develop national cyber power: that is the case with the **industry** sector, more specifically the technologically-focused one and producer of ICTs. Here, the problem for the States in the contention with the industry for the acquisition of professionals in the field of ICTs, who often converge into the private sector. For this reason, cooperative agreements between governments and the industry are promoted[120]. These mostly consist in exchanges of best

[118] Patriotic hackers are citizens or supporters of a specific country that deploy their hacking capabilities to perpetrate cyberattacks or other forms of digital sabotage against another State or non-State entity perceived as an enemy.

[119] Nye Jr. 2010

[120] Czosseck 2013

practice, collaborative incident simulations as well as private-public partnerships for the notification of breaches into sensitive networks to relevant authorities. Such partnerships also exist in the context of critical infrastructure protection: the European Commission for example has implemented two directives in this sense, the EU Initiative on Critical Information Infrastructure Protection in 2007 and the European Public-Private Partnership for Resilience program in 2010. The more recent Network and Information Systems directive, included in the EU Strategy for Cybersecurity, is also structured along the same guidelines[121]. Increased resilience in national critical infrastructure augments the defensive potential of national networks, and thus the degree of cyber power, but in absence of national capabilities the State has to build a reliable collaboration with the industry sector.

Cyber Power can be also built through the use of **volunteers**. Estonia represents the best example in this perspective: prior to the cyberattacks faced in 2007 in fact, Estonia could only rely on the protection provided by the national CERT (Computer Emergency and Response Team), established in 2006. In the wake of the cyberattacks, most of the reaction was handled by a joint effort made up of representatives of the industry and of members of civil society consisting of technically skilled individuals, who operated under the supervision of the CERT. These individuals were subsequently recognized officially and ended up forming the Estonian Cyber Defence League[122]. In addition to that, the Estonian government set up a new organisational framework that included volunteers in the State's strategy for cybersecurity.

Cyber power can be then acquired with the support of **Hacktivist groups**. If a hacker community and culture is present in the country, the State can consider

[121] More detail on the European Union Cybersecurity Strategy is presented in the chapter on Cyber Diplomacy.

[122] Czosseck 2013; Estonian Defence League 2013

the possibility of enrolling these individuals for its own interests. Hacktivist groups have gained massive prominence in the current political discourse, and the power that they have gained in cyberspace is advantageous for the State in terms of technical expertise and of intelligence data.

China is widely regarded as being actively engaged in cyberspace, as the multiple accusations it received from different countries of operating systematic economic and political espionage have showed. These actions, although undertaken autonomously, are allegedly conducted under the knowledge and the direction of Chinese authorities, despite the fact that they have always denied any involvement and have instead declared China to be a target as much as the other countries are[123]. An incident occurred some time ago demonstrated that the Chinese government has direct authority over hackers located within its territory: in 2001, during a series of cyberattacks between hackers from the US and China (known as the 'Cyber World War One'), a foreseen second wave of attacks was allegedly scrapped as a result of an official request to the hackers originating directly from the Chinese government[124].

The involvement of elements of civil society, which comprises individuals involved in criminal activities, hackers and ICT-specialized personnel employed by the industry is increasingly being incorporated into China's information warfare capabilities, and is also a key provision included in its newly adopted Integrated Network Electronic Warfare Strategy[125].

Finally, cyber power can be also developed by exploiting elements of organized **cybercrime**. The efficiency and the infiltration potential offered by the criminal activities conducted in cyberspace can be used strategically by

[123] 'Obama warns of 'weaponising the internet' ahead of Xi Jinping's US visit', The Guardian (online article), September 2015

[124] Nye Jr. 2010

[125] Krekel, B., Bakos, G., & Barnett, C., *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation*, Northrop Grumman Corporation, 2009

States that are trying to enhance their national capabilities, preserving for them the possibility of denying any involvement once the cyberattacks were to be exposed. Russia represents a valid example in this sense. The Russian Business Network (RBN) is a prominent organization in the field of cybercrime, and is, up until now, the only criminal organization to be officially recognized as a threat by NATO[126]. In 2007, the RBN made up for 40% of the revenues generating from cybercrime globally and has been since dismantled by authorities[127]. Despite this, the group is believed to continue its operations covertly within a network of smaller organizations, and also to be unofficially tied to the Russian government. The Russians are suspected of tolerating cybercrime activities within its borders, using the criminal networks as a source for recruitment. The cyberattacks against Georgia in 2008 are believed to having been conducted by elements of the Russian cybercrime[128].

In addition to that, Russia, along with China, is not part of the European Council's Convention on Cybercrime, which further testifies Russia's unclear approach to the issue.

From these observations on States and the means they deploy to acquire a certain degree of power in the cyber realm, it is clear that the importance given to the digital domain is as strong as it has ever been.

Conclusion

The peculiar features of the informational substrate consisting mostly in the low barriers for entry, anonymity and asymmetries in vulnerabilities have manged to reduce power differentials among actors in a way that is not identified in the other traditional domains of international relations. This is

[126] 'The Evil (Cyber) Empire', The Daily Beast (online article), December 2009
[127] Klimburg 2011
[128] Nye Jr. 2010

also to be linked to the diffusion of power witnessed in the global politics of the current century. But “diffusion of power does not mean equalization”[129]: State actors are still the ones that detain the resources that renders them predominant in the digital environment, but they find nevertheless the cyber domain more challenging as they have to compete for influence with subjects that would not have the same power in the physical world. Power distribution in cyberspace does not mirror the balances established in the real world[130]; subjects with historical access to power find themselves in the condition of facing threats emerging from a wide range of interest-driven subjects that are able to exercise both forms of hard and soft power. Non-state actors are likely to gain more power in the cyber realm and States will have to come to terms with the growing relevance of networks as the key dimension for the contention of power.

[129] Ibid.

[130] Czosseck 2013

Chapter Four

Cyber War

Preface

In recent years, the threats deriving from cyberspace have grabbed the attention of a wide range of stakeholders, from transnational enterprises, to governments and international organizations, who are struggling in defining the challenges of the 'cyber-threat' in the wider picture of the shifting strategic context of the 21st century. Smith has described it as "a world of confrontations and conflicts rather than one of war and peace"[131], where the main threats are constituted by conflictual and asymmetric hostilities between States that are operated mostly through non-military means (like propaganda and the diffusion of soft power), and by the increase in power of non-State actors and by intense political and economic espionage. In this sense, cyberspace appears the most appropriate environment for mastering these activities. As a result, the digital environment is being increasingly militarized both for the purpose of ensuring the security of computer networks and for the achievement of offensive capabilities to effectively deter opponents. The proliferation of sophisticated cyber weapons such as the Stuxnet worm has disclosed the disruptive potential of cyber war and the growing vulnerabilities of networked societies and economies; cyberspace has then become an environment of contention and of confrontation between powers.

[131] Rupert Smith, *The Utility of Force*, 2005

Cyber War: hype or reality?

While war has been a constant in global history, the ways in which warfare is conducted differs greatly among epochs, reflecting advancements in social organization and in technology. Indeed, warfare conducted in cyberspace differs greatly from the one conducted in the other traditional domains. Physical presence is absent, the strategy and the identity of the enemy are usually unclear, and offensive actions with potentially disruptive effects can be undertaken at an almost instant speed from any location around the globe. Cyberattacks have been growingly concerning policy makers up to the point of identifying unauthorised intrusions into governmental networks and network-based disruptions of critical infrastructure as threats to national security that may lead up to responses involving the use of force, as foreseen by the Obama administration in its International Strategy for Cyberspace[132]. Moreover, cyberattacks have also been shaped as to become potential foreign policy and military instruments. In the light of this, the present environment of cyberspace is an increasingly securitized and militarized one, where the approach chosen by many States is that of 'preparation for the battlefield'[133], which involves low-scale confrontations between State and non-State actors and sporadic informational conflicts, in the perspective of scaring off contenders by demonstrating one's offensive potential.

Offensive and defensive cyber capabilities are being increasingly developed around the world: a survey conducted by the United Nations Institute for Disarmament Research in 2012 assessed that 114 States had developed national cybersecurity programmes, where 47 of those had given a specific role to the military, while the others had only initiated programmes with

[132] *International Strategy for Cyberspace: Prosperity, Security and Openness in a Networked World*, White House, 2011

[133] The term is contained in US-specific operational terminology and refers to the close cooperation between military forces and the intelligence community in the preparation of (usually) covert actions in foreign soil.

civilian purposes[134]. The survey goes further affirming that 12 of the 15 largest military spenders have already developed or are in the process of developing proper cyber-warfare units; of these, 10 are considered of detaining established offensive capabilities. The US, China, Russia, the UK and France are widely regarded as the countries with the most advanced cyber arsenal.

The current discussion about cyber war and cyber warfare, although hyped by the media and by academics, is controversial: among the strategic community, there are those who advocate for more offensive uses of cyber means and who recognize the advent of cyber war as the most pressing national security issue of our times, and others who consider the 'cyber' dimension of conflict between nations as a natural extension of human affairs into a different environment[135]. What makes the debate even more unclear is that, at the present time, a regulative framework comparable to that for traditional warfare is absent. There exists indeed a strong debate over what constitutes an act of cyber warfare and what approaches are needed, and what are the implications under current international law; only future State practice and events will pave the way for regulation among nations at international level.

A middle ground in this debate is generally found in the assumption that a new hi-tech model of warfare, instead of replacing traditional instruments of warfare, will be growingly added to military doctrines and strategies serving as support for conventional operations. Taking a glance at how military operations are conducted currently, one could assume that this process has already taken place: most of the instruments deployed for conventional warfare are in fact massively dependent on information and communication technologies. That is the case with remotely controlled weapons, such as nuclear command and control systems, and drones, that are the prime

[134] UNIDR 2012

[135] David J. Betz and Tim Stevens, *Cyberspace and the State: Toward a Strategy for Cyber-Power*, The International Institute for Strategic Studies, 2011

instrument utilized in the War on Terror. It can be then fair to assume that, at the time being, cyber warfare is an essential component of the current instruments of war[136]. Despite this, it is unlikely that standalone acts of cyber war will be as effective as conventional ones[137]. Up until now, no cyberattack has managed to provoke physical destruction or harm to the population: this finding undermines the assumption of those who wish to treat cyberattacks as equivalent to armed attacks, and further complicates the interpretation of conflicts conducted via cyber means according to international law. Nonetheless, the issue of cyber warfare continues to pose a threat to national security and engages the international community on how to adapt to this new strategic domain.

The following list of notable cyber conflicts between State actors will shed light on what are the main features characterizing acts of cyber warfare and what nations are (often believed to be) involved; the next section will then clarify whether cyberattacks can be interpreted as uses of armed force under current international law.

Notable Instances of Cyber Conflicts involving State actors

- The 1991 Gulf War was the first international conflict where the use of informational operations was considered. The intent was to disrupt the sophisticated Iraqi air defence and missile network so that US and allied aircrafts would enter the Iraqi airspace unnoticed. The cyber component of the operation was scrapped as it was deemed unreliable by high ranks of the US military. In spite of that, the Gulf War was conceived as the first of a new generation of conflict where physically overcoming the enemy was not the ultimate goal but winning the

[136] Hakan Mehmetcik, *A New Way of Conducting War: Cyberwar, Is That Real?* in Kremer and Muller (ed.), *Cyberspace and International Relations: Theory, Prospects and Challenges*, Springer 2014

[137] Betz and Stevens, *Cyberspace and War*, 2011

'information war' was conceived, starting from then, as being just as important for the achievement of 'information dominance'[138];

- A sophisticated cyber weapon codenamed 'Moonlight Maze' attacked in 1998 the computer network of the Pentagon extracting confidential files containing information about military hardware designs and plans from defence contractors. The attack is believed to having originated from Russia, but the Russian government has denied any involvement[139];
- The 1999 Operation 'Allied Force' is considered as the first 'Internet War'. In the context of the internal turmoil in Yugoslavia and of the Serbian contraposition to the allied forces, extensive informational campaigns through the Internet were carried out by each of the parties involved in the conflict; in addition to that, incidents caused by hackers also occurred[140];
- In 2001, a confrontation between US and Chinese hackers rose as a consequence of a mid-air collision between a Chinese fighter and a US spy plane. Following that event, massive waves of cyberattacks from both sides caused the defacement of American and Chinese governmental websites, and Distributed Denial of Service attacks were also deployed. The event is commonly known as 'Cyber World War One' as hackers from other nations were also involved (Saudi Arabia, Pakistan, India, Brazil, Argentina, Malaysia, Korea, Indonesia and Japan)[141];

[138] Richard A. Clarke, Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do About It*, HarperCollins, 2010; Alan Collins, *Contemporary Security Studies – Cybersecurity*, Oxford, 2013

[139] Katharina Ziolkowski, *Peacetime Espionage – New Tendencies in Public International Law*, in Katharina Ziolkowski (ed.), *Peacetime Regime for State Activities in Cyberspace*. International Law, International Relations and Diplomacy, NATO CCD COE Publication, Tallinn 2013

[140] Collins 2013; 'Inside The First "Internet War"', Wired (online article), January 1999

[141] Collins 2013

- 'Titan Rain' is a series of coordinated cyberattacks on high-profile US computer systems that have been active since 2003, but are believed to have been ongoing for at least three years. The cyberattacks were aimed at gathering information on the US computer systems, and targeted sensitive information from defence industries as well as from NASA. Chinese-sponsored hackers are believed to be responsible[142];
- A persistent series of cyberattacks that lasted over three weeks affected Estonia in 2007 following a political dispute with Russia over the removal of a World War Two memorial representing a Soviet soldier. Distributed Denial of Service attacks and defacements were deployed against websites of the Estonian parliament, banks, ministries, newspapers and broadcasters, affecting their functioning by overwhelming with web traffic the servers providing the websites. Some ethnic Russians located both in Estonia and in Russia were found responsible for the attacks, and although it is yet to be proven officially, there exists a wide consensus over Russia being supportive in the conduction of the operations. The cyberattacks against Estonia are generally considered as the first inter-State conflict to take place in cyberspace and in the wake of the attacks, Estonia even turned to NATO requesting the collective defence clause to be activated[143];
- In September 2007, Israeli air forces bombed a suspected nuclear materials site in Syria that was allegedly being developed with the support of North Korea. The Israelis managed to carry out the offensive action by compromising the Syrian Russian-bought air defence radar, so that the Syrians were not be able to detect foreign aircrafts entering their airspace. The type of technology deployed for this kind of attack has not been disclosed, though many believe it to be a US-developed

[142] Ziolkowski 2013

[143] Clarke and Knake 2010; Betz and Stevens 2011; Collins 2013

airborne system code-named ‘Senior Suter’. This event sealed the first military operation in which informational means were used along with conventional ones[144];

- In August 2008, in the context of the conflict between Russia and Georgia over the Abkhazia and South Ossetia regions, a series of cyberattacks were directed against the Georgian digital infrastructure: DDOS attacks and defacements hit Georgian governmental websites, as well as the Georgian President’s own web page, where the pictures of the leader were replaced with ones of Adolf Hitler. The attacks had more serious consequences, as Georgian servers were flooded with web traffic at the same time of the Russian counterattack in South Ossetia, preventing the Georgians from accessing foreign news websites such as the CNN and the BBC. Moreover, the banking sector was paralyzed and the national ‘.ge’ web domain was suspended. The level of coordination with the conventional operations on the ground suggest that the cyberattacks against Georgia were not only the work of patriotic hackers, but as it was later confirmed, Russian intelligence was seemingly once again involved[145];
- In March 2009, an extensive espionage network was discovered, later named ‘GhostNet’. Reports indicated that the computer systems of the Tibetan offices around the world had been infiltrated through the introduction of malware, and that in two years the operation had managed to spy on 1259 computers in 103 countries. In addition to the Tibetan offices, foreign ministries of Iran and Indonesia were also spied on, along with the Indian, South Korean, Taiwanese, Portuguese, German and Paki embassies. The reports found that the operation had

[144] Clarke and Knake 2010; Sharon Weinberger, ‘How Israel Spoofed Syria’s Air Defense System’, Wired (online article), April 2007

[145] Clarke and Knake 2010

originated from servers located in China, and though the Chinese government denied any responsibility, it has been assumed that the sophistication of the techniques and the political nature of the targets imply the involvement of a major government[146];

- The Stuxnet worm, discovered in June 2010, is a sophisticated type of malware that was deployed to compromise the functioning of the Supervisory Control and Data Acquisition (SCADA) system used for the Iran's debated uranium enrichment programme in the Iranian nuclear plant of Natanz. The Stuxnet worm is widely considered as the world's first digital weapon, as it managed to cause physical damage in the centrifuges of the nuclear facility and to actually slow down the Iranian nuclear programme; the sophistication of the malware and the political intent behind it have led experts to link the United States and/or Israel to the attack[147].

All of the incidents listed above are theoretical instances of cyber conflicts between State actors, although only circumstantial evidence that links the cyberattack to a specific country has been since recovered, as the techniques used for the concealment of the source's identity are very sophisticated. Aside from the issue of attribution, most of these incidents (except for Stuxnet) have not resulted in damage to human beings or to physical assets, and so cannot be treated as traditional instances of war. The next session will try to define, under current international law, whether cyberattacks can be intended as armed attacks, and whether the resort to self-defence is admissible.

[146] Ziolkowski 2013; Collins 2013

[147] Kim Zetter, 'An Unprecedented Look at Stuxnet, The World's First Digital Weapon', Wired (online article), March 2014; Sascha Knoepfel, *Clarifying the International Debate on Stuxnet: Arguments for Stuxnet as an Act of War*, in Kremer and Muller (ed.), *Cyberspace and International Relations*, Springer 2014; Clarke and Knake 2010

Cyberattacks as Armed Attacks?

Violations under international law of the prohibition of the use of force and of interference via cyber means can be assumed at this point as constituting lower-level violations rather than uses of force. Actions carried out in cyberspace can only be assumed as acts involving the use of force against another State only if they result in the damage of physical entities or in the death or injury of people, and overall in disruptive effects on the territory of said State. While precise criteria for the identification of what threshold a cyberattack must reach in order to be treated as an armed attack are absent, conflicts between States in the cyber realm have grown in numbers and intensity. The political and legal implications in this context are peculiar to the specific characteristics of cyberspace, that are unseen in other traditional domains. In particular, the most debated issue is whether a State that has faced a cyberattack can invoke measures of self-defence as included in Article 51 of the UN Charter, thus responding with the use of force against the attacking entity, which might be a State or a non-State actor[148].

On a theoretical level, self-defence can be admissible only in the event that the cyberattack is shaped as an armed attack, as prescribed in Article 2(4) of the Charter. Given the fact that an armed attack in the wording of Article 51 is only intended as consisting in conventional means, it appears that no cyberattack can be assumed in the same way. The interpretation of the notion of armed attack as enshrined in Article 51 leads to the conclusion that no cyberattack would constitute an armed attack in any case; such an assumption has been unanimously rejected by academics and the strategic community, as cyberattacks can result in having the same disruptive potential as

[148] Robin Geiβ, Henning Lahmann, Freedom and Security in Cyberspace: Shifting the Focus Away from Military Responses Towards Non-Forcible Countermeasures and Collective Threat-Prevention, in Katharina Ziolkowski (ed.), Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy, NATO CCD COE Publication, Tallinn 2013

conventional ones. The solution is then found in considering cyberattacks as armed attacks only when its consequences are equal to those provoked by kinetic force. The *effects-based* approach is the preferred one when dealing with conflicts in the cyber domain, which implies that the consequences of a cyberattack must result in physical destruction or in injuries or death of people. There exists a broad consensus on the effects-based approach, as it brings similarities with the way biological and chemical weapons are treated in international law[149].

The main obstacle in the application of the doctrine of self-defence with regards to cyberattacks is the **attribution** of the source, be it a non-State entity or a State. The issue of attribution and the violations of international law linked to cyber incidents is still regarded by Director of US National Intelligence James R. Clapper as the "greatest strategic challenges regarding cyber threats"[150], despite the ongoing advancements in technology and research. In order for the notion of self-defence to be applied entirely, an individual must be identified in relation to a State in the conduction of a wrongful act as prescribed by Part One, Chapter II of the International Law Commission Draft Articles on Responsibility of States for Internationally Wrongful Acts (Articles 4 to 11). However, the use of the provisions included in the ILC Articles on State Responsibility is limited, since in cyberspace sophisticated technical tools allow for source concealment and for the obscuration of action. Therefore, the determination of the attacker's identity in cyberspace is ever more difficult and will be hardly overcome; even in the most notorious

[149] Ziolkowski 2013

[150] Director of U.S. National Intelligence James R. Clapper, Unclassified Statement for the Record on
the Worldwide Threat Assessment of the US Intelligence Community for the Senate Select Committee on
Intelligence, 31 January 2012. Found in Robin Geiβ, Henning Lahmann, *Freedom and Security in Cyberspace: Shifting the Focus Away from Military Responses Towards Non-Forcible Countermeasures and Collective Threat-Prevention*

instances of inter-State cyber conflicts, attribution to a specific entity has never been definite, as only circumstantial evidence could be collected. Conversely, when State responsibility is invoked, in international jurisprudence a 'clear and convincing' degree of evidence is always required[151].

Even when definite attribution can be proved, it usually takes a reasonable amount of time for analysts and experts to collect enough evidence that would link with certainty a cyberattack to a State. The possibility of a State retaliating in self-defence following a period of time used for attributing the cyberattack faced is provided by the Tallinn Manual on the International Law Applicable to Cyber Warfare. Despite admitting the requirement of immediacy with regards to self-defence, in the Manual's perspective the State victim of a cyberattack can resort to self-defence even some time after the violation has occurred. That period must serve for the correct identification of the attacker, and once its identity is known, the State would be able to retaliate. In the case that such process might not result in attribution, the victim State might still act in self-defence if it has reason to believe that additional cyber operations are "likely to follow"[152]. Assuming this approach, the period of time necessary for the identification of the attacking entity becomes more relevant and undermines the principle of immediacy required by the notion of self-defence. Such an interpretation is a dangerous one, as it would justify uses of force outside of established temporal dimensions. Moreover, it would increase the risk of unexpected escalations of inter-State conflicts[153].

Although the assumption that current international law is entirely applicable to cyberspace is widely shared, the legal implications regarding issues of inter-State conflicts in the cyber realm are controversial and can result in the

[151] *The Trail Smelter Arbitration Case* (United States of America v. Canada), Inter-American Court of Human Rights, 1941

[152] International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence, *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Michael N. Schmitt (ed.), Cambridge 2013

[153] Geiβ and Lahmann 2013

doctrine of self-defence being ruled out due to the problems related to attribution. International law demands attribution, and the degree of evidence required for invoking State's responsibility for an armed attack cannot be found in relation to cyberattacks. Therefore, the possibility of retaliating to cyberattacks through use of force is, under current international law, unlikely. Scholars have then tended to find alternatives to self-defence, legal instruments that would justify the State's unlawful reaction to cyberattacks without implying military means. Such an instrument can be found in countermeasures.

Legal alternatives to self-defence: Countermeasures

Since not every malicious operation conducted via cyber means constitutes an armed attack as described by Article 51 of the Charter, several scholars believe that countermeasures can be used as the preferred unilateral tool for States to respond to cyberattacks. Countermeasures, as enshrined in Article 49 of the ILC Articles on State Responsibility, are defined as instruments of self-help available to States that are directed at inducing the State responsible of an unlawful act to comply with its international obligations[154]. These instruments are pacific reactions to wrongful acts that, although constituting violations, are justified by international law. As opposed to self-defence, countermeasures do not necessarily entail uses of force, and their ultimate goal is the termination of the unlawful conduct. Limitations to countermeasures prescribe that they be directed only at the State deemed responsible, and that they shall not violate the prohibition of the use of force as enshrined in the UN Charter; moreover, they must comply with the principle of proportionality.

[154] Article 22 of the ILC Articles on State Responsibility states that "the wrongfulness of an act of a State not in conformity with an international obligation towards another State is precluded if and to the extent that the act constitutes a countermeasure taken against the latter State".

The use of countermeasures as remedies for cyberattacks has different implications.

Firstly, by using countermeasures, a State that is facing or that has been a victim of cyberattacks can 'offensively' protect itself through the use of 'active defence' systems installed in its computer networks. Active defence systems are tasked both with the identification of a malicious action or unauthorised intrusion and with the automatic offensive capacity of terminating such actions by affecting in turn the attacker's computer with the same malicious code deployed for the attack[155]. These sophisticated systems are effective but have the potential to cause collateral damage additional to the one first intended.

Secondly, countermeasures can be used as responses to violations of the legal duty for States to prevent cyberattacks from generating within their territory. The 'duty to prevent' principle is present in contemporary international jurisprudence: the International Court of Justice has mentioned it in its case law multiple times and is especially relevant with regards to cybersecurity. In the *Corfu Channel* case for example, the Court affirmed the principle that every State is under an "obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States"[156]. In this situation, the violation does not appear to be the attack, but rather the fact that a State was not able to prevent it from happening. The duty to prevent originates from the principle of 'due diligence', meaning the State's due diligence in respecting the obligations towards other States. Within international organizations, the principle of due diligence found its application in the context of international cybersecurity, as it is the case with the UN's General Assembly Resolution

[155] Active defences are defined are "in-kind responses […] against the attacker's system" in order to "offensively disable the source of the attack". Hathaway OA et al, *The Law of Cyber Attack* (2012) 100 California Law Review 817

[156] *Corfu Channel Case* (United Kingdom v. Albania); Merits, International Court of Justice (ICJ), 9 April 1949

55/63 of December 2000, and is also reflected in the Tallinn Manual[157]. The problem with this approach lies in the evidence required to claim a State's responsibility for cyberattacks generating from its territory. The US for instance has often claimed to detain evidence of cyberattacks hitting its networks originating in particular from China and Iran, but that evidence is mostly circumstantial and collected from intelligence and political sources rather than technical ones; technical evidence is hard to obtain, and so is the establishment of legal responsibility.

The types of countermeasures listed above are adapted to the cyber context, but more traditional categories can also be used, such as economic coercion, suspension of bilateral agreements and so forth. Nonetheless, in the current international cybersecurity framework countermeasures are likely to become the prevalent tool in dealing with inter-State cyber conflicts[158]. Although the issue of attribution applies to countermeasures as much as to self-defence, those instruments allow for pacific conflict resolution and do not foresee unexpected escalations and unregulated resorts to the use of force as implied in the 'cyber' interpretation of the self-defence doctrine. As regards international law, only future State practice will establish definite normative frameworks and will pave the way for agreements on conflict regulation in the cyber realm at international level.

Although it might appear distant and theoretical when applied to current international law, the issue of cyber war is constantly engaging the strategic community and finds its application in the military doctrines of the most powerful nations, such as the United States and China. In the light of this, the next section will analyse the first 'cyber weapon', the Stuxnet worm, and will

[157] The Tallinn Manual states in particular: "a State shall not knowingly allow the cyber infrastructure located in its territory or under its exclusive governmental control to be used for acts that adversely and unlawfully affect other States".

[158] Geiβ and Lahmann 2013

try to provide a theoretical foundation, according to traditional strategic thought, to acts of cyber war.

The Effectiveness of Cyber Weapons: the Stuxnet worm

The revelation of the Stuxnet worm in June 2010 introduced to the world the first cyber weapon. Being specifically designed to target and to disrupt the supervisory control and data acquisition (SCADA) system used for the functioning of centrifuges for uranium enrichment in the nuclear facility of Natanz in Iran, the Stuxnet worm showed the vulnerability of the industrial infrastructure in the face of cyberattacks[159]. In fact, the increased exposure of power grids and of critical infrastructure supplying vital services to societies (energy, water) to cyberspace by enhancing their automation and interconnectivity has resulted in growing vulnerabilities that can be exploited through cyber means causing disruptive effects[160]. In this sense, the Stuxnet worm has disclosed this potential and has consequently started a lively debate on the effectiveness of cyber weapons, found to be just as damaging as conventional ones.

In June 2010, it was revealed that a sophisticated type of malware, called 'Stuxnet', managed to destroy 1000 out of the 9000 centrifuges at the Iranian nuclear site in Natanz. Stuxnet was designed to do so following specific steps. Firstly, the worm affected the Microsoft operating system of the computers that command the centrifuges; in a second phase, it managed to spread its malicious code directly to the centrifuges, compromising the functioning of the Siemens-produced SCADA system, that was the program used by Iran in most of its nuclear facilities. The technical experts that analysed the Stuxnet worm have found that the sophistication of the malware must have been the product

[159] Kim Zetter, 'An Unprecedented Look At Stuxnet, The World's First Digital Weapon', Wired (online article), March 2014

[160] Joseph S. Nye, Jr., *Cyber Power*, Belfer Center for Science and International Affairs, 2010

of governments for the amount of financial resources needed to create it and the human expertise involved. In addition to that, there must have been also detailed knowledge of the layout of the nuclear site and understanding of the functioning of the centrifuges; the suspects are then found in State actors, specifically the United States and/or Israel. The strong suspicion that governments might be involved in the deployment of the Stuxnet worm have led the strategic community to deem it as the first 'cyber weapon' and as the first explicit use of offensive cyber means to physically compromise strategic assets such as nuclear plants. As a result, international media have speculated on the rise of cyber warfare describing Stuxnet as an act of war[161].

The Stuxnet worm as an act of war

As it was mentioned previously, the debate on what constitutes an act of war in the context of cyber warfare is ongoing. The finding that was reached with the analysis of this chapter is that cyberattacks can be considered acts of war only if they provoke physical damage with long-term consequences for the State and bring harm to the population. The effect-based approach is then the one to be preferred. But at international level, the identification of an act of war in cyberspace, in the absence of a shared definition, rests upon the perception of the individual State. According to Martin Libicki, a notable cybersecurity expert at RAND Corporation, there are three modalities through which an act of war in cyberspace is defined internationally: universally, multilaterally and unilaterally[162]. A universal definition would certainly be the result of a resolution from the General Assembly of the United Nations or one agreed with an international treaty as inclusive as possible. Multilaterally, the definition might come from international or regional organizations such as

[161] Sascha Knoepfel, *Clarifying the International Debate on Stuxnet: Arguments for Stuxnet as an Act of War*; Collins 2013

[162] Martin Libicki, *Cyberdeterrence and Cyberwar*, Santa Monica: RAND Corporation, 2009

NATO; ultimately though, since none of these entities has generated a shared definition so far, cyber warfare can only be identified unilaterally by individual States. Delegating the definition of an act of war in cyberspace solely to the subjective perception of States would bring great instability to the international system and would increase the risk of conflict escalations. One solution to this situation is provided by Sascha Knoepfel, who proposes the classic interpretation of war by Clausewitz as the key for defining war in cyberspace, so that it would be shared by actors in the international community[163].

War is defined by Clausewitz as "an act of violence to compel our opponent to fulfil our will" in the first chapter of its book *On War*[164]. Knoepfel breaks down the components of the definition identifying five fundamental variables: violence, the presence of an attacker and a victim, the fulfilment of the attacker's will, and an issue of a conflict between the attacker's will and the one of the victim, and applies them to the Stuxnet worm, in order to identify it as an act of war following Clausewitz's definition. In the context of the Stuxnet worm, it was previously stated that the Supervisory Control and Data Acquisition system running the centrifuges in the Iranian nuclear facility in Natanz were directly targeted. The malicious code of the worm was found to be designed specifically for that purpose. Consequently, we can identify the issue of conflict, as included in Clausewitz's definition of war, in the Iran's uranium enrichment program. The fact that a conflict is present is testified by the general adversity of the international community towards the program, as proved by the six United Nations Security Council resolutions on the topic and by several affirmations from political leaders. The United States and Israel are particularly vocal against Iran, who defends its nuclear program claiming that it is for peaceful purposes. Iran then appears to be clearly the target of the

[163] Knoepfel 2014

[164] Carl Von Clausewitz, *On War* (Reprint ed.), Princeton University Press. 1989

cyberattack, the ‘victim’ following Knoepfel’s approach. Evidence to prove this can be found in the specificities of the malicious code, which was designed to compromise precise functionalities of the centrifuges for uranium enrichment present in the Iranian nuclear facility in Natanz. Moreover, the Command and Control servers that received the data sent by the malware where for the most part located in Iran. The discovery of Stuxnet by Iranian authorities likely happened around the Summer of 2010, but the official announcement where President Ahmadinejad acknowledged its nuclear program of being attacked happened in September 2010. The United States and Israel are believed to be behind the deployment of the Stuxnet worm, the ‘attackers’. The malware, being programmed to specifically affect the software running the centrifuges, must have been tested in protected environments with the same infrastructure present in the nuclear facility. The amount of intelligence data both on the layout of the site and on the functionalities of the centrifuges, in addition to evidence of access to that technology, have led experts to consider the US and Israel as responsible. Furthermore, it is speculated that Israel had expressed its will to attack nuclear facilities in Iran to the US in early 2008[165]; the US, rejecting this plan, who would have then authorized initiatives to “undermine the electrical and computer systems around Natanz”. David Senger, in his book *Confront and Conceal: Obama’s secret Wars and Surprising Use of American Power* adds that President Obama, when taking office in 2008, had inherited the initiative undertaken by Bush with Israel and included it in a series of cyber activities codenamed ‘Olympic Games’[166]. Moreover, the New York Times has stated that special Israeli forces had collaborated with the US to launch a cyberattack on an Iranian nuclear facility. Their involvement can be then considered an open secret, even if direct involvement has never been

[165] D. E. Sanger, ‘U.S. rejected aid for Israeli raid on Iranian nuclear site’, New York Times (online article), January 2009

[166] D. E. Sanger, *Confront and Conceal: Obama’s secret wars and surprising use of American Power*, Crown, 2012

explicitly expressed by neither parties. Continuing to follow the Clausewitz definition of war and applying it to the Stuxnet worm, the element of violence needs to be found. Although not in its physical dimension, the malicious code incorporated in Stuxnet can represent an act of violence: its technical configuration is aimed at disrupting control systems used in industrial processes by compromising the code of the Programmable Logic Controllers (PLC) that run the machines, ultimately causing the disruption of the centrifuges and thus physical damage.

All of the variables (an issue of conflict, the presence of an attacker and a victim, the fulfilment of the attacker's will and the involvement of violence) identified in the definition of war proposed by Clausewitz are respected in relation to the Stuxnet worm, according to the analysis operated by Knoepfel; the malware can be then considered an act of war. The Stuxnet worm however is somewhat of an exception in the context of cyber warfare, and can be considered as the sole act of cyber war that does not involve conventional means. Taking a glance to all of the other instances of cyber conflicts between States in fact, it can be stated that the fundamental properties of war as theorized by Clausewitz cannot be met[167]. First of all, in order for cyberattacks to be labelled as traditional acts of war, according to Clausewitz war must have a political nature, that is fought among organized communities and that involves specialised armed forces. Plus, it should be fought for the achievement of specific goals set by political units, which do not always coincide with nation States. In the context of cyberattacks, identifying the source of the attack, in most cases, is nearly impossible, as it was mentioned previously discussing the pressing issue of attribution. Furthermore, cyberattacks are generally directed more towards private entities rather than governments: in this case, they should be treated as acts undertaken by

[167] Hakan Mehmetcik, *A New Way of Conducting War: Cyberwar, Is That Real?*, in Kremer and Muller (ed.), *Cyberspace and International Relations*, Springer 2014

individuals and treated as acts of espionage, subversion and sabotage rather than acts of war. Therefore, cyberattacks can be regarded as acts of war when their political nature is implemented by organized forces. Secondly, the political aim of an act of war entails the presence of a definite purpose.

As Clausewitz states that war is "in the first place, that under all circumstances, regarded not as an independent thing, but as a political instrument" a political aim that underlies the offensive action undertaken in cyberspace must be present. With regards to cyber war, Nye defines it as "hostile actions in cyberspace that have effects that amplify or are equivalent to major kinetic violence"[168]. The aim underlying such acts is that of disrupting and degrading the enemy's networks: in the view of Richard J. Harknet, cyberattacks would amount to the complete destruction of the opponent's societal connectivity, meaning a social community's ability to access to the networked services of communication, financial transaction, health and transportation[169]. These type of offensive actions would have an enormous impact on today's societies, considering the degree of reliance on information technologies that most basic infrastructure show nowadays. Nonetheless, so far no cyberattack has reached such level of intensity, although the threat potential is certainly present. Finally, Clausewitz identifies violence as the defining feature of war that distinguishes it from simple political contention. Even though it is commonly acknowledged that cyberattacks have the potential to cause considerable harm, the degree of violence resulted from cyberattacks cannot be treated equally as the one resulting from conventional uses of force. The Stuxnet worm, in this case, stands out as the most sophisticated and effective cyber weapon in history, showing to the world the degree of damage that can be

[168] Joseph S. Nye, Jr., 'Nuclear lessons for cybersecurity?', Strategic Studies Quarterly, 2011

[169] R. J. Harknett, *Information Warfare and Deterrence*, 1996

caused with information technologies and the disruptive potential that these new instruments of war can represent in future conflicts.

Although fascinating in its originality, the existence of cyber weapons like Stuxnet have the potential to cause great instability to the international system by initiating an 'arms race' directed at enhancing the States' offensive cyber capabilities.

Cyber Deterrence against the proliferation of cyber weapons

The unmonitored proliferation of offensive cyber weapons has the potential to affect security in the international system bringing tension and imbalances in power. As it is the case with Stuxnet, the victim of such an attack could eventually replicate the code of the malware to deploy it either against the attacker or against another target. Although Iran has not yet resorted to such a possibility, it is likely that the proliferation of sophisticated and effective cyber weapons can bring States to invest more in the development of offensive cyber capabilities in order to retain strategic advantages for themselves. China, the United States, France, the United Kingdom, Russia and Israel have all dedicated institutions that deal with the cyber realm, often within branches of the military. The United States in particular have postulated that the response to cyberattacks might not just be limited to cyber weapons, but that other appropriate means would be considered. In this situation, a deterrence system needs to be ensured, so that offensive capabilities do not offset defensive ones. According to the Offence-Defence theory, there exists in the international system an offence-defence balance that dictates the advantages of offensive and defensive strategies, thus impacting on the structure of the system itself[170]. If the balance is altered towards an offensive strategy, the probability of war increases and competition among States is heightened; conversely, if

[170] Salma Shaheen, *Offense-Defense Balance in Cyber Warfare*, in Kramer and Muller (ed.), *Cyberspace and International Relations*, Springer 2014

the defensive strategy is chosen, cooperation prevails and the system is characterized by peace. The situation present in cyberspace currently is a militarized and competitive one, and that is enhanced by the increasing proliferation of offensive cyber weapons, among which Stuxnet represents the prime example. Developing offensive cyber weapons is an attractive option for States, as it entails considerable strategic advance and power concentration, but by doing so, instances of conflict might degenerate into wars involving conventional means.

The deterrence theory developed during the Cold War can then become adapted to the cyber domain. After World War Two, and especially during the Cold War, the conception that a State's ability to deter an enemy enhances its security meant that stability in the international system could be reached if the costs of attacking were greater than its gains: this then translated into the concept of Mutually Assured Destruction, which implied the ability to absorb a nuclear attack from the Soviet Union with an equal counterattack (second strike capability). In the context of cyberspace, deterrence can be achieved through the development of defensive capabilities: superiority in defence decreases the attacker's incentive to strike first and consequently the chances of war decrease[171]. However, given the effectiveness of cyber weapons, it rests upon the State whether to use them to enhance deterrence or to acquire offensive capability; it is likely that they would serve for both purposes, but once defensive strategies are enhanced, the attacker's offensive intent would be discouraged and in the long-term, disruptive uses of cyber weapons might cease.

A concrete example of defensive strategy is represented by the so-called Active Defence systems. These systems, incorporated into the State's network gateways, are able to detect malicious code and to respond accordingly by

[171] Shaheen 2014

overwhelming the attacker's network with the same malware that was utilized in its operation. Infiltrations into governmental networks can also be deterred through systems called Virus Walls. If an attacker attempts infiltration, the Virus Wall detects it and acts as a defence shield that sends viruses to the attacker's computer and that ultimately disables its functioning[172]. These defensive techniques aim at making offensive cyberattacks harder to succeed and costly, just as deterrence theory suggests. In order for defence to be more effective, States must also invest in reducing the vulnerabilities of the networks running critical infrastructure and its exposure to the internet. Stuxnet highlighted the potential vulnerability of the various types of software utilized for industrial processes; the exploitation of previously unknown vulnerabilities in operating systems ('zero-day vulnerabilities') can be an incentive for the affected parties to fix them and to render the networks more resilient.

Concentrating on the development of defensive cyber capabilities can potentially deter the proliferation of offensive cyber weapons such as Stuxnet and create security, but ultimately the effectiveness of the offence-defence balance depends on whether cyber weapons are dedicated to one strategy or to the other[173]. The fact that cyberspace remains a largely unregulated environment renders this choice more difficult; this lack of governance implies that States, with regards to the regulation of cyber weapons, are left to operate in an international system characterized by self-help and by individual threat perception.

[172] Hann Samir Kassab, *In Search of Cyber Stability: International Relations, Mutually Assured Destruction and the Age of Cyber Warfare*, in Kramer and Muller (ed.), *Cyberspace and International Relations*, Springer 2014

[173] Ibid.

Cyber Defence: the EU Solidarity and Mutual Defence Clauses and NATO

While the regulatory framework surrounding the definition of cyberattacks as armed attacks according to international law remains unclear, it is widely regarded by strategists and academics that cyberattacks can provoke the same amount of damage as conventional ones. For this reason, regional and international organizations such as the European Union and NATO have developed cooperative mechanisms for a common response to cyberattacks resorting to existing treaties. In the European context, the EU has been increasingly engaging with issues concerning cyber war and cyber warfare, in particular with the adoption of the European Council's 'EU Cyber Defence Policy Framework' in November 2014. Despite the cooperative mechanisms set out by the document and moreover by the EU Cybersecurity Strategy (which will be discussed in the following chapter), a cohesive cyber defence policy that relies on existing binding obligations is absent[174]. In particular, it is unclear how the two main provisions dealing with the EU response to natural or man-made disasters, or to military aggressions contained in the Treaty of Lisbon are to be applied in connection to cyberattacks[175]. The first of such provisions is the Solidarity Clause. The Clause (Article 222 TFEU) binds Member States to cooperate in the assistance of an individual country facing disasters or crises which it cannot face individually through its own resources. Interpretation of this norm has remained unclear since its conception, and Member States are uncertain over the practical mechanisms for its invocation. For this reason, the European Council has adopted, in June 2014, rules and procedures for the implementation of the Solidarity Clause ('Implementation

[174] 'Cybersecurity and cyberdefence: EU Solidarity and Mutual Defence Clauses', briefing by Patryk Pawlak, European Parliamentary Research Service (EPRS) Members' Research Service, European Parliament, June 2015

[175] European Union, Consolidated version of the Treaty on the Functioning of the European Union, 13 December 2007, 2008/C 115/01

of the Solidarity Clause')[176]. Through this Decision, the Council widens the meaning of the term 'disaster' and provides a broader definition including "any situation which has or may have a severe impact on people, the environment or property, including cultural heritage", which may therefore require coordination and timely response at EU level. Conceiving a 'disaster' or 'crisis' in these terms can potentially imply the activation of the Solidarity Clause by a Member State as a result of a cyberattack. In this situation, the Clause would only deal with the consequences of a cyberattack and not with the cyberattack itself.

The second provision, the Mutual Defence Clause, was introduced in Article 42(7) of the Treaty of the European Union and can be assumed as the European equivalent of Article 5 of the North Atlantic Treaty on collective defence[177]. The Clause states an armed aggression on the territory of a Member State triggers the military involvement of all the others. Therefore, if the damages provoked by a cyberattacks were to equate those of an armed attack, theoretically this provision can be invoked. The implementation of the Mutual Defence Clause has witnessed less engagement by the EU bodies as its limits and conditions are not well defined. Moreover, it is regarded as a rhetorical concept as it has never been put to use so far; it could however be reinforced with its application to cyberattacks, following the ongoing process in this field within NATO. The declaration adopted in the aftermath of the 2014 NATO Summit in Wales, states that members of the organization may invoke the provisions included in Article 5 of the Treaty concerning collective defence when a cyberattack equates the effects of an armed attack[178]. Considering the involvement of Member States of the EU in NATO (of which only six are not

[176] 2014/415/EU: Council Decision of 24 June 2014 on the arrangements for the implementation by the Union of the solidarity clause

[177] The North Atlantic Treaty, 1949

[178] 'NATO Summit Updates Cyber Defence Policy', NATO Cooperative Cyber Defence Centre of Excellence website, ccdcoe.org, 24 October 2014

members), a similar perspective could be adopted with respect to the Mutual Defence Clause; it has to be noted however that the NATO stance on the matter is still theoretical and implies that political decisions in this regard have to be taken on a case-by-case basis. Overall, it is likely that the European Union and NATO will take steps forward in the development of precise collective defensive measures against cyberattacks, especially taking into account a statement included in the EU Cyber Defence Policy Framework, according to which "the objectives of cyber defence should be better integrated within the Union's crisis management mechanisms"[179]; furthermore, the EU Cybersecurity Strategy directly outlines the issue of EU-wide cooperative mechanisms in case of a major cyber incident or attack. In its wording, it is stated that "a particularly serious cyber incident or attack could constitute sufficient ground for a Member State to invoke the EU Solidarity Clause"[180].

Conclusion

The topic of cyber war has been embraced by the strategic community and by some academics as the most pressing issue concerning national security. In the findings of this chapter, it was highlighted how scholars are divided on the eventuality of cyber war, and while strongly debated, it can be assumed that in some ways cyber warfare has already happened. Informational means are being used along conventional instruments of war, as it is the case with remotely controlled devices like drones; instances of cyber conflicts, despite the difficulties of attribution, engage an increasing number of entities, ranging from States to non-State actors. Cyberspace is characterized by low-level confrontations and the major part of cyberattacks is constituted by acts of sabotage, subversion and espionage. Moreover, by defining the features of

[179] EU Cyber Defence Policy Framework, Council of the European Union, 18 November 2014

[180] Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, European Commission, 2013

armed attacks according to international law, it was stated that cyberattacks do not reach the threshold of uses of force and that consequently cannot be responded with military means in self-defence. The rising conception of 'pre-emptive' self-defence in response to presumed State-sponsored cyberattacks or resulting from mistrust towards a State's behaviour in cyberspace needs to be rejected; the automatic assumption that a cyberattack (or threats deriving from cyberspace, such as cyber espionage) constitutes an armed attack would end up considerably lowering the threshold for the use of force in international relations and would create systemic instability and proliferation of conflicts. Nonetheless, strategies around the world (especially in the United States) advocate for this eventuality, in the face of the growing number of informational attacks and of the impact that these have on modern societies and economies. What renders the rise of cyber warfare threatening for governments is the absence of established norms to regulate behaviour in cyberspace: cyber weapons, if left to proliferate freely, can seriously affect the patterns of the international system and war can arise. However, it was noted that acts of cyber war are unlikely to take place exclusively, and that their damaging potential does not equate that of conventional attacks. Moreover, despite being said to be entirely applicable to cyberspace, it was pointed out that, for now, international law does not detain the adequate responses to instances of cyber war. It can then be affirmed that standalone cyber war is not likely to happen. What is likely however, is that cyber means will be more and more utilized along with traditional instruments of warfare. The damaging potential inherent to cyber weapons has to be taken into account, considering how much of the infrastructure and of the industrial processes constituting vital assets for economies are networked and thus vulnerable to cyberattacks. Cyberspace will continue to be characterized by competition and contention for informational dominance as long as actors in the international community do not establish behavioural norms to be followed and limitations to offensive attitudes, so that the digital domain, given its universal and borderless dimension, can be shared peacefully by all the components of global societies. But then again, the strategic advantages that States can acquire through the channels of cyberspace are unprecedented, and for this reason they will continue to preserve and to develop cyber capabilities in the eventuality of the ‘preparation to the battlefield’.

Chapter Five

Cyber Diplomacy

Preface

Cyber diplomacy is a new and developing branch of international relations, and can be defined as the political interactions among States that shape cyber issues globally within bilateral, multilateral relations and international organizations[181]. Despite not being fully incorporated into foreign policies yet, the need to categorize cybersecurity talks as 'cyber diplomacy' testifies the relevance of cyber issues in today's international affairs. Given the absence of internationally agreed treaties on the topics of cybersecurity, cyber warfare and of State behaviour in cyberspace, cyber diplomacy represents a powerful foreign policy tool that aims at filling the legal and political gaps currently present in the field of international cybersecurity and at harmonising the actors' policies to secure the cyberspace. The most relevant issues that explored through cyber diplomacy are: ICT policies, transnational cybersecurity, cyber dialogues between countries, internet governance and protection of human rights online[182]. Cyber issues are prioritized differently depending on the individual country but the most pressing issue concerning policy makers globally nowadays is represented by the quest to find shared perceptions of the cyber threats and to ensure responsible behaviour with regards to offensive uses of cyber means. The difficulties in reaching universal agreements are due to the divergences on the

[181] Heli Tiirmaa-Klaar, *Cyber Diplomacy: Agenda, Challenges and Mission*, in Katharina Ziolkowski (ed.), *Peacetime Regime for State Activities in Cyberspace*. International Law, International Relations and Diplomacy, NATO CCD COE Publication, Tallinn 2013

[182] Ibid.

political dimension that is to be given to cyberspace: some States promote the multi-stakeholder governance of the internet with partial governmental overlook, while others, mainly developing States, advocate for a stricter regulation and for the entire application of principles of public international law, namely State sovereignty as well as territorial integrity, allowing for increased State control of the information flow channelled through cyberspace.

Given the absence of universally shared treaties on cyber issues and the reluctance of States to commit internationally, cyber diplomacy aims at finding a balance in the tension between freedom and security experienced in cyberspace through practical remedies which do not involve obligations on behalf of States, but that set behavioural norms for rendering cyberspace more secure and immune to inter-State conflicts[183]. The key priorities in the international cyber diplomacy agenda are: critical infrastructure protection, the transnational fight against cybercrime and espionage, confidence building measures and capacity building, as well as the most pressing one of internet governance.

Critical infrastructure protection is a topic that has been transferred into inter-State dialogues on cyber issues as a result of the acknowledgement that nowadays most critical infrastructure and related industrial processes are highly networked and heavily reliant on information and communication technologies; such vital assets for modern societies and economies can be potentially targeted by cyberattacks in the context of an armed conflict, and the rise of sophisticated cyber weapons such as Stuxnet have disclosed the vulnerabilities underlying those systems that can be exploited by malicious software. In this context, cooperation between CERTs (Computer Emergency

[183] Katharina Ziolkowski, *Confidence Building Measures for Cyberspace*, in Katharina Ziolkowski (ed.), *Peacetime Regime for State Activities in Cyberspace*. International Law, International Relations and Diplomacy, NATO CCD COE Publication, Tallinn 2013

Response Teams) and law enforcement authorities is required in order to monitor incidents and to share information for timely responses. National CERTs cooperate through international forums where best practice among technical experts and governmental representatives is exchanged[184]. Securing critical information infrastructures has been also prioritized within the United Nations through the 2003 Resolution entitled 'Creation of a global culture of cybersecurity and the protection of critical information infrastructure', later updated into a resolution on the 'Creation of a global culture on cybersecurity and taking stock of national efforts to protect critical information infrastructure' adopted in 2010[185]. This last resolution was sponsored by 40 countries led by the United States who established a voluntary self-assessment tool for national capabilities in ensuring the protection of critical information infrastructure. The European Union issued a directive on Critical Infrastructure Protection (CIP) in 2008, setting out a procedure that enabled Member States to identify critical infrastructure designated as European[186]. Furthermore, following the cyberattacks against Estonia in 2007, an Action Plan on Critical Information Infrastructure Protection (CIIP) was created within the Commission's 2009 Communication on Critical Information Infrastructure Protection. The Plan was later implemented in 2011[187].

Transnational Cybercrime represents another relevant topic in the international cybersecurity agenda. Despite the absence of official statistics concerning the economic losses provoked by criminal activities operated in

[184] Tiirma-Klaar 2013

[185] UNGA Res 64/211

[186] 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

[187] 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 'Achievements and next steps: towards global cyber-security', European Commission 2011

and through cyberspace, its impact on modern economies is considerable[188]. As cybercrime is often organized transnationally, national responses and policies are incoherent and thus inefficient; cybercrime needs to be addressed through international cooperation, as individual approaches of States are not enough. The complexity of the offences and the contrast between different jurisdiction have managed to make the issue of cybercrime ever more difficult to identify and to counteract. The fight against cybercrime represents a key aspect in national security policies as cybercrime networks could be exploited by hostile States and by terrorist groups; plus, States that fail to address cybercrime within their territories create 'safe havens' for cyber criminals that inevitably end affecting other States.

The most important international effort in the fight against cybercrime is represented by the 2001 Council of Europe's Convention on Cybercrime, also known as the Budapest Convention[189]. The Convention has managed to reach 51 signatory States, many outside of Europe, and stands out as the only internationally agreed treaty on cyber issues. The Convention sets out rules aimed at harmonising internal laws and at enhancing the fight against cybercrime; in addition to that, it provides guidelines for law enforcement and judicial authorities and for the implementation of national cybersecurity strategies. The initiatives on cybercrime promoted by the European Union have gone further: in 2011, a joint EU-Council of Europe Eastern Partnership launched a regional project on cybercrime, as well as a new project on international cybercrime established in 2013[190]. The Council of Europe's approach to cybercrime initiated with the Convention, besides representing the sole international treaty on the topic of cybersecurity, can serve as a

[188] Symantec estimated in 2011 that the losses experienced by individuals globally as a result of cybercrime amounted to 388 billion USD annually.

[189] Council of Europe, Convention on Cybercrime, Budapest 2001

[190] 'EU launches new project to battle cybercrime in Eastern Partnership countries', EU Neighbourhood Info Centre (online article), January 2016

blueprint for other agreements dealing with other cyber issues and as the most relevant source for setting normative standards with regards to transnational cybercrime.

In the European Union context, a European Cybercrime Centre (EC3) was created in 2013 within Europol, that facilitates operational coordination among the Member States' law enforcement agencies and provides for information exchange in investigations. Furthermore, in 2013 a Directive on Attacks Against Information Systems was adopted and replaced a previous Framework Decision of the European Council[191]. The Directive aims at establishing shared definitions of criminal offences and relative sanctions; the main crimes identified are: illegal access to information systems, illegal system interference, illegal data interference and illegal interception.

Cyber espionage also poses a sever threat and is being increasingly addressed in discussions on cyber issues. Since espionage is being increasingly regarded as a matter concerning national security and has massively increased in scale and influence, cooperation among international actors is the sole effective tool to counteract the phenomenon: once inserted into the cyber diplomacy agenda, behavioural norms to be established at international level can be achieved. Again, cyber espionage is dealt with mostly in the context of bilateral relations, and it is especially relevant in the political relationship between the United States and China: during the meeting between President Obama and Xi Jinping in September 2015, cybersecurity was one of the main priorities discussed between the two leaders. In the press conference following the meeting, President Obama announced that the United States and China had reached an agreement stating that neither government "will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information for commercial

[191] Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA

advantage”[192].

Cyber espionage is a tricky topic to discuss internationally, as espionage is an acknowledged custom in international relations and no State wants to give up on that tool by exposing other State’s activities, especially if conducted covertly and anonymously, as it is the case for espionage conducted through informational means. In addition to that, attribution is never definite and accusations between States need to be handled carefully. It is then unlikely that cyber espionage would be regulated at international level, but its impact can be contained through the establishment on mutually agreed behavioural norms between States.

Overall, the ongoing shift of the topic of cybersecurity into the strategic field concerns policy makers all over the world and has managed to pressure States to develop national cybersecurity strategies, but attempts at formulating universally agreed sets of rules to be followed in cyberspace have failed. The strategic advantages and the political implications derived from the exploitation of the potentialities inherent to the informational substrate have prevented States to assume transparent positions and have instead managed to polarize the political discussion on cybersecurity. The risk underlying the absence of international regulation is that of transforming cyberspace into a new global battlefield: asymmetries in capabilities and the development of offensive cyber weapons can result into a conventional military conflict. For this reason, international agreements directed at reducing the risk of cyber war have been proposed in the past, but with scarce success. The wish to prevent an ‘arms race’ from happening in cyberspace through the creation of an arms control regime is not feasible due to the peculiarities of the cyber realm and of the ineffectiveness that the control provisions would have with

[192] Dan Roberts, ‘US and China back off internet arms race but Obama leaves sanctions on the table’, The Guardian (online article), September 2015

regards to cyber weapons and capabilities[193]. Therefore, the international community has dealt with cyber issues resorting to alternative tools, namely to diplomatic efforts and to more practical and non-invasive remedies, among which Confidence Building Measures (CBMs) stand out.

Confidence Building Measures as a remedy to cyber conflicts

Confidence Building Measures (CBMs) are an instrument of international politics aimed at establishing, through inter-State negotiation, practical rules and processes of preventive crisis management directed at discouraging the eventuality of war in the context of inter-State conflicts by limiting miscalculations over the other States' military capabilities and by reducing threat misperception, in order to mitigate conflicts and to impede the outbreak of an armed confrontation[194]. CBMs have proven to represent an effective remedy against the use of nuclear weapons in the context of the Cold War, and their provisions for transparency, cooperation and stability can be applied to cyberspace, despite some difficulties. Since the established notions contained in CBMs display a heavy reference to conventional arms and military strategies as they were conceived in the context of disarmament, the application to cyberspace cannot be automatic[195]. But conceiving CBMs as instruments directed at identifying a certain degree of predictability of State behaviour and at discouraging the resort to uses of force, they can serve for the purpose of securing cyberspace and for reaching a shared conception of State behaviour in cyberspace as well as a dimension of stability in the cyber dimension of international relations.

In particular, CBMs containing provisions related to information exchange and cooperation can represent valuable instruments for the implementation of

[193] Katharina Ziolkowski, *Confidence Building Measures for Cyberspace*

[194] Zdzislaw Lachowski, *Confidence-Building Measures*, in Max Planck Encyclopedia of Public International Law

[195] Ziolkowski 2013

cybersecurity. Such measures can be found listed in several documents originated within international and regional organizations: the OSCE-promoted *Vienna 2011 Document on Confidence and Security Building Measures*[196], besides binding all of its 57 Member States, includes, among others, information exchange and cooperation measures that are applicable to the cyber context. Furthermore, a list of CBMs is displayed in the *Consolidated List of Confidence and Security Building Measures* elaborated in 2009 in a document elaborated within the Organization of American States (OAS)[197]. The document emphasizes cooperation measures that can be adapted to cyberspace: the notion regarding information sharing about the respective military structures and forces for example, can be transferred into the cyber context assuming the composition of the military forces as the cyber units; programmed training exercises for military forces can be translated into exercises between Computer Network Operations (CNOs) units; regular visits to military infrastructures from foreign officials can become visits to cyber units, and the monitoring of new installations can regard developments of new methods of hacking[198]. This process is an easy task at a theoretical level, but in reality these measures would be difficult to implement in the cyber context at international level due to the secrecy that States usually reserve for their cyber capabilities. However, some measures listed in the OAS document can be applied to cyberspace more easily: information sharing between militaries on defence policies and national doctrines, cooperation for technological research, and most importantly inter-State collaboration for the protection of critical infrastructure. Currently, CBMs are being developed mostly within international and regional organizations.

[196] Organization for Security and Co-operation in Europe, *Vienna Document*, 22 December 2011

[197] Organization of American States, Consolidated List of Confidence and Security Building Measures for Reporting according to OAS Resolutions (Approved at the meeting of January 15, 2009) CP/CSH-1043/08 rev. 1

[198] Ziolkowski 2013

Within the United Nations, the topic of cybersecurity was first introduced in 1998 with a draft resolution proposed by the Russian Federation entitled *Developments in the field of information and telecommunications in the context of international security*[199]. The United Nation's General Assembly First Committee on Disarmament and International Security deals with international security in cyberspace: following a proposal from the Russian Federation in 2001, a special Group of Governmental Experts (GGE) was established, called Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security[200]. Despite failing to reach consensus, this first GGE was followed by a second (2009-2010)[201] which, among other things, called for States to enhance cooperation in the field of cybersecurity and defined CBMs as the preferred tool for conflict prevention in cyberspace available to States. The third GGE (2012-2013)[202] went further and listed in detail the following CBMs for cyberspace:

- Voluntary exchange of views and information on national strategies and policies, best practices, decision-making processes, relevant national organizations, and measures to improve international cooperation;
- Creation of bilateral, regional and multilateral consultative frameworks for confidence building e.g., workshops, seminars and exercises;
- Expanded information sharing on ICT security incidents;
- Exchanging names and contact information of national points of contact for crisis management, including Computer Emergency Response Teams (CERTs);

[199] UNGA Res 53/70, 4 December 1998

[200] *Developments in the field of information and telecommunications in the context of international security* UNGA Res 53/70 (4 December 1998)

[201] UNGA Res 60/45 (8 December 2005)

[202] UNGA Res 66/24 (13 December 2011)

- Increased cooperation to address security incidents that could affect ICT infrastructures or critical infrastructure, and
- Enhanced mechanisms for law enforcement cooperation (with regards to incidents that could otherwise be misinterpreted as hostile State actions)[203].

This set of CBMs as elaborated by the GGE in 2013 does not mirror the traditional notions of CBMs by including in its assessment other cyber threats (uses of cyber means by terrorist groups, for example): this rather suggests an attempt at formulating an international strategy for cybersecurity directed at all Member States of the United Nations and thus not limited to the 15 countries represented in the GGE[204].

The Organization for Security and Co-operation in Europe is an international institution that has fully embraced the issue of cybersecurity. Between 2009 and 2013, OSCE hosted several meetings on international cybersecurity that allowed multilateral discussions on State behaviour in cyberspace, on cybersecurity awareness and on the identification of the cyber threats. The *Resolution on the Overall Approach of the OSCE to promoting Cybersecurity* of 2011[205] initiated a more normative-oriented process of cybersecurity: in 2012 the OSCE Permanent Council established a working group tasked with the elaboration of a set of Confidence Building Measures applicable to cyberspace. The final set of draft measures (2013)[206] includes CBMs aimed at enhancing

[203] UNGA, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, UN Doc A/68/98, 7 June 2013

[204] Ziolkowski 2013; Members of the GGE include representatives from: Argentina, Australia, Belarus, Canada, China, Egypt, Estonia, France, Germany, India, Indonesia, Japan, Russia, the United Kingdom, the United States.

[205] *Resolution on the Overall Approach of the OSCE to Promoting Cybersecurity*, in OSCE, *Resolutions of the OSCE Parliamentary Assembly Adopted at the Twentieth Annual Session*, Belgrade, 6 to 10 July 2011

[206] United States mission to the OSCE, *Informal Working Group Established by PC Decision 1039: Revised Draft Set of CBMs*, 7 November 2012

co-operation, transparency, predictability, stability, and at reducing the risks of misperception, escalation, and conflict that may stem from the use of information and communication technologies. The norms-based approach initiated with the cybersecurity talks within OCSE has been welcomed by its members and can serve as a blueprint for other initiatives in sein of other international institutions.

Cyber issues are also discussed at bilateral level. In 2013, the United States and Russia concluded an agreement on CBMs for cyberspace in the framework of a bilateral meeting on information and communication technology security[207]. Among others, the measures include: arrangements for information exchange between CERTs and the creation of a hotline for crisis management and communication; direct collaboration between the US Cybersecurity Coordinator and the Russian Deputy Secretary of the Security Council for monitoring potential threats deriving from incidents derived from ICTs; and the establishment of a bilateral working group on ICTs and international security included in the context of the US-Russia Bilateral Presidential Commission. The inclusion of communication channels that link directly high offices is proof of the importance that cybersecurity represents for both countries, and chances are high that the cyber dialogue between the US and Russia will continue in the future. The United States have also an ongoing, despite conflictual, dialogue on cybersecurity with China: the talks on cyber issues that led up to the bilateral presidential meeting of September 2015 resulted in an agreement that committed both parties to cooperate in conducting investigations on malicious activity in cyberspace and to identify and endorse norms of behaviour; in addition, two high level working groups and a hotline for incident management were established. Along official channels, the academic environment is also used for the US-China cyber

[207] *Joint Statement by the Presidents of the United States of America and the Russian Federation on a New Field of Cooperation in Confidence Building*, The White House, 17 June 2013

dialogue: the 'Sino-U.S. Cybersecurity Dialogue' took place between 2009 and 2012 as a result of the collaboration between the US-based Center for Strategic and International Studies and the China Institute of Contemporary International Relations[208].

In face of the fact that an international treaty on State behaviour and on the limitation to offensive uses of cyber means is unlikely to happen, it was highlighted that CBMs are the most valuable instrument available to international actors for the establishment of stability in cyberspace. But are they entirely applicable to the cyber context? CBMs can assume the form of legally binding obligations or can exist as political commitments. In the traditional disarmament and arms control regimes the first form was preferred, but such a modality is difficult to apply to cyberspace. Hypothetically, a violation of a legally binding norm contained in a treaty on cybersecurity could not potentially be contested by a participating State as a consequence of the difficulty in attributing, technically and legally, malicious cyber activities to a State. This renders any attempt at formulating obligations based on treaties not feasible to the cyber context. Furthermore, the possibility for States of conducting covert cyber operations anonymously gives them the advantage of preserving a high degree of deniability with regards to their operations; additionally, the secrecy regarded to cyber operations would result in the ineffectiveness of binding transparency measures contained in eventual treaties.

Overall, the peculiarities of the technical infrastructure underlying the cyberspace can prevent CBMs in this environment from being fully implemented[209]. Nevertheless, CBMs in this context have a better chance at succeeding than legal obligations. The formulation of measures for

[208] China Institute of Contemporary International Relations (CICIR) and Center for Strategic and International Studies (CSIS), *Joint Statement. Bilateral Discussions on Cooperation in Cybersecurity*, June 2012

[209] Ziolkowski 2013

transparency, cooperation and stability through political declarations are a powerful tool in international relations, and in the cyber domain they serve the scope of influencing the actors' behaviour so that politically binding rules can be established. In particular, political commitments and declarations are proven to be effective in the construction of shared perspectives within the internationally community and are especially useful in the formation of the *opinio iuris*, which often results in norms of customary international law. CBMs for cyberspace can then constitute a form of 'soft law,' as opposed to the establishment of legally binding norms that would otherwise be ineffective: provisions referring to rules on transparency, information sharing and cooperation then become the most appropriate notions of traditional CBMs applicable to cyberspace[210]. Political commitments and declarations can be then considered as the preferred instrument for establishing responsible State behaviour in cyberspace, for reducing risk perception and for limiting conflict escalations, but only future diplomatic endeavours will prove their efficiency. A potential obstacle in the establishment of shared CBMs in cyberspace is however posed by the emerging ideological and political divergences upon internet governance, and more broadly on the role of governments with regards to the oversight of cyberspace.

The international debate on Internet Governance

During the past two decades, security in cyberspace has been increasingly concerning governments. The shaping of global societies into networked horizontal dimensions, supported considerably by the spread of the internet, brought into the field of international security the debate on cybersecurity. In this sense, as it was highlighted in the previous chapters, States are urged as to how to restore sovereign control over the flow of information channelled

[210] Ziolkowski 2013

through the digital architecture of cyberspace, which can be perceived as a threat by liberal and authoritarian governments alike. Despite the common goal, among State actors, of ensuring a safer cyberspace, the modalities through which this is to be reached see the international community divided by political priorities and strategic interests[211]. Security in cyberspace was first addressed, within the United Nations, with a resolution proposed by the Russian Federation in 1998 called '*Developments in the field of information and telecommunications in the context of international security*', which has been discussed every year since. In 2002, the United States put forward the proposal of a similar resolution entitled '*Creation of a global culture of cybersecurity and the protection of critical infrastructure*', which was later adopted in 2010. The content of the resolution was directed at "prioritizing cybersecurity planning and management" and contained nine elements with the purpose of ensuring a global culture of cybersecurity. Despite the two resolutions being similar in contents and in the underlying goals, initial differences could have been noticed in the wording of certain concepts and on the terminology used. While the 1998 resolution sponsored by Russia referred to 'information security', the 2002 adopted the term 'cybersecurity'. The terminologies contained in the two resolutions, although not formulated in detail, managed to attract other countries to support one or the other: despite being the only one to sponsor the 1998 resolution, the Russian Federation was joined by China in 2006, among other countries; the 2002 one instead, saw the initial support of Australia, Japan and Norway, and later additional 36 countries backed the proposal[212].

In the early stage of the formulation of cybersecurity at the international level,

[211] Thomas Renard, *The rise of cyber-diplomacy: the EU, its strategic partners and cyber-security*, European Strategic Partnership Observatory (ESPO), June 2014

[212] Roxana Radu, *Power Technology and Powerful Technologies: Global Governmentality and Security in the Cyberspace*, in Kremer and Muller (ed.), *Cyberspace and International Relations*, Springer 2014

a certain degree of polarization among States is visible, but at that point a shared definition and conceptualization of what was to be understood as cybersecurity was absent. None of the two resolutions from 1998 and 2002 explicitly provided a definition, whether on 'cyber' or on 'information' security. This task was taken up by other non-governmental or transnational institutions, such as the International Telecommunications Union (ITU). In 2008, ITU issued an 'Overview on Cybersecurity', which lists in detail all of the security threats related to the use of ICTs, along with suggestions on the security standards, best practices and policies guidelines to be applied for the protection of networks[213]. While the ITU attempted at defining the concept of cybersecurity, the constant shift of the topic as a consequence of advancements in technologies led the Study Group that elaborated the Overview to leave it up to the international community to define which policies were to be adopted for the future.

In time, the governments' threat perception over malicious uses of ICTs increased. A certain degree of emergency was given in particular to the wording of the 1998 resolution, whose phrase "may adversely affect the security of States" was changed a year later into "may adversely affect the security of States in both civil and military fields"[214]; also following 9/11, a more explicit securitization of cyberspace can be noticed through the identification of the risks stemming from the use of ICTs as "threats" rather than "dangers". This understanding of cyberspace is further enforced by the request put forward in 2011 by the Russian Federation along with China, Tajikistan and Uzbekistan through a letter to the UN Secretary General to introduce an '*International Code of conduct for information security*'[215].

[213] ITU-T Study Group 17, 18 April 2008

[214] UNGA Res 53/70

[215] Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General, UN Doc A/66/359, 14 September 2011

Through this document, the sponsoring parties call for a stricter governmental oversight of cyberspace through the entire application of concepts of public international law, namely sovereignty and territoriality. It is proposed, indeed, that signatories States commit to "prevent other States from using their resources, critical infrastructure, core technologies and other advantages to undermine the right of the countries, [...] to independent control of information and communication technologies or to threaten the political, economic and social security of other countries"[216]. The wording of this statement, besides implying a reconfirmation of the principle of non-interference in cyberspace, also represents the will of some States to implement sovereign control of cyberspace so that it mirrors national policies and legal standards. This attempt at defining the responsibilities of individual States exposes the struggle of States to establish a position of power with regards to cyberspace and the shared perception of cyberspace as the new field for strategic confrontation; furthermore, it testifies the emergence of a growing contestation to the current framework of internet governance, of its priorities, and of its participants.

Conducted in its early stages by technical experts, namely computer scientists and engineers, internet governance is managed internationally by two transnational institutions: the Internet Corporation for Assigned Names and Numbers (ICANN) and the International Telecommunications Union (ITU). ICANN is tasked with the allocation of domains and names on the internet, and therefore plays a key role in ensuring global network operability, while ITU represents the main multilateral entity that deals with issues concerning telecommunications and the interconnectedness of networks across the world by setting technology standards. In addition to these institutions, an Internet Governance Forum (IGF) is held every year and brings together the various

[216] Ibid.

stakeholders involved in internet governance, including the private sector, civil society and representatives of governments. ITU, since its creation, has had a longstanding tradition in promoting network security and cooperation among States in the ICT field, and has also provided guidelines for behavioural norms to be followed in cyberspace: the 1988 International Telecommunication Regulations (ITRs) states that countries are obliged to "avoid technical harm to the operation of the telecommunication facilities of third countries"[217]. Issues and modes of internet governance were addressed in the two meetings, promoted by ITU, of the World Summit on Information Society in Geneva in 2003 and in Tunis in 2005. These initiatives have managed to amplify ITU's powers by reaching a wide range of stakeholders, *de facto* becoming the principal organization dealing with internet governance functions; following these meetings, a rule-making agenda on internet governance emerged at the international level. For this reason, ICANN was created in order to balance the growing empowerment of ITU. ICANN is a multi-stakeholder entity in which governments have a seat within the Government Advisory Committee. Despite claiming to be a non-profit and non-governmental institution, the US-based ICANN remains under the supervision of the US government, in particular of the Department of Commerce[218]. Internet governance is an issue that sees governments increasingly involved and the political discussion ever more ideological and polarized; competing interests and distinct values are employed for changing the existing mechanisms and powers involved in internet governance. This trend assumed concrete form during the World Conference on International Telecommunications (WCIT) held in Dubai in 2012.

[217] International Telecommunication Union, Final Acts of the World Administrative Telegraph and Telephone Conference, Melbourne 1988 (WATTC-88), Geneva 1989
[218] Betz and Stevens, *Cyberspace and the State*, 2011

At the Conference, States convened to the rearrange the 1998 International Telecommunication Regulations (ITRs): the outcome resulted in 89 States signing the new treaty while 55 others explicitly opposed it. The main issue that interfered with the negotiation was represented by to what extent the internet was to be part of the agreement: while the US and its allies wished to prevent it from being mentioned, China, Russia and some Arab countries managed to adopt a new version of the ITRs where the role of the State in internet governance is expanded and the ITU becomes the main body where these issues are discussed and implemented. Ultimately, differences could not be reconciled and the vote showed an increasing global polarisation over the issue of internet governance[219]. In this context, the international community seems divided and in open disagreement: on one hand, a multi-stakeholder framework that includes the private sector, civil society and governments is supported by a group of States, while on the other, a top-down framework managed predominantly by governments with an empowered role for the ITU is promoted by another group of States. A new model of internet governance in which governmental control is enhanced can potentially lead to a lack of fundamental rights protection and would make the implementation of censorship measures easier. The European Parliament, in a resolution from November 2012, is particularly vocal against the outcome of the Conference, stressing that "some of the ITR reform proposals would negatively impact the internet, its architecture, operations, content and security, business relations and governance, as well as the free flow of information online"[220].

[219] Stephen D. McDowell, Zoheb Nensey and Philip E. Steinberg, *Cooperative International Approaches to Network Security: Understanding and Assessing OECD and ITU Efforts to Promote Shared Cybersecurity*, in Kremer and Muller (ed.), *Cyberspace and International Relations*, Springer 2014; R. Bennett, *The gathering storm: WCIT and the global regulation of the internet*, The Information Technology & Innovation Foundation, 2012

[220] European Parliament resolution on the forthcoming World Conference on International Telecommunications (WCIT-2012) of the International Telecommunications Union, and the possible expansion of the scope of international telecommunication regulations (2012/2881(RSP)), European Parliament 2012

While the opposed groups could be easily categorized as ‘democratic’ against ‘non-democratic’, a study conducted by the Centre for International Governance Innovation (CIGI) showed how at the Conference some States behaved differently from expected: Belarus and Brazil for example, have voted against and in favour respectively, despite the fact that the former is considered an authoritarian regime and the latter is characterized by an active civil society. Besides these original patterns in the voting and in coalitions, it appears clear that the opposed groups in the field of internet governance are led by the US and its allies on one side, and by Russia and China and their allies on the other side[221]. This seems to reflect the wider systemic shift in international relations from the unipolar system characterizing the post-Cold War period to an increasing multipolar world. As internet governance continues to be prioritized by policy makers, it is likely that tensions and disagreements will continue to rise.

A remedy to the polarization caused by the debate over internet governance and more broadly, on cybersecurity, can be represented by the creation of common strategies within regional organizations or cooperative groups. The convergence of like-minded States on divisive topics such as these ones can result in the development of cohesive strategies to be promoted with third countries, potentially harmonizing policies internationally through a bottom-up framework: the European Union’s Strategy for cybersecurity is an example of this process.

[221] Tim Mauer and Robert Morgus, *Tipping the Scale: An Analysis of Global Swing States in the Internet Governance Debate*, CIGI, May 2014

Capacity Building at regional level: the European Union's Strategy for Cybersecurity

The European Commission introduced in 2013 the European Union Cybersecurity Strategy. The motivations that led the Commission to focus on increasing the Union's resilience against cyberattacks and cybercriminal activities are driven by different factors. The first one is ecomomic: the EU's economy relies heavily on information and communication technology, thus securing the cyberspace is fundamental for growth and innovation; moreover, this is even more important in the context of the development of the Digital Single Market. The second motivation is political: the implementation of an internal strategy for cybersecurity allows the EU to apply its rule of law and core values of human rights protection and democracy onto the digital environment.

The diverse characteristics of each Member State result in evident discrepancies in the cyber capabilities: the measures of harmonisation, capacity-building and coordination set out by the Strategy aim at enhancing capabilities and the resilience of European critical information infrastructure. In particular, the Strategy identifies 5 main objectives:

- Achieving cyber resilience;
- Reducing cybercrime;
- Developing cyber defence policies and capabilities related to the Common Security and Defence Policy (CSDP);
- Implementing internal industrial and technological resources for cybersecurity;
- Shaping a cohesive cybersecurity policy along core EU values to be promoted internationally[222].

[222] Joint Communication to the European Parliament, the Council, the European Social and Economic Committee and the Committee of the Regions, *Cybersecurity Strategy of the European Union: An Open, Safe, and Secure Cyberspace*, European Commission, 2013

Complementary to the achievement of cyber resilience across the EU is the implementation of the European Commission-proposed Directive on Network and Information Security (NIS). The concept of reinforcing NIS is included in the actions listed by the Digital Agenda for Europe, launched in 2010 as one of the seven flagship initiatives of the Europe 2020 Strategy. The Agenda considers network resilience a fundamental condition for the smooth functioning of the Internal Market, indicating the proposal of a NIS Directive as one of the relevant actions (Action 123)[223]. The proposed Directive, in order to ensure a high common level of network and information security across the EU, sets out measures of minimum harmonisation of cybersecurity policies and require Member States to detain a certain level of national cyber capabilities. NIS strategies are to be developed internally and competent authorities are to be established, especially Computer Emergency Response Teams (CERTs), which have to be present in every Member State. CERTs oversee the security standards required for critical information infrastructure and cooperate with businesses and service providers in the identification and notification of incidents. Their work is enhanced through the collaboration with European institutions such as the European Network and Information Security Agency (ENISA) and the European CERT (CERT-EU)[224]. ENISA, whose mandate expanded significantly by the Commission in 2013, is tasked with threat identification and with risk management; moreover, it acts as an intermediary between the various stakeholders providing assistance the Commission, single Member States and private entities on issues concerning network and information security, harmonising cybersecurity policies at national and international level. CERTs on the other hand are fundamental in the implementation of the Directive, which requires every Member State to set

[223] Digital Agenda for Europe, European Commission website

[224] 'Cyber security in the European Union', Piotr Bakowski, briefing by the European Parliamentary Research Service, European Parliament, 12 November 2013

up one. Their role would be to act as a ‘security point of contact’, exchanging information on security incidents with law enforcement authorities and governments, in addition to provide services such as advising, warnings and trainings. CERT-EU was instituted to strengthen resilience and to mitigate threats against European networks, and its mandate was recently renewed in the perspective of enforcing ties with national CERTs of Member States and international IT security companies[225]. The ultimate goal of the NIS Directive is to change the European approach to cybersecurity from a voluntary and informal one to a legally binding and formal one. Presently, cooperation between Member States on NIS-related issues is on a voluntary basis, and mechanisms for information exchange are absent. The aim of the Directive is to tackle this phenomenon as it represents a disadvantage for the EU as a whole, especially considering the existing gaps in terms of the capabilities of Member States. The proposal of the Directive to ensure high common levels of Network and Information Security through binding obligations for Member States has been met with some reservations. In particular, disagreements regard the definition and scope of the ‘market operators’ that would have to comply with security standards and with incident notification, as well as the indications for national NIS strategies[226]. Despite the debate, an important step in the advancement of the NIS Directive was made in January 2016: members of the European Parliament (MEPs) within the Internal Market Committee (IMCO) agreed to the provisions that require Member States to identify critical operators in energy, transport, health or banking systems, which in turn will have to comply with security measures and will have to notify incidents; moreover, providers of these services will have to ensure that their networks

[225] ‘Cybersecurity in the European Union and Beyond: Exploring the Threats and Policy Responses’, study commissioned by the European Parliament’s Policy Department for Citizen’s Rights and Constitutional Affairs, European Parliament, October 2015

[226] Cybersecurity in the European Union and Beyond, European Parliament 2015

are resilient enough to stand cyberattacks[227]. The criteria used for the identification are: whether the service is critical for society and the economy, whether it depends on network and information systems and whether an incident could have significant disruptive effects on service provision or public safety. Digital service providers, search engines (Google) and online platforms (eBay, Amazon), will also be required to adopt security measures and to report relevant incidents to the competent authorities. In addition to these provisions, the agreed draft rules entail the institution of strategic cooperation groups that will serve as platforms for exchange of information and best practices, and that will help Member States to shape national NIS strategies[228]. The NIS Directive represents a solid attempt at coordinating and enhancing cybersecurity capacity building at regional level through cooperation mechanisms; it will be fully effective once endorsed by the European Council and by the Parliament as a whole, which will most likely happen by the end of the year.

With regards to the second objective, the fight against cybercrime is implemented in the Strategy through the development of a common approach. The already mentioned Council of Europe's Convention on Cybercrime (also known as the Budapest Convention), is widely regarded as the most advanced legal framework in the field of cybercrime: for this reason, the Strategy aims at inducing every Member State to ratify the Convention by December 2015, so to update and harmonise national criminal legislation. Other specialised bodies of the Union are involved in the combating cybercrime: Europol (particularly EC3), Eurojust and ENISA. The role of the European Cybercrime Centre (EC3), established within Europol in 2013, is to tackle organized transnational cybercrime and to focus on attacks targeting critical networks

[227] 'First-ever EU-wide cyber-security rules backed by Internal Market Committee', European Parliament Press Release, 14 January 2016

[228] European Parliament, 2013/0027(COD) 'High common level of network and information security across the Union'

and infrastructure. It also represents the centre of EU cyber-intelligence: this institution connects national CERTs, law enforcement authorities and the private sector in the context of cross-border investigations and provides strategic background on emerging threats[229]. Internationally, the EC3 launched in 2014 the Joint Cybercrime Action Taskforce (J-CAT), that brings together specialised agencies from the United States and the United Kingdom and that is tasked with the response to transnational threats. Eurojust, the agency of the European Union that deals with judicial cooperation in criminal matters, has been increasingly involved in the cyber field, as the 2014 Annual Report highlights[230]. Specifically, Eurojust contributed to the institution of the European Cybercrime Task Force (EUCTF), created in 2010 and that serves as a platform for synchronization of EU action and information exchange between heads of national cybercrime units, Europol and the Commission. Overall, the Strategy emphasizes the importance of reducing cybercrime across the Union and of the creation of a EU-wide platform for coordination and harmonisation.

The third objective listed by the Strategy regards fortifying cyber defence in the EU, in particular referring to the Common Security and Defence Policy (CSDP). This specific point is to be considered independently, as it somewhat represents a separate issue from the previous two. In fact, while ensuring an "open, safe and secure cyberspace" is an important part of the CSDP, measures concerning cyber defence have been mostly conducted within single Member States, as national security is regarded as being outside the competences of the Union. Therefore, the implementation of common strategies at a wider EU level concerning cyber defence may meet greater reservations, as significant transfers of sovereignty would have to be agreed. Nevertheless, European institutions have recognised the security implications of cyberspace and its

[229] Cybersecurity in the European Union and Beyond, European Parliament, 2015

[230] Eurojust, Annual Report, 2014

inclusion in military doctrines: for this reason, the European Council adopted in 2014 the Cyber Defence Policy Framework. The main goal of the Framework is to harmonise cyber capabilities of Member States, addressing the existing gaps, along with cooperation within the EU as well as internationally. It sets out five priorities:

- Enhancing cyber defence capabilities of Member States related to CSDP;
- Improving the CSDP's communication networks resilience;
- Promoting civil-military cooperation within wider EU cyber policies;
- Implementing training, awareness and exercises;
- Strengthening international cooperation[231].

In the Strategy, the European Defence Agency (EDA) is indicated as the institution providing the operational support necessary for enhancing cyber capabilities of Member States. In recent years, the EDA has managed to expand its efforts in building national and EU capabilities, which were absent before 2012. Among these, the most relevant initiative undertaken by the EDA in the cyber defence field is the promotion of Cyber Europe in 2014, a crisis management exercise that managed to test the Member States' capabilities in responding to incidents[232]. Furthermore, the EDA provides Member States with research on technical requirements and with the development of detection systems. A stocktaking study on the cyber defence capabilities of EU institutions and Member States published in 2013 results in the finding that, despite the proactive role undertaken by the EDA, capability gaps between Member States remain a major disadvantage and that the EU take a more pronounced stance on cyber defence[233]. As it was mentioned previously, the

[231] EU Cyber Defence Policy Framework, Council of the European Union, 18 November 2014

[232] 'Biggest ever cyber security exercise in Europe today', European Commission press release, 27 December 2014

[233] Robinson, Neil, Agnieszka Walczak, Sophie-Charlotte Brune, Alain Esterle & Pablo Rodriguez, Stocktaking Study of military cyber defence capabilities in the European Union, RAND Corporation, 2013

reason why this issue is not addressed properly by the EU is the reluctance of Member States to transfer sovereignty on matters concerning national security on one hand, and the limited competences of the CSDP on the other. Due to the limits of competence in CSDP, Member States rather tend to cooperate with NATO. Moreover, the traditional approach characterizing defence policies in the EU may be unsuitable in the context of threats deriving from cyberspace; only future implementation of the CSDP and stronger commitments by Member States will overcome these limitations in order to address properly cyber defence policies and capacity building.

The fifth objective listed by the Strategy calls for the creation of a cohesive EU cybersecurity policy, to be promoted internationally and shaped along core European values. The EU is fully involved in the global debate surrounding internet governance, security of ICTs and international law applicable to cyberspace, and engages in several 'cyber' dialogues with key international players. The Strategy's suggestion to strengthen cooperation with third countries was put into action by the European Council through the adoption of the 'Conclusions on Cyber Diplomacy'. The document indicates five policies that are to be developed and promoted by the Union internationally[234]. The first priority listed by the document is the protection of the digital economy. Economic diplomacy is on top of the EU's cyber agenda: the internet's impact on growth and innovation has urged the EU to focus on economic development based on ICTs promoting the Digital Single Market on one hand and to secure its network resilience through the NIS Directive on the other; furthermore, the EU has already accomplished steps forward in the fields of privacy and data protection, so the application of its regulatory framework to cyberspace appears as a natural consequence. The second priority is the reduction of cybercrime. As it was previously mentioned, the Council of Europe has

[234] Council of the European Union, Council Conclusions on Cyber Diplomacy, 11 February 2015

pioneered international cooperation on the fight against cybercrime with the promotion of the Budapest Convention, and the EU's priority in this field is to promote the Convention globally and to persuade international partners to converge to the legal standards enshrined in the Convention. Moreover, talks on cybercrime are part of most of the cyber talks initiated by the EU with its partners, and cooperation programs are also sustained in venues other than European ones (regional organizations and international forums). Security implications of cyberspace are also included in the European cyber diplomacy agenda. The EU stands for the application of existing international law and for the development of norms for responsible behaviour in cyberspace: in this context, the EU supports the legal and behavioural framework provided by the United Nation's Governmental Group of Experts on developments in the field of Information and Telecommunications in the context of international security (GGE) on the norms of international law applicable to cyberspace, and seeks to promote it to its partners. Moreover, the EU played a key role in the definition of Confidence Building Measures (CBMs) for cyberspace within OCSE, and supports similar attempts in regional organizations such as the ASEAN Regional Forum. Peculiar to the European Union's core values is the protection of human rights online. The European Council has adopted in this regard an important document entitled 'EU Guidelines on Freedom of Expression online and offline', where it is stated that the EU should include human rights protection in its external action in particular referring to their dimension on the internet; further, the Guidelines call for ensuring universal access to the internet, especially in developing countries, and for impeding the spread of technologies that would allow governments to implement restrictive measures online such as censorship and surveillance[235]. Internet governance is therefore linked to these issues: the EU endorses the current multi-

[235] Council of the European Union, EU Human Rights Guidelines on Freedom of Expression online and offline, Foreign Affairs Council Meeting, Brussels 12 May 2014

stakeholder framework and seeks to mitigate the proposals set forth by some countries to increase governmental supervision. The fifth and last objective regards capacity building. Cyber capacity building is perceived strategically in the EU cyber diplomacy agenda, and for this reason the Council's Conclusion indicates it as representing the ultimate tool for the development of a free, open and secure internet: in this perspective, the EU is pushed to enhance capabilities worldwide through the implementation of cooperation measures concerning the fight against cybercrime and the strengthening of networks resilience.

The European cyber diplomacy is shaped along the above mentioned priorities, and has managed to create spaces with strategic international players where cyber issues are discussed and negotiated.

The European Union's cyber dialogues with third countries

In order to follow the Strategy's provision on establishing a coherent international cybersecurity policy, the EU engages in dialogues with third countries where cyber issues are the core subject of discussion and negotiations. Special initiatives, directed at enhancing cyber dialogues, were launched with China, India, Japan, South Korea, Brazil and the United States. The dialogues are mostly managed by the European External Action Service (EEAS) and by other bodies of the European Commission, in coordination with the Interparliamentary Delegations of the European Parliament.

The EU collaborates with **China** on cyber issues through the EU-China Taskforce, established with the bilateral meeting of February 2012 held in Beijing[236]. China is a controversial actor in the cyber domain, mostly for its restrictive policies towards national networks and on civil liberties online, and is often blamed by foreign governments of sponsoring network intrusions and

[236] Council of the European Union, Joint Press Communiqué of the 14th EU-China Summit, 14 February 2012

of favouring corporate data theft through cyber espionage; in this context the two partners, despite sharing the understanding that an open and secure internet is fundamental for economic growth, have contrasting views on several matters. First of all, with regards to cybercrime, China does not support the Budapest Convention's framework for law enforcement cooperation, and rather seeks to create legal instruments within the United Nations. Secondly, with regards to the behavioural norms to be followed in cyberspace and the applicability of international law, the EU and China fail to find consensus. While the former supports the applicability of the UN charter of international humanitarian law, the latter is keen on preserving governmental control over cyberspace, and therefore highlights the application of principles of public international law such as State sovereignty, non-interference and non-use of force. Increased governmental control is also implied in the Chinese stance on internet governance: while China formally supports the multi-stakeholder model, at the same time seeks to influence the regulatory framework of the internet emphasizing the role of States, as testified by the voting at the 2012 World Conference on Information and Telecommunications in Dubai. Diverging views also regard State behaviour in cyberspace. In this context, China has put forward a proposal on behavioural norms in cyberspace entitled 'Code of Conduct for Information Security' within the Shanghai Cooperation Organisation[237]. The EU has welcomed the proposal with suspicion and is following it closely, as its adoption would entail an increased role for governments in cyberspace and a negative impact on human rights. In fact, China's attitude towards privacy and human rights represents the main obstacle in the EU-China cooperation on cyber issues.

The seventh EU-**Brazil** summit established an EU-Brazil Dialogue on

[237] Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General, UN Doc A/69/723, 13 January 2015

International Cyber Policy, where the two partners discuss, among other things, on regulatory and security standards, ICT cooperation and exchange views on policies related to cyberspace[238]. Brazil has been particularly active in the field of internet governance, and its stance on the matter coincide with the multi-stakeholder vision promoted by the EU. Brazil's former president Dilma Rousseff, in the wake of the Snowden revelations of the NSA mass surveillance program, openly expressed her concern for the impact on civil liberties and referred to the NSA's activities as a violation of international law[239]. Moreover, she called upon the international community to develop a civilian multilateral framework for internet governance. For this reason, Brazil hosted in 2014 the Global Multi-Stakeholder Meeting on the Future Internet Governance (NETMundial), which enabled Brazil to promote its own principles on internet governance and that resulted in a Statement that set out general principles for internet governance along with more pressing issues like the institutionalization of ICANN[240]. While the Global Meeting testified the existence of divergences (Russia and India did not sign the statement), it managed to create closer cooperation between the EU and Brazil on the issue of internet governance. The two partners' strategic interests in the field of ICTs also have an economic aspect: an undersea fibre-optic cable linking Latin America with Europe is currently being developed, and would serve as a direct communication channel between the two continents without passing through the United States, as it has been the case since now. With this project, the EU and Brazil wish to cut costs and to boost the growing data flow between the two regions; moreover, it will manage to make the connection more secure and

[238] Council of the European Union, Joint Statement of the 7th EU-Brazil Summit, Brussels 24 February 2014

[239] General Assembly of the United Nations, Statement Summary of President Dilma Russeff, 68th Session, 24 September 2013 (gadebate.un.org)

[240] NETmundial multistakeholder statement, 24 April 2014 (netmundial.br)

more resilient against cyber espionage[241]. **India** became involved in a cyber dialogue with the EU after the EU-India summit of 2010, where a EU-India Cyber Dialogue was established[242]. As India bases its economic growth on innovation and on technological research, the cyber dialogue between the two partners has mostly revolved around security standards and capacity building through exchange of expertise and of best practices. In addition to that, the EU and India discuss cybercrime as well. Given the importance regarded by India on resilience against cyberattacks for economic reasons, the Indian government has increasingly expanded its presence on cyberspace and consequently civil liberties have suffered. For this reason, the EU wishes to include India in the Budapest Convention, despite India claiming that the Convention does not support the positions of developing countries[243]. With regards to internet governance, India's stance is formally for increased governmental control, but the shiftiness of its position on the matter, as witnessed in several fora, has the potential to be rearranged by the European partners[244].

The EU finds consensus with **Japan** on most cyber issues: Japan was the first among the other Asian country to ratify the Budapest Convention, and supports the European views on internet governance and on the applicability of international law. The EU-Japan Cyber Dialogue was established in 2014 within the 22nd EU-Japan Summit and is mostly focused on exchange of information and of best practice for capacity building and increased resilience

[241] Nancy Scola, 'Brazil Begins laying its own Internet cables to avoid U.S. surveillance', The Washington Post (online article), 3 November 2014

[242] The most recent round of the EU-India cyber dialogue took place in May 2015 (EEAS Press Release, 22 May 2015)

[243] Pratap Vikram Singh, 'India won't sign Budapest pact on cyber security', Governance Now (online article), 15 October 2013

[244] India is defined as a 'swing state' by the CIGI report on the voting during the WCIT-12 (Tim Mauer and Robert Morgus, *Tipping the Scale: An Analysis of Global Swing States in the Internet Governance Debate*, 2014)

sharing security standards[245]. The EU and Japan collaborate further in the development of CBMs for cyberspace within ASEAN. Similarly, the cyber dialogue with **South Korea** is particularly fruitful as the Asian country is one of the most networked economies in the world and detains a considerable amount of internet users. Cooperation between the two partners, besides focusing on a number issues ranging from international security, best practice exchange and capacity building, has a strategic aspect as well. South Korea is increasingly targeted by cyberattacks originating from North Korea: in March 2013, cyberattacks hit television stations and banking systems[246] while in December 2014 the IT systems of a nuclear facility were affected by orchestrated malware[247]. For this reason, the latest round of the EU-South Korea Cyber Dialogue in 2015 included exchange of intelligence on the hacking incidents that involved the South Korean nuclear plant and Sony Pictures Entertainment[248].

Being the **United States** one of the key players in cybersecurity, the EU maintains special cooperative channels with the US on cyber issues. The EU-US Working Group on Cybersecurity was established in 2010, and was recently implemented in the aftermath of the bilateral summit of 2014[249]. The US approach to cybersecurity is again a controversial one: it comprises both diplomatic and military measures, and the inclusion of cyber issues into the national security agenda has led the United States to address cyber threats in any way was found appropriate. For example, in 2015 President Obama authorised an order according to which the Treasury Department was allowed

[245] Memo from the European Commission, *EU-Japan relations and the 22nd EU-Japan Summit*, Brussels, 7 May 2014

[246] In-Soo Nam and Alastair Gale, ‘Seoul Investigates Web Shutdown’, The Wall Street Journal (online article), 20 March 2013

[247] Ju-Min Park and Meeyoung Cho, ‘South Korea blames North Korea for December hack on nuclear operator’, Reuters.com, 17 March 2015

[248] Republic of Korea, Ministry of Foreign Affairs Press Release, 30 April 2015

[249] Memo from the European Commission, EU-US Summit (Brussels, 26 March 2014) and EU-US relations, 24 March 2014

to use economic sanctions against companies that engage in cyberattacks resulting in threatening national security and economic and financial stability[250]; always in 2015, the Department of Defense-proposed Defense Cyber Strategy (DCS) laid out the foundations for a 'preventive cyber-offensive doctrine', according to which the President would be enabled to respond to cyberattacks deploying military forces, in the face of an ongoing or imminent threat deriving from cyberspace[251]. The United States are greatly involved in the military aspects of cyberspace, but the cyber diplomatic cooperation with the EU has a more political angle. Both actors are aligned on most cyber issues, including support to the UN GGE view that international law is applicable to cyberspace, to the multi-stakeholder model of internet governance and capacity building. Furthermore, the EU and the US collaborate in the elaboration of CBMs and behavioural norms for cyberspace: in particular, during the latest reunion of the UN GGE, the United States have submitted a set of peacetime norms ('rules of the road')[252] for the preservation of stability in cyberspace, which are widely supported by its Western allies, especially Member States of the EU. These include: refraining from supporting cyberattacks that could potentially damage or impair national critical infrastructure; abstaining from interfering with national emergency responders (namely CERTs) through cyberattacks; and implementing cooperation with foreign law enforcement authorities for cybercrime investigations. A fourth norm was excluded from the submission as it does not deal with security but with trade instead: according to this norm, that the United States pledged to abide, States should refrain from engaging in cyber

[250] Nathan Vardi, 'From Iran To Russia And Now Hackers, Sanctions Have Become America's Weapon Of Choice', Forbes (online article), 1 April 2015

[251] Denise E. Zheng, '2015 DOD Cyber Strategy', Center for Strategic and International Studies (CSIS), 24 April 2015

[252] Joseph Marks, 'U.S. makes new push for global rules in cyberspace', Politico.com, 5 May 2015

espionage that damages a foreign economy and that benefits their own.

Discussion and Conclusions

The analysis operated heretofore was directed at underscoring how cyberspace represents one of the most challenging and thought-provoking dimensions of today's international affairs and more broadly, of modernity. The penetration of the virtual world onto the physical one, besides affecting the way in which societies and economies develop and interact with one another, creates new and urging concerns for governments all over the world. Despite the uneven distribution of internet in the world, estimates account that by 2020 there will be 16 billion connected devices thanks to the rise of the 'Internet of Things'[253]. In the light of this, it is likely that States will engage more and more actively in the cyber domain and adapt their national and international performance to the virtual dimension, as a response to the increasing tensions between globalizing tendencies and sovereignty. Castells for example suggests that, if States wish to remain relevant in the future, they must organize themselves into 'network States'[254]. For the time being however, States seem to find themselves torn between two different attitudes towards cyberspace: on one hand, the rising increase in international debates on cybersecurity and related national strategies testify the widespread sense of urgency and concern with regards to the cyber domain, while on the other States, as much as societies, fail to comprehend the extension of the transformations generated by technological progress, that can potentially result damaging if exploited with the wrong intentions. On a broader level, the historical processes of globalization that have deeply affected demography, global production and societal identities, have also managed to redefine the patterns of international security in the 21st century: along with the perceived

[253] '16bn Devices Online by 2020, Says Report', Telegraph (online article), 30 October 2010

[254] Manuel Castells, *Communication Power*, Oxford University Press, 2009

erosion of sovereignty, the global distribution of power is shifting in favour of small groups and destabilizing actors in the international community. In this context, the strategic dimension of cyberspace and its insertion into contemporary inter-State conflicts acquires great relevance, and some recent developments contribute in validating this assertion.

Some States' attitude in cyberspace is growingly being perceived as threatening, especially by the United States. China and Russia in particular are being indicated as the entities that engage more intrusively in cyberspace. This is due to a conflicting dynamic regarding mainly internet governance and the economic and strategic advantages originated from the internet, that nowadays see the United States as the favoured entity. US corporations and hi-tech firms dominate the virtual market, providing with enormous revenues for the commercial capitalization of internet-based activities; moreover, this results in the prevalence of US cybersecurity products and standards at international level. Since the mid-90s, Russia and China have been challenging the American dominance in this field by proposing different perspectives on internet oversight and on the principles of public international law that would drive State conduct in cyberspace[255]. This struggle for informational dominance results in increasing tensions and incidents. Most recently, Hans-Georg Maaßen, who is the head of the Federal Office for the Protection of the Constitution (Germany's security agency) has blamed Russia of conducting widespread "operations for espionage and sabotage" targeting, among the others, the lower house of the German Parliament[256]. These operations also include attacks against NATO, US military and governmental networks, as well as Ukrainian and Russian activists. According to the same source, Russian hackers are being instructed by authorities and engaging in cyberattacks that

[255] Scott L. Malcomson, 'The open, universal internet is over. But did it ever really exist?', The Guardian (online article), 3 April 2016

[256] Agence France-Presse in Berlin, 'Russia accused of series of international cyber-attacks', The Guardian (online article), 13 May 2016

in the past year have hit the French TV station TV5Monde, sending jihadi propaganda messages on the station's website and social network accounts, and also the Dutch Safety Board's computer systems, in order to access sensitive documents containing the final report on the MH17 flight shooting that took place in the skies over Eastern Ukraine in the summer of 2014. Most recently, Russian hackers are also suspected of compromising the automated controlling systems of a Ukrainian electricity power grid station that led to extended black-outs in the Eastern region of the country leaving up to 80,000 people with the power cut[257]. Ukrainian authorities were quick to attribute the attacks to the Russians, considering especially the turbulent relationship between the two countries due to the conflicts taking place in Crimea and Eastern Ukraine. The event has also led Former National Security Agency chief Gen. Michael Hayden to affirm that the cyberattacks against the Ukrainian power grid are manifestations of a trend that can potentially affect the United States as well, identifying Russia and North Korea as the entities that are most likely to engage in such operations against American infrastructure[258]. Not all threats however generate from States deemed as 'destabilizing': the United States for example, despite accusing China of conducting extensive espionage and of stealing corporate data and intellectual property from US firms, is engaging in cyber espionage just as much as China or any other country is[259].

As defined in the cybersecurity terminology, the 'threat landscape' characterizing cyberspace poses unprecedented challenges for national and international security. Computer-based attacks on physical infrastructure represent at this stage the most relevant threat to modern societies. In this context, their highly networked connotation can therefore be considered an

[257] Kim Zetter, 'Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid', Wired (online article), 3 March 2016

[258] Paul F. Roberts, 'Ex-spy chief: Ukrainian cyberattack a warning sign for US utilities', The Christian Science Monitor (online article), 12 January 2016

[259] Associated Press in Beijing, 'China demands halt to 'unscrupulous' US cyber-spying', The Guardian (online article), 27 May 2014

advantage and a vulnerability at the same time. For this reason, international efforts to regulate State-conduct in cyberspace must be put in place. But as this thesis pointed out, the strategic developments in the cyber domain are only being tested and additional potentialities can result from the ceaseless technological progress that has characterized the 21st century.

Currently, the discussion over cybersecurity seems to be driven by two opposite attitudes: on one hand, there are some who see the ‘cyber’ feature of international affairs as the most pressing issue concerning modern warfare and national security, while on the other there are those who consider cyberspace as an additional dimension where human interactions take place, and that the nature of such interactions isn’t fundamentally changed. The approach that was chosen for this thesis situates itself in a somewhat halfway position: while the current situation does not lean towards one position or the other, it should appear clear from the analysis conducted heretofore that the potential for a destabilizing effect generating from the cyber domain is definitely there. Inter-State conflicts originating from incidents and confrontations taking place in cyberspace, in addition to the tensions deriving from the power diffusion in favour of smaller actors could escalate uncontrollably and destabilize not only the international system as a whole, but also historically established practices among States. If State conduct were to remain unregulated, the prevailing situation would be one in which the resort to armed force is easier and with less constraints. Narrowing power differentials between States and non-State actors will also contribute to the increase in instances of hybrid warfare and of sporadic confrontations. For this reason, governments must come to understand the implications of cyberspace as the upcoming strategic context, and realize that the penetration of the virtual world into real one has made it so that actions undertaken in one of the domains has necessarily immediate consequences on the other.

Bibliography

Agence France-Presse. (2016, May 13). *Russia accused of series of international cyber-attacks.* Tratto da The Guardian: https://www.theguardian.com/technology/2016/may/13/russia-accused-international-cyber-attacks-apt-28-sofacy-sandworm

Arthur, C. (2011, February 7). *Anonymous attacks US security company.* Tratto da The Guardian: https://www.theguardian.com/technology/2011/feb/07/anonymous-attacks-us-security-company-hbgary

Associated Press. (2013, October 27). *Haifa Tunnel Paralyzed by Cyberattack, Expert Reveals.* Tratto da Haaretz: http://www.haaretz.com/israel-news/1.554729

Bakowski, P. (2013). *Cyber Security in the European Union.* European Parliament Research Service, European Parliament.

Bennett, R. (2012). *The gathering storm: WCIT and the global regulation of the internet.* The Information Technology & Innovation Foundation.

Bradley, G. (2005, August 25). *Hackers Attack via Chinese Web Sites.* Tratto da The Washington Post: http://www.washingtonpost.com/wp-dyn/content/article/2005/08/24/AR2005082402318.html

Case Concerning Military and Paramilitary Activities In and Against Nicaragua (Nicaragua v. United States of America), case no. 70 (International Court of Justice June 27, 1986).

Castells, M. (2009). *Communication Power.* London: Oxford University Press.

Cirlig, C.-C. (2014). *Cyber Defence in the EU: Preparing for Cyber Warfare?* European Parliament Research Service (EPRS), European Parliament.

Clarke, R. A., & Knake, R. K. (2010). *Cyber War: The Next Threat to National Security and What To Do About It.* New York: HarperCollins Publishers.

Clausewitz, C. V. (1989). *On War (Reprint ed.).* Princeton University Press.

Collins, A. (2013). *Contemporary Security Studies.* Oxford, United Kingdom: Oxford University Press.

Corfu Channel Case (United Kingdom v. Albania); Assessment of Compensation (International Court of Justice December 15, 1949).

Council of Europe. (2001). *Convention on Cybercrime.* Budapest.

David J. Betz, T. S. (2011). *Cyberspace and the State: Toward a Strategy for Cyber-Power.* London: The International Institute for Strategic Studies.

Farrell, M. B. (2009, December 18). *Iranian Cyber Army Hack of Twitter Signals Cyberpolitics Era.* Tratto da The Christian Science Monitor: http://www.csmonitor.com/USA/2009/1218/Iranian-Cyber-Army-hack-of-Twitter-signals-cyber-politics-era

Government of the United Kingdom. (2010). *A Strong Britain in an Age of Uncertainty: The National Security Strategy.* London: The Stationery Office.

Guéhenno, J.-M. (1995). *The End of the Nation-State.* Minneapolis: University of Minnesota Press.

Harknett, R. J. (1996). *Information Warfare and Deterrence.* Parameters.

Hern, A. (2016, January 7). *Ukrainian blackout caused by hackers that attacked media company, researchers say.* Tratto da The Guardian: https://www.theguardian.com/technology/2016/jan/07/ukrainian-blackout-hackers-attacked-media-company

International Law Commission. (2001). *Draft Articles on Responsibility of States for Internationally Wrongful Acts.*

Klimburg, A. (2011). *Mobilising Cyber Power.* International Institute of Strategic Studies.

Kramer, F., Starr, S., & Wentz, L. (2009). *Cyberpower and National Security.* National Defense University.

Krasner, S. (2009). *Power, the State and Sovereignty: Essays on International Relations.* Abingdon: Routledge.

Krekel, Bakos, & Barnett. (2009). *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation.* Northrop Grumman Corporation.

Kremer, J.-F., & Müller, B. (2014). *Cyberspace and International Relations: Theory, Prospects and Challenges.* Bonn: Springer.

Libicki, M. (2009). *Cyberdeterrence and Cyberwar.* Santa Monica: RAND Corporation.

Malcomson, S. L. (2016, April 3). *The open, universal internet is over. But did it ever really exist?* Tratto da The Guardian: http://www.theguardian.com/commentisfree/2016/apr/03/internet-web-politics-money-freedom-state

Marks, J. (2015, May 5). *U.S. makes new push for global rules in cyberspace.* Tratto da Politico: http://www.politico.com/story/2015/05/us-makes-new-push-for-global-rules-in-cyberspace-117632

Mauer, T., & Morgus, R. (2014). *Tipping the Scale: An Analysis on Global Swing States in the Internet Governance Debate.* Center for International Governance & Innovation (CIGI).

NATO Cooperative Cyber Defence Centre of Excellence. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare.* Cambridge University Press.

Nye, J. S. (2004). *Soft Power: The means to success in world politics.* New York: Public Affairs.

Nye, J. S. (2010). *Cyber Power.* Harvard Kennedy School: Belfer Center for Science and International Affairs.

Nye, J. S. (2011). *Nuclear Lessons for Cybersecurity?* Strategic Studies Quarterly.

Nye, J. S. (2011). *The Future of Power.* Harvard Kennedy School: Belfer Center for Science and International Affairs.

Park, J.-M., & Cho, M. (2015, March 17). *South Korea blames North Korea for December hack on Nuclear Operator.* Tratto da Reuters.

Paul, V. (2006). *Speed and Politics: An Essay on Dromology.* Los Angeles, CA: Semiotext(e).

Pawlak, P. (2015). *Cybersecurity and Cyberdefence: EU Solidarity and Mutual Defence Clauses.* Brussels: European Parliament Research Service (EPRS), European Parliament.

Policy Department for Citizens' Rights and Constitutional Affairs. (2015). *Cybersecurity in the European Union and Beyond: Exploring the Threats and Policy Responses.* Brussels: European Parliament.

Renard, T. (2014). *The rise of cyber-diplomacy: the EU, its strategic partners and cyber-security.* European Strategic Partnership Observatory (ESPO).

Roberts, D. (2015, September 16). *Obama warns of 'weaponising the internet' ahead of Xi Jinping's US visit.* Tratto da The Guardian: https://www.theguardian.com/technology/2015/sep/16/obama-china-cybersecurity-weaponise-the-internet-xi-jinping-visit

Roberts, D. (2015, September 25). *US and China back off internet arms race but Obama leaves sanctions on the table.* Tratto da The Guardian: http://www.theguardian.com/us-news/2015/sep/25/us-china-cyber-security-obama-xi-jinping-inconclusive-summit

Roberts, P. F. (2016, January 12). *Ex-spy chief: Ukrainian cyberattack a warning sign for US utilities.* Tratto da The Christian Science Monitor: http://www.csmonitor.com/World/Passcode/2016/0112/Ex-spy-chief-Ukrainian-cyberattack-a-warning-sign-for-US-utilities

Sanger, D. E. (2009, January 10). *U.S. Rejected Aid for Israeli Raid on Iranian Nuclear Site.* Tratto da The New York Times: http://www.nytimes.com/2009/01/11/washington/11iran.html

Sanger, D. E. (2012). *Confront and Conceal. Obama's Secret Wars and Surprising Use of American Power.* Crown Publishers.

Sassen, S. (1996). *Losing Control? Sovereignty in an Age of Globalization.* New York: Columbia University Press.

Savage, L. C. (2010, December 13). *Julian Assange: The Man Who Exposed The World.* Tratto da Macleans: http://www.macleans.ca/society/technology/a-man-of-many-secrets/

Smith, R. (2005). *The Utility of Force.* London: Allen Lane.

The European Commission. (2013). *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace.*

The SecDev Group. (2009). *Tracking GhostNet: Investigating a Cyber Espionage Network.* InfoWar Monitor Report.

Traynor, I. (2007, May 17). *Russia accused of unleashing cyberwar to disable Estonia.* Tratto da The Guardian: https://www.theguardian.com/world/2007/may/17/topstories3.russia

United Nations. (1945). *Charter of the United Nations.*

United Nations General Assembly. (2013). *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunication technologies in the Context of International Security.* United Nations.

US Department of Defense. (2011). *Strategy for Operating in Cyberspace.*

Vardi, N. (2015, April 1). *From Iran To Russia And Now Hackers, Sanctions Have Become America's Weapon Of Choice.* Tratto da Forbes: http://www.forbes.com/sites/nathanvardi/2015/04/01/from-iran-to-russia-and-now-hackers-sanctions-have-become-americas-weapon-of-choice/#50f506f47921

White House. (2011). *International Strategy for Cyberspace: Prosperity, Security and Openness in a Networked World .* White House.

Zetter, K. (2014, March 11). *An Unprecedented Look At Stuxnet, The World's First Digital Weapon.* Tratto da Wired: https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/

Zetter, K. (2016, March 3). *Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid.* Tratto da Wired: https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/

Zheng, D. E. (2015, April 24). *2015 DOD Cyber Strategy.* Tratto da Center for Strategic and International Studies (CSIS): https://www.csis.org/analysis/2015-dod-cyber-strategy

Ziolkowski, K. (. (2013). *Peacetime Regime for State activities in cyberspace. International Law, International Relations and Diplomacy.* Tallinn: CCD COE Publications.