

**T.C.
GALATASARAY UNIVERSITY
INSTITUTE OF SOCIAL SCIENCES
DEPARTMENT OF PUBLIC LAW**

**CONFRONTING ECONOMIC AND INDUSTRIAL CYBERESPIONAGE
UNDER INTERNATIONAL LAW**



LL.M THESIS

Oğuz Kaan PEHLİVAN

**Thesis Supervisor:
Prof. Dr. Akif Emre ÖKTEM**

December 2016

T.C.
GALATASARAY UNIVERSITY
INSTITUTE OF SOCIAL SCIENCES
DEPARTMENT OF PUBLIC LAW

**CONFRONTING ECONOMIC AND INDUSTRIAL CYBERESPIONAGE
UNDER INTERNATIONAL LAW**



LL.M THESIS

Oğuz Kaan PEHLİVAN

Thesis Supervisor:
Prof. Dr. Akif Emre ÖKTEM

December 2016

FOREWORD

I would like to express my heart-felt thanks and gratitude to my supervisor Prof. Dr. Akif Emre ÖKTEM for his invaluable guidance. Additonally I would like to present my special thanks to Asst. Prof. Mehmet KARLI and Asst. Prof. Zeynep PİRİM for their valuable feedbacks. I have been amazingly fortunate to have such an advisor who gave me the freedom to explore on my own. I am deeply grateful for his encouragement that helped me sort out the legal details of my work. I would like to thank to Amy Hume for her efforts. I am indebted to my friends for their continuous assistance and feedbacks, but also the institutions that covered my expenses to attend conferences and courses in the Washington D.C., London, Paris and Kiev.

Most importantly, none of this would have been possible without the support and patience of my family.

CONTENTS

FOREWORD	I
ABBREVIATIONS	V
TABLES & CASES	VIII
RESUMÉ	X
ABSTRACT	XIV
ÖZET	XVIII
INTRODUCTION	1

Chapter One CYBERSPACE, ESPIONAGE AND CYBERESPIONAGE

A. Regulating Cyberspace and Espionage	8
1. Challenges Inherent to Regulating Cyberspace	8
a) Defining Cyberspace	8
b) Regulating Cyberspace	10
2. Regulating Espionage	13
a) Legality of Wartime Espionage Activities	14
b) Legality of Peacetime Espionage Activities	17
(1) Customary International Law and Espionage	18
(2) Principles of International Law and Espionage	20
B. Cyberespionage and Changing Features of Espionage	24
1. Defining Cyberespionage	24
2. Changing Features of Espionage	26
a) New Purpose and Targets	27
b) New Methods and Means	29
c) New Actors and Incidents	33
(1) Actors and Incidents Relating to China	34
(2) Actors and Incidents Relating USA	38
(3) Attribution Problem	41
C. Evaluation of Cyberespionage under International Legal Theory	43
D. Concluding Remarks	46

Chapter Two
TACKLING ECONOMIC AND INDUSTRIAL CYBERESPIONAGE

A. Legal Responses to Economic and Industrial Cyberespionage.....	49
1. Domestic Legal Responses	49
a) Turkish Legal System	51
(1) Protection of Trade Secrets	51
(a) Civil Remedies.....	53
(b) Criminal Remedies	55
(2) Cyber Crimes.....	56
(a) Unauthorized Access	56
(b) Illegal Interception of Data and Systems.....	58
b) American Legal System	60
(1) Economic and Industrial Espionage	61
(2) Theft of a Trade Secret	63
(3) Computer Fraud.....	67
2. Regional Legal Responses	72
a) European Trade Secret Protection.....	72
b) European Cybercrime Protection	77
(1) European Convention on Cybercrime	78
(2) EU Directive 2016/943 on Attacks against Information Systems....	80
3. International Legal Responses	84
a) Cyberespionage during Wartime.....	84
b) Cyberespionage during Peacetime	85
(1) Prohibition on Use of Force	86
(2) Internationally Wrongful Act	90
(a) Countermeasures against Cyberespionage.....	94
(b) Retorsion against Cyberespionage.....	95
(c) Legal Rationale	96
(3) International Treaty Law and Cyberespionage	97
(a) Violation of Good Faith Principle	99
(b) Invalidity of Treaty by Fraud.....	102

(4) WTO Dispute Settlement Mechanism.....	105
E. Concluding Remarks	110
CONCLUSION.....	114
BIBLIOGRAPHY	117
CURRICULUM VITAE.....	129



ABBREVIATIONS

AFCEA	: Armed Forces Communication and Electronics Association
AFDIA	: Annuaire Français de Droit International Année
ANSSI	: Agence Nationale de la Sécurité des Systèmes d'Information
APT	: Advance Persistent Threat
ASD	: Australian Signals Directorate
ASIO	: Australian Security Intelligence Organization
ASIS	: Australian Secret Intelligence Service
ASIL	: American Society of International Law
ASEAN	: Association of Southeast Asian Nations
AYIL	: Australian Yearbook of International Law
COMINT	: Communication Intelligence
CNO	: Computer Network Operations
CCDCOE	: NATO Cooperative Cyber Defense Committee of Excellence
CERT	: Cyber Emergency Response Team
CNA	: Computer Network Attack
CND	: Computer Network Defense
CNE	: Computer Network Exploitation
CSEC	: Communications Security Establishment Canada
CMAT	: Certain Maritime Arrangements in the Timor Sea
DJILP	: Denver Journal of International Law and Policy
DDoS	: Distributed Denial of Service
EJIL	: European Journal of International Law
EU	: European Union
FISA	: Foreign Intelligence Surveillance Act

GCHQ	: UK Government Communications Headquarters
GCSB	: Government Communications Security Bureau
GJICLR	: Georgia Journal of International and Comparative Law Review
HILJ	: Harvard International Law Journal
HUMINT	: Human Intelligence
HPCR	: Harvard Program on Humanitarian Policy and Conflict Research
ICJ	: International Court of Justice
IP Address	: Internet Protocol Address
IP Rights	: Intellectual Property Rights
ILC	: International Law Commissions
ICLQ	: International and Comparative Law Quarterly
JIPLP	: Journal of Intellectual Property Law and Practice
MJIL	: Michigan Journal of International Law
NIST	: National Institute of Standards and Technology
NSA	: US National Security Agency
NGO	: Non-Governmental Organization
par.	: Paragraph
PCA	: Permanent Court of Arbitration
PCIJ	: Permanent Court of International Justice
PLC	: Programmable Logic Controllers
PLA	: Chinese People's Liberation Army
RUSI	: Royal United Services Institute
SIGINT	: Signal Intelligence
SCADA	: Supervisory Control and Data Acquisition
SANS	: Escal Institute of Advanced Technologies
SOE	: State-Owned Enterprises
TPC	: Turkish Penal Code with n. 5271
TCC	: Turkish Commercial Code with n. 6102
TRIPS	: Trade-Related Aspects of Intellectual Property Rights
USA/US	: United States of America

USCC	: U.S. - CHINA Economic and Security Review Commission
US DOD	: United State Department of Defense
UN	: United Nations
UNDP	: United Nations Development Program
UKUSA	: United Kingdom - United States of America Agreement
UNTS	: United Nation Treaty Series
UTSA	: Uniform Trade Secrets Act
YILC	: Yearbook of the International Law Commission
VCLT	: Vienna Convention on the Law of Treaties
VJIL	: Virginia Journal of International Law
WTO	: World Trade Organization
WWW	: World Wide Web

TABLES & CASES

TABLES

Table I-1: China-Based APT Group's Targeting of Strategic Emerging Industries	28
Table I-2: Economic and Industrial Cyberespionage Circle	29
Table I-3: Top Trending Cyberespionage Actors in 2016	34
Table I-4: Publicly Reported Cyberespionage Activities Attributed to China.....	36
Table I-5: Strategies of Stronger and Weaker Parties	44
Table II-1: Comparison of Traditional Espionage and Cyberespionage.....	111
Table II-2: Regulation of Wartime Cyber/Espionage	112
Table II-3: Regulation of Peacetime Cyber/Espionage.....	112

CASES

Advisory Opinion on Legality of the Threat or Use of Nuclear Weapons, (1996).....	91
Anglo-Iranian Oil Co. Case (United Kingdom v Iran) (Preliminary Objection) (1951).....	101
Case Concerning The Continental Shelf (Libyan Arab Jamahiriya vs Malta) (1985).....	19
Corfu Channel, Merits, (Judgment),(1949).....	93
E. I Du Pont de Nemours & Company vs. Rolfe Christopher 28254 5th Cir. (1970).....	67
Fisheries Jurisdiction Case (United Kingdom v Iceland) (Merits) (1974).....	103
Gabcikovo-Nagymaros Project (Hungary vs Slovakia) (1997)	103
ICJ, (Timor-Leste v. Australia) (Application) (2013).....	100
ICJ, (Timor-Leste v. Australia) (Judgement) (2013)	100
Lansig Linde Ltd. vs. Kerr (1991)	66
Mars UK Ltd. vs. Technowledge Ltd (1999).....	67
Military and Paramilitary Activities in and Against Nicaragua (Nicaragua vs. US) (1986)..	19
North Sea Continental Shelf Case (Germany v. Denmark; Netherland) (1969).....	19
Nuclear Tests Case (Australia v France) (Merits) (1974)	102
PCIJ., Phosphates in Morocco, (Judgment), (1938).....	93
PCA, Timor-Leste v. Australia, 2013-16 (2013)	99

IX

Rainbow Warrior (New Zealand v France) (1990)	93
Sheridan v. Mallinckrodt, Inc., 568 F. Supp. 1347 (1983)	67
The Barcelona Traction (Belgium v. Spain) (1970).....	93
The Case of the S.S. Lotus, Series A. No. 70, (1927).....	18
United States v. Michael J. Oberhard, No. 89-1503 7th Cir. (1989).....	67
United States v. Caesar Bottone, Seymour Salb, Nathan Sharff, 365 F.2d 389 (1966).....	67
United States v. Aleynikov, No. 11-1126 2d Cir. (2012)	68
United States v. Stegora, 849 F.2d 291, 292 (1988)	67
United States v. Wang Dong, and Others (2014).....	65



RESUMÉ

Cette étude s'inscrit dans une dynamique de discussion en sciences sociales, sur une des questions difficiles de la cybersécurité en particulier, le cyber-espionnage ainsi que des réponses juridiques appropriées qui pourraient être adoptées par les États victimes. Le but de cette étude est d'étudier et d'identifier le cyber-espionnage économique et industriel et d'offrir et d'analyser des réponses juridiques nationales et internationales efficaces.

Tout d'abord, nous avons assisté à une révolution numérique qui affecte globalement les systèmes sociaux, économiques, politiques et juridiques existants dans le monde. Cette révolution a transformé notre interaction avec la société et l'environnement. Comme c'est la règle pour tous les nouveaux développements, ils peuvent offrir à la société une occasion d'alléger les luttes, mais les nouveaux débuts ne sont pas toujours clairs et certainement pas simples. Les individus cherchent à saisir de vastes opportunités offertes par les technologies de l'information tant que les gens les perçoivent comme sûrs. Cependant, de telles révolutions doivent être abordées par des mécanismes juridiques afin d'équilibrer la vie privée, la protection des données et la nécessité de la sécurité. En ce sens, les chercheurs et les législateurs cherchent des mécanismes juridiques efficaces pour réglementer le nouveau domaine appelé cyberspace. Il existe essentiellement deux points de vue principaux: 1) Cet espace est libre du contrôle des souverains de l'espace réel, mais aussi les structures juridiques traditionnelles sont insuffisantes pour réglementer cette zone, 2) Cet espace n'est pas différent que l'espace, l'air et la mer ; Il a des dimensions et des composants physiques; Les structures juridiques existantes sont donc adéquates pour offrir une protection. Nous adopterons et discuterons des points de vue hybrides qui indiquent que les structures juridiques existantes sont suffisantes, mais nous avons également besoin de nouvelles approches à un moment donné.

Cette thèse est composée de deux chapitres principaux, à savoir: 1) Le cyberspace, espionnage et cyber-espionnage, 2) Lutter contre le cyber-espionnage économique et industriel. Dans le premier chapitre, les défis inhérents à la définition et à la réglementation du cyberspace et des activités d'espionnage sont présentés. Cela montre que les juristes internationaux ont des opinions différentes sur la question de savoir si les activités de renseignement sont autorisées ou restreintes par le droit international lorsqu'elles sont menées en temps de paix ou de guerre. La thèse traite ensuite de la légalité des activités de guerre et des activités d'espionnage en temps de paix. En ce qui concerne les activités d'espionnage en temps de paix, nous analyserons les principes internationaux coutumiers qui permettent ou limitent ces activités. Bien que le droit international ignore les activités d'espionnage en temps de paix, Il ya plusieurs incidents et tentatives de réglementer ce domaine en particulier en temps de paix. Par exemple, des vols de reconnaissance U-2 ont ouvert la voie à la signature du Traité sur le ciel ouvert comme conclusion de confiance et des mesures de la sécurité.

Par conséquent, nous avons envisagé la même procédure peut se produire en ce qui concerne cyber-espionnage. Cependant, en raison de la prolifération des opérations de cyber-espionnage, les États et les sociétés recherchent fortement des réglementations ou des mécanismes internationaux pour protéger leurs intérêts stratégiques.

En outre, cette thèse identifie le cyber-espionnage et les caractéristiques changeantes de l'espionnage, telles que son objet et ses cibles, ses méthodes et moyens, ses acteurs et ses incidents. Fondamentalement, ceci est de montrer que les activités d'espionnage moderne ne peuvent pas être comparées à celles que les gens ont l'habitude de voir dans James Bond ou d'autres films d'Hollywood. Bien que l'espionnage semble avoir été accepté comme un outil adopté par les partis de guerre en temps de conflit, en fait, l'espionnage et ses techniques, mécanismes et outils sont à double usage dans la nature. Cette nature a été comprise, observée et expérimentée au cours de la dernière décennie à la suite de la prolifération de la technologie, ce qui ouvre la voie à des cyber-armes, des attaques, des crimes et de l'espionnage. Nous allons expliquer les caractéristiques changeantes de l'espionnage face à l'évolution de la technologie. Par exemple, l'un des outils importants fréquemment adoptés par le cyberespionnage est appelé MPA, Menace Persistante Avancée, qui est une technique sophistiquée utilisée par les pirates pour extraire de grandes quantités de données des industries ciblées sur une longue période de temps. Ce type d'attaque est bien adapté aux secteurs ou réseaux informatiques prévus et possède des capacités avancées pour extraire des données et compromettre l'entité ciblée. Un tel adversaire peut passer des années à exfiltrer des documents de l'entité ciblée sans être repéré.

Dans une section centrale détaillée, la thèse fournit une évaluation du cyber-espionnage sous la théorie juridique internationale. A ce point, la thèse soutient le choix rationnel et la théorie des jeux plutôt que les approches classiques. Nous considérons l'application de choix rationnels et de théories de jeu pour expliquer la logique derrière cyber-espionnage et cyberattaques. En d'autres termes, les acteurs du cyberspace agissent et décident rationnellement dans le cas du choix de leurs cibles donc, leurs choix finissent par créer une norme ou offrir un moyen de créer une norme. Ainsi, nous concluons que des mesures de confiance et de renforcement de la sécurité peuvent être proposées en ce qui concerne les activités ou l'inactivité des acteurs adoptant le cyber-espionnage.

Le deuxième chapitre est consacré aux outils juridiques nationaux et internationaux appropriés à adopter en cas d'incidents de cyberespionnage. Nous avons accepté et construit notre analyse sur le fait que les activités de cyberespionnage sont une sorte de cyberattaque qui viole les droits de propriété intellectuelle, les secrets commerciaux et la confidentialité, l'intégrité et parfois la disponibilité des réseaux ciblés. Beaucoup d'États n'ont pas de règlement spécifique consacré à lutter contre le cyberespionnage, alors les approches juridiques traditionnelles proposent d'appliquer des crimes de propriété intellectuelle à de telles activités. Par conséquent, les réglementations relatives à la protection des secrets commerciaux et des cybercrimes sont des outils juridiques nationaux si un réseau privé est ciblé par le cyberespionnage. Il existe également des règlements spécifiques pour pénaliser l'espionnage économique et industriel. Ces règlements n'existent que dans le cadre du système juridique américain, de sorte que nous analyserons également ces règlements. En ce qui concerne les réglementations nationales, nous avons comparativement analysé les systèmes juridiques turc et américain en matière de protection des secrets commerciaux et de crimes informatiques.

En ce qui concerne les réponses juridiques internationales, nous avons comparé les réponses juridiques données et discuté des sections précédentes sur les activités de cyberespionnage en temps de guerre et en temps de paix. Toutefois, les activités de cyberespionnage en temps de paix et les réponses juridiques appropriées sont les points focaux de l'étude, puisqu'ils sont fréquemment appliqués. Nous avons soutenu que les activités de cyberespionnage devraient être acceptées comme une forme d'utilisation de la force compte tenu de leurs effets extrêmement négatifs. En outre, les opérations cybernétiques ne sont pas nécessairement équivalentes au recours à la force au sens de l'article 2/4 de la Charte des Nations Unies pour être internationalement illicites, de telles opérations peuvent également violer certaines obligations et principes du droit international coutumier. En ce sens, les activités de cyberespionnage violent les principes coutumiers contraignants du droit international, qui interdit l'ingérence dans la souveraineté et les affaires intérieures d'autres États. Un État a la responsabilité juridique internationale d'un cyberfonctionnement qui lui est imputable et qui constitue une violation d'une obligation internationale. L'argument juridique fondamental pour invoquer la responsabilité de l'État à l'égard du cyberespionnage économique est la souveraineté de l'État, qui couvre également le concept même de souveraineté économique. Que l'opération vise des infrastructures publiques ou privées, les États ont la souveraineté sur les deux. Nous soutiendrons que les opérations de cyberespionnage fournissent des motifs juridiques suffisants pour invoquer la responsabilité de l'État et adopter des mesures appropriées compatibles avec des faits internationalement illicites, qui sont considérés comme des rétorsions et des contre-mesures couvrant les sanctions diplomatiques et économiques. Par conséquent, le premier mécanisme est de déclarer la responsabilité des États pour les actes illégitimes et de prendre des mesures appropriées.

De plus, nous avons constaté que de nombreuses activités de cyber-espionnage sont menées avant ou pendant les négociations bilatérales ou multilatérales. En ce sens, la thèse soutient que la Convention de Vienne sur le droit des traités peut protéger et jouer un rôle dissuasif important pour de telles activités, car elles violent le principe de bonne foi et limitent la capacité des parties à négocier librement et équitablement. Par conséquent, de telles violations peuvent entraîner la nullité du traité par la fraude, qui est adopté par la Convention de Vienne sur le droit des traités. À titre d'exemple, nous avons étudié l'affaire *Timor-Leste vs. l'Australie*. En ce qui concerne l'affaire, la violation des obligations découlant du droit conventionnel et des normes et principes établis du droit international (inviolabilité des locaux diplomatiques, bonne foi dans les négociations, souveraineté des États et non-intervention) fournissent une base juridique concrète pour affirmer l'illégalité du cyber-espionnage. Cependant, établir le lien juridique et factuel entre l'espionnage et la conduite frauduleuse est complexe et problématique en raison de l'absence de tout précédent.

Enfin, comme les activités de cyber-espionnage économique et industriel ciblent les propriétés intellectuelles, nous avons discuté des mesures légales adoptées par l'Accord sur les Aspects des Droits de Propriété Intellectuelle qui Touchent au Commerce (ADPIC). Dans les limites des accords de l'Organisation Mondiale du Commerce (OMC), l'interprétation du préambule de l'Accord sur les ADPIC inclut les opérations de cyber-espionnage économique dans le cadre de l'accord. Comme dans le commentaire de l'article 39 de l'Accord sur les ADPIC, «une manière contraire aux pratiques commerciales honnêtes» a été expliquée comme «rupture de contrat, violation de la confiance et incitation à la violation et comprend l'acquisition d'informations non divulguées par des tiers qui connaissaient ou ont commis une négligence grave en omettant de savoir que de telles pratiques étaient impliquées dans

l'acquisition.» Conformément au libellé de l'article, il convient de reconnaître que les opérations de cyberespionnage sont en quelque sorte contraire aux pratiques commerciales honnêtes. Toutefois, les obligations créées par l'OMC ne sont efficaces et contraignantes que sur le territoire des parties. Nous avons conclu que le mécanisme de règlement des différends de l'OMC est politiquement «le forum le plus approprié et le plus efficace», mais légalement, les parties de l'OMC et l'ADPIC devraient d'abord s'entendre sur les normes et principes internationaux limitant explicitement les opérations de cyber-espionnage économiques dans le cadre des accords de l'OMC.

À cette fin, en cas de réponses extraterritoriales, les États peuvent adopter certaines mesures conformément au droit international. Par exemple, déclarer ces activités comme des faits internationalement illicites et déployer des contre-mesures; Rechercher des réponses en droit conventionnel en conséquence, telles que la résiliation des traités bilatéraux en raison de fraudes; Ou d'appliquer des forums internationaux tels que l'OMC. Afin de répondre légalement aux activités de cyber-espionnage, nous devrions consulter les documents juridiques pour les définitions, la criminalisation et les sanctions pour les personnes physiques et morales.

Cette thèse offre aux États et aux entreprises ciblées par le cyber-espionnage économique et industriel des mesures juridiques efficaces pour faire face à de telles activités, et ainsi apporter une petite contribution pour améliorer la littérature juridique sur ce sujet.

ABSTRACT

This study joins a vibrant discussion in the social sciences about one of the challenging issues of cyber security in particular, cyberespionage, as well as appropriate legal responses that might be adopted by victim States. The aim of this study is to investigate and identify economic and industrial cyberespionage and to offer and analyze effective domestic and international legal responses.

First of all, we have witnessed a digital revolution, which affects the existing traditional social, economic, political and legal systems around the world globally. This revolution has transformed our interaction with societies and environments. As it is the rule for all new developments, they can offer society an opportunity to ease struggles, but new beginnings are not always clear and certainly not simple. Individuals seek to embrace vast opportunities offered by information technologies as long as they perceive them safe. However, such revolutions have to be addressed by legal mechanisms in order to balance privacy and the need for security. In this sense, scholars and law makers seek for effective legal mechanisms to regulate the new realm called cyberspace. Basically, there are two mainstream views: 1) this space is free from the control of real space sovereigns, but also traditional legal structures are insufficient to regulate this area, 2) this space is no different from space, air and sea; it has physical dimensions and components, therefore existing legal structures are adequate to offer protection. We will adopt and discuss hybrid views, which indicate that existing legal structures are sufficient, but we also need new approaches at some point.

This thesis is composed of two main chapters namely, 1) Cyberspace, espionage and cyberespionage, 2) Tackling economic and industrial cyberespionage. In the first chapter, challenges inherent to defining and regulating cyberspace and espionage activities are presented. This shows that international legal scholars have different opinions about deciding whether intelligence activities are permitted or restricted by international law when they are conducted in times of peace or war. The thesis then discusses the legality of wartime and peacetime espionage activities. Regarding peacetime espionage activities, we will analyze customary international principles which allow or restrict such activities. Although international law is oblivious to espionage activities during peaceful times, there are several incidents and attempts to regulate this area especially in peacetime. For example, U-2 reconnaissance flights paved the way for the signing of the Treaty on Open Skies as conclusion of confidence and security building measures. Therefore, we envisaged the same procedure can occur with regards to cyberespionage. However, due to the proliferation of cyberespionage operations, states and corporations strongly look for international regulations or mechanisms to protect their strategic interests.

This thesis further identifies cyberespionage and the changing features of espionage, such as its purpose and targets, methods and means, and actors and

incidents. Basically, this is to show that modern day espionage activities can not be compared to those people are used to seeing in James Bond or other Hollywood movies. Although espionage seems to have been accepted as a tool adopted by parties of war in times of conflict, actually, espionage and its techniques, mechanisms and tools are dual-use in nature. This nature has been understood, observed and experienced within the past decade as a result of the proliferation of technology, which paves the way for cyber weapons, attacks, crimes and espionage. We will explain the changing features of espionage in the face of evolving technology. For instance, one of the significant tools frequently adopted by cyberespionage is called APT, Advanced Persistent Threat, which is a sophisticated technique used by hackers to extract large amounts of data from targeted industries over a long period of time. This type of attack is well-tailored for intended sectors or computer networks and has advanced capabilities to extract data and compromise the targeted entity. Such an adversary can spend years to exfiltrate documents from the targeted entity without being spotted.

In a detailed central section, the thesis provides an evaluation of cyberespionage under international legal theory. Here, the thesis supports rational choice and game theory rather than classical approaches. We consider the application of rational choice and game theory for explaining the logic behind cyberespionage and cyber attacks. In other words, the actors in cyberspace act and decide rationally in the case of choosing their targets therefore, their choices eventually create a norm or offer a way for creating a norm. Thus, we conclude that confidence and security building measures can be proposed regarding activities or inactivity of the actors adopting cyberespionage techniques.

The second chapter is devoted to the domestic and international legal tools appropriate to adopt in cases of cyberespionage incidents. We accepted and built our analysis upon the fact that cyberespionage activities are a kind of cyber attack, which violates intellectual property rights, trade secrets and confidentiality, integrity and sometimes availability of the targeted networks. Many states do not have specific regulations dedicated to tackle cyberespionage so, traditional legal approaches offer to apply regulations covering intellectual property crimes for such activities. Therefore, regulations related to the protection of trade secrets and cybercrimes are domestic legal tools if any private network is targeted by cyberespionage. There are also specific regulations to penalize economic and industrial espionage. Those regulations exist only under the American legal system, so we will also analyze these regulations as well. With regards to domestic regulations, we comparatively analyzed the Turkish and American legal systems in terms of protection of trade secrets and computer crimes.

In terms of international legal responses, we have compared legal responses given and discussed previous sections on wartime and peacetime cyberespionage activities. However, peacetime cyberespionage activities and the appropriate legal responses are the focal points of the study, as they are frequently applied. We argued that cyberespionage activities should be accepted as a form of use of force considering their extremely adverse effects. Moreover, cyber operations need not amount to use of force within the meaning of article 2/4 of the UN Charter to be internationally wrongful, such operations can violate certain obligations and principles of customary international law either. In this sense, cyberespionage activities violate the binding customary principles of international law, which prohibits interference with the sovereignty and domestic affairs of other states. A state bears international legal responsibility for a cyber operation attributable to it and which constitutes a breach of

an international obligation. The basic legal argument to invoke state responsibility with regard to economic cyberespionage is state sovereignty, which also covers the very concept of economic sovereignty. Whether the operation targets public or private infrastructures, states have sovereignty over both of them. We will argue that cyberespionage operations provide sufficient legal grounds to invoke state responsibility and adopt appropriate measures compatible with internationally wrongful acts, which are considered retorsion and countermeasures covering diplomatic and economic sanctions. Therefore, the first mechanism is declaring responsibility of states for illegitimate acts and taking appropriate measures.

Furthermore, we have identified that cyberespionage activities are also conducted before or during bilateral or multilateral treaty negotiations. In this sense, the thesis argues that the Vienna Convention on the Law of Treaties can provide protection against and play a significant deterrent role for such activities, as they violate the good faith principle and limit the parties' ability to negotiate freely and fairly. Therefore, such violations can trigger invalidity of the treaty by fraud, which is adopted by the Vienna Convention on the Law of Treaties. To illustrate, we have investigated the *Timor-Leste vs. Australia* case. With regard to the case, violation of both treaty law obligations and established international law norms and principles (inviolability of diplomatic premises, good faith in negotiations, state sovereignty and non-intervention) provide concrete legal basis to assert illegality of cyberespionage. However, establishing the legal and factual link between espionage and fraudulent conduct is complex and problematic due to the lack of any precedent.

Lastly, as economic and industrial cyberespionage activities target intellectual properties, we have discussed legal measures adopted by the Trade-Related Aspects of Intellectual Property Rights (TRIPS) Agreement. Within the limits of World Trade Organization (WTO) agreements, the interpretation of the preamble of the TRIPS Agreement include economic cyberespionage operations within the agreement. As in the commentary of the Article 39 of the TRIPS, "a manner contrary to honest commercial practices" has been explained as a "breach of contract, breach of confidence and inducement to breach, and includes the acquisition of undisclosed information by third parties who knew, or were grossly negligent in failing to know, that such practices were involved in the acquisition." Pursuant to the wording of the article, it should be acknowledge that cyberespionage operations are kind of manner contrary to honest commercial practices. However, obligations created by the WTO are only effective and binding within the territories of the parties. Therefore, we have concluded that the WTO dispute resolution mechanism is politically "the most appropriate and effective forum", but legally, parties of the WTO and TRIPS should first agree on international norms and principles explicitly restricting economic cyberespionage operations under WTO agreements.

To this end, in case of extraterritorial responses, states may adopt certain measures in accordance with international laws. For instance, declaring such activities as internationally wrongful acts and deploy countermeasures; seek for treaty law responses accordingly such as terminating bilateral treaties due to fraudulence; or apply international forums such as the WTO. In order to respond to cyberespionage activities legally, we should consult legal documents for definitions, criminalization, and punishments for individuals and legal entities.

This thesis offers, States and corporations targeted by economic and industrial cyberespionage, several effective legal measures on confronting such activities, and thus make a small contribution to improve the legal literature on this subject.



ÖZET

Bu çalışma, sosyal bilimlerde giderek daha fazla ilgi gören ve pek çok çalışmaya konu olan siber güvenlik altında yer alan siber espionaj ve bu siber espionaj operasyonlarına hedef olan Devletlerin başvurabileceği hukuki mekanizmalara dair tartışmalara katkı sunmaktadır. Bu çalışmanın öncelikli amacı, ekonomik ve endüstriyel siber espionajı tanımlamak ve araştırmak, öte yandan bu tehdide karşı başvurulabilecek etkili, ulusal ve uluslararası hukuki çareleri analiz ederek çözüm önermektir.

İlk olarak belirtmek gerekir ki, bu çalışmanın çıkış noktası, dünya çapında geleneksel sosyal, ekonomik, siyasal ve hukuki sistemleri derinden etkileyen ve değişmeye zorlayan dijital bir devrime tanıklık edişimizdir. Bu devrim bizim toplumla ve çevremizle olan etkileşimimizi kökten etkiledi. Her yeni gelişme doğası gereği, var olan zorlukları ve engelleri aşabilmek adına bir fırsat sunmaktadır. Ancak yeni başlangıçlar her zaman sanıldığı kadar kolay ve kabul edilebilir olmaz. Bireyler, bilgi teknolojilerinin onlara sunduğu sınırsız fırsatları bu teknolojilerin güvenli olduklarına *inandıkları* zaman kabul etme eğilimindedirler. Bireylerin inançları bir yana, bu dijital devrimin güvenlik-özgürlük ya da kişisel mahremiyet ikileminde dengelenmesi hukuki araçlarla mümkündür. Bu çerçevede, düşünürler, akademisyenler ve kanun koyucular, siber uzay olarak adlandırılan bu yeni dünyayı düzenlemek için gerekli ve etkili hukuki mekanizma ve prensipleri tartışmaktadır. Bu konuda temel olarak iki ana akım görüş olduğunu söyleyebiliriz. İlk görüşe göre, bu alan Devletlerin kontrol ve düzenlemesinden bağımsızdır ve geleneksel hukuki yapılar bu alanı düzenlemekte yetersiz kalmaktadır. İkinci görüşe göre ise bu alan uzay, hava, denizden farklı değildir; bu alanın fiziksel bir yanı ve onu oluşturan somut bileşenleri vardır. Bu açıdan mevcut hukuki yapılar ve prensipler bu alanı düzenlemek için yeterlidir. Bu çalışmada, yukarıdaki iki görüş dışında mevcut hukuki yapı ve prensiplerin yeterli olduğunu ama bazı noktalarda yenilenmeye ve yeni yaklaşımlara ihtiyaç duyulduğunu savunan hibrit bir bakış açısı benimsenecektir.

Bu tez, iki ana bölümden oluşmaktadır. İlk bölüm siber uzay, espionaj, siber espionaj ile ilgilidir. İkinci bölüm ise ekonomik ve endüstriyel siber espionaj ile mücadelede başvurulabilecek hukuki mekanizmalara ayrılmıştır. İlk bölümde, siber uzay ve espionaj faaliyetlerinin tanımlanması ve düzenlenmesine ilişkin sorunlar ele alınmıştır. Siber uzayın düzenlenmesine dair fikir ayrılığı, espionaj faaliyetlerinin düzenlenmesi konusunda da karşımıza çıkmaktadır. Uluslararası hukukçular, barış zamanı ya da savaş zamanı gerçekleştirilen espionaj faaliyetlerinin uluslararası hukuk altında izin verilmesi ya da yasaklanması konusunda fikir ayrılığı yaşamaktadır. Bu noktada, tezimiz, savaş ya da barış zamanı espionaj faaliyetleri hukukiliğini kuşatıcı bir şekilde tartışmaktadır. Barış zamanı espionaj faaliyetleri bağlamında, uluslararası hukuk prensipleri ve teamül hukuku, bu faaliyetlere onay verme ya da sınırlama bakımından incelenmiştir. Her ne kadar uluslararası hukuk barış zamanı espionaj faaliyetleri konusunda sessiz kalsa da, bu alanı düzenlemek için bazı girişimler ve

Devletleri bu alanı düzenlemeye zorlayacak bazı vakıalarda yaşanmıştır. Örneğin, U-2 istihbarî keşif uçuşlarının yol açtığı uluslararası kriz, sonraki yıllarda güven ve güvenlik artırıcı önlemlerin geliştirilmesi ve nihayetine Açık Gökyüzü Anlaşması'nın akdedilmesini sağlayacaktır. Aynı sürecin, siber espionaj açısından da yaşanacağı, gerçekleşen saldırıların böylesi bir uluslararası uzlaşmayı ya da uluslararası normların kabulünü için (state practice) Devlet uygulaması oluşturacağını; Devletlerin bu faaliyetleri yasaklayan ve cezalandıran yasal düzenlemelerinin ise opinio juris olarak kabul edilebileceğini düşünüyoruz. Tallinn Manual-1 ve hâlihazırda devam eden Tallinn Manual-2 çalışmaları bu alanda uluslararası bir konsensüs oluşması noktasında kayda değer gelişmelerdir. Ancak şu aşamada Devletler ve şirketler, uluslararası norm oluşturmak ve bu saldırıları azaltmak yerine, stratejik çıkarlarını koruyabilecek mevcut hukuki mekanizmaları kullanma eğilimindedirler. Dolayısıyla tezimiz ulusal ve uluslararası düzeyde yer alan bu mekanizmaları ele alacaktır.

Tezimiz, yükselen bir trend olan siber espionajı ve geleneksel espionaj faaliyetlerinin değişen özelliklerini açıklamaktadır. . Espionajın tarihsel olarak amaç ve hedefleri, metot ve araçları, aktörleri ve vakıalara değişime uğramıştır. Temel olarak, bu araştırma, modern çağlarda gerçekleştirilen espionaj faaliyetlerinin, James Bond ya da Hollywood filmlerinde görmeye alıştığımız espionaj faaliyetlerinden oldukça farklı olduğunu göstermektedir. Her ne kadar espionaj ve gözetleme faaliyetlerinde kullanılan araçların, taraflarca savaş zamanında uyguladığı kabul edilse de, gerçekte, teknolojik araçların doğası gereği çift kullanıma sahip olduğu anlaşılmıştır. Bir yandan sivil diğer yandan askeri amaçlarla kullanıma açık olan bu araçların çoğalması siber silah, siber saldırı, siber suçlar ve siber espionajın ortaya çıkmasına yol açmıştır. Bu açıdan teknolojik gelişmelerin espionaj faaliyetlerini nasıl değiştirdiği ve geliştirdiği açıklanmıştır. Örneğin, APT, Advanced Persistent Threat olarak adlandırılan bilgi toplama amacı ile yapılan hedef odaklı saldırılardır. Belirli bir hedefe veya kuruma yönelik olması, geleneksel güvenlik mekanizmalarını atlatabilmesi ve hedef kurumlarda uzun süreli olarak faaliyet göstermesi bu saldırıların tespitini zorlaştırmaktadır. Bu tip saldırılar hedef alınan sektör veya bilgisayar sistemine özel olarak tasarlanmış siber silahlarla gerçekleştirilmekte ve tespit edilmeden bilgi sızdırmaya devam etmektedir.

Birinci bölümün son kısmında, siber espionaj faaliyetleri uluslararası hukuk teorileri bağlamında ele alınmıştır. Rasyonel seçim ve oyun teorisinin siber espionaj ya da siber saldırıların arkasında yatan motivasyonu açıklamada yeterli olduğu düşünülmektedir. Bir başka değişle, siber espionaj aktörleri hedeflerini stratejik ve rasyonel bir seçimle belirlemektedir.

İkinci bölümde, ekonomik ve endüstriyel siber espionaj faaliyetlerine maruz kalan mağdur Devletlerin ve şirketlerin uygulayabileceği ulusal ve uluslararası hukuki mekanizmalar ele alınmıştır. Siber espionaj faaliyetlerinin bir siber saldırı olduğu kabul edilmiştir. Dolayısıyla, hedefleri değerli ticari sırları, fikri mülkiyet ürünlerini ele geçirmek olan bu saldırılara karşı başvurulabilecek cezai ve hukuki fikri mülkiyet ve ticari sır düzenlemeleri açıklanmıştır. Öte yandan siber saldırılar bilgisayar sistemlerinin gizliliğini (confidentiality), bütünlüğünü (integrity) ve kullanılabilirliğini (availability) ihlal etmektedir. Bu ihlal ise pek ulusal hukuk sisteminde siber suçlar olarak ceza hukuku altında düzenlenmiştir. Amerika Birleşik Devletleri ve Birleşik Krallık dışında pek çok Devlet özellikle siber espionaj faaliyetlerini yasaklamak için çıkarılmış bir düzenlemeye sahip değildir. Geleneksel hukuki yaklaşım bu faaliyetleri, fikri mülkiyet suçları ya da ticari sırların korunması ile siber suçlar kapsamında değerlendirmektedir. Yeni hukuki yaklaşım ekonomik ve

endüstriyel siber espionaj faaliyetlerinin artırılmış para ve hapis cezalarıyla düzenlenmesini önermektedir. Bu noktada, Amerika Birleşik Devletlerinde var olan özel düzenleme ele alınacaktır. Türk hukuk sistemi altında ise ticari sırların korunması ile siber suçlar mevzuatı, siber espionaj bağlamında değerlendirilecektir.

Uluslararası düzeyde başvurulabilecek hukuki mekanizmalar savaş ve barış zamanı olarak ikili bir ayrım altında ele alınmıştır. Ancak barış zamanı siber espionaj faaliyetleri, sıklıkla karşılaşıldığı için, çalışmamızın odak noktasını oluşturmaktadır. Öncelikle, barış zamanı siber espionaj faaliyetlerinin, yıkıcı sonuçlar doğurma potansiyeli dolayısıyla bir çeşit kuvvet kullanımı olduğu kabul edilmiştir. Birleşmiş Milletler Şartı'nın 2/4 maddesinde ifadesin bulan kuvvet kullanımı, siber saldırılar bağlamında pozitif ve negatif hukuki argümanlarla ayrıntılı olarak tartışılmıştır. Bunun yanı sıra, siber saldırıların kuvvet kullanımı seviyesine ulaşmadığı düşünülse de, yine de bu saldırılar doğaları gereği uluslararası hukukun, ekonomik egemenliği de kapsayan Devletlerin egemenliği ve içişlerine müdahale yasağı gibi temel prensiplerini ihlal etmektedir. Uluslararası yükümlülükleri ihlal eden ve kendisine atfedilen bir siber saldırı dolayısıyla Devletlerin sorumluluğu gündeme gelmektedir. Saldırının özel ya da kamusal bir altyapı ya da sistemi hedef almış olması saldıran Devletin sorumluluğunu etkilemeyecektir. Siber espionaj faaliyetlerinin, saldıran devletin uluslararası sorumluluğunu ileri sürmek için yeterli hukuki gerekçeyi sağladığı açıklanmıştır. Bu faaliyetlere karşı ise uluslararası hukuka aykırı davranışla orantılı karşı önlem ve misillemelere başvurulması mümkün olmaktadır. Bu açıdan mağdur devletlerin ilk olarak benimseyebileceği hukuki mekanizma, siber espionaj faaliyetlerinin uluslararası hukuka aykırılığının açıklanması ve sonrasında saldıran devlete karşı orantılı önlemlere başvurulmasıdır.

Bununla birlikte, siber espionaj faaliyetlerine iki ya da çok taraflı anlaşmaların müzakere aşamasında başvurulduğunu görülmektedir. Dolayısıyla bu tez, Uluslararası Anlaşmalar Viyana Sözleşmesinin mağdur Devlete bu faaliyetleri önleyecek, uygulayan devletleri ise caydırabilecek birtakım hukuki korunma yolları önerdiğini ileri sürmektedir. Öyle ki, siber espionaj faaliyetleri, tarafların özgür ve dürüstçe müzakere etme kabiliyetini ve müzakerelerde iyi niyet prensibini açıkça ihlal etmektedir. Bu ihlal, Uluslararası Anlaşmalar Viyana Sözleşmesi'nin 49. maddesinde karşılığını bulan hile yoluyla anlaşmanın geçersizliğine yol açabilecektir. Hile yoluyla anlaşmanın geçersizliğine örnek olarak, güncel *Timor-Leste vs. Australia* davası incelenmiştir. Bu davada, uluslararası anlaşma hukukuna ilişkin yükümlülüklerin ihlali ile uluslararası temel ilkelerin ihlali (diplomatik konutların dokunulmazlığı, müzakerelerde iyi niyet prensibi, devlet egemenliği ve müdahale yasağı) siber espionaj faaliyetlerinin hukuksuzluğunu ileri sürmek için yeterli ve gerekli hukuki gerekçeleri sağlamaktadır. Yine de bu faaliyet ile hileli davranış arasında hukuki ve fiili illiyet bağıni kurmak, geçmiş bir örnek bulunmadığı için tartışmalı olmaktadır.

Son olarak, bu tez, ekonomik ve endüstriyel siber espionaj faaliyetleri fikri mülkiyete konu ürünleri hedef aldığı için, Ticaretle Bağlantılı Fikri Mülkiyet Hakları Anlaşması'nı (TRIPS) ihlal ettiğini ve Dünya Ticaret Örgütü (WTO) altında birtakım mekanizmaların harekete geçirilebileceğini tartışmaktadır. TRIPS Anlaşmasının 39 maddesinde yer alan "dürüst ticari uygulamalara aykırı" ifadesi "sözleşmenin ihlali, güvenin ihlali ve ihlale teşvik gibi uygulamalar anlamında olacak ve açıklanmamış bilgilerin elde edilmesinde bu uygulamaların katkısı olduğunu bilen veya bilmemesinde ağır ihmalin söz konusu olduğu üçüncü taraflarca açıklanmamış bu bilgilerin elde edilmesini" kapsamaktadır. Bu açıdan siber espionaj faaliyetleri dürüst ticari uygulamaları açıkça ihlal etmektedir. Bu ihlale karşı WTO uyuşmazlık çözüm

mekanizması teorik olarak harekete geçirilebilecektir. WTO uyuşmazlık çözüm mekanizmasının siber espionaj faaliyetlerine karşı siyaseten etkili olduğunu ancak hukukten WTO'ya taraf devletlerin öncelikle bu faaliyetleri yasaklayan ya da sınırlayan hükümler üzerinde uzlaşması gerektiği açıklanmıştır. Zira 39. madde anlaşmaya taraf devletlere bu maddenin gereklerine uygun hukuki düzenlemeleri hayata geçirmesini istemektedir. Siber espionaj faaliyetlerinin sınıraşan niteliği dikkate alındığında sadece iç hukuk düzenlemeleri yapılmasını şart koşan 39. madde WTO uyuşmazlık çözüm mekanizmasının harekete geçirilebilmesi için başlı başına hukuki bir temel olması tartışmalıdır. Bu sebeple WTO'ya taraf devletlerin mutlaka bu konuya değinen bir madde üzerinde uzlaşması gerekmektedir.

Bu bağlamda, mağdur Devletler ve şirketlerin siber espionaj faaliyetlerine karşı, birtakım ulusal ve uluslararası hukuk mekanizmalarını harekete geçirebileceği tartışılmıştır. Ulusal düzeyde, ticari sırların korunması, cezai ve hukuki fikri mülkiyet haklarının korunması ile siber suçlar; uluslararası düzeyde ise uluslararası hukuka aykırılığın ilanı ve orantılı karşı önlemlere başvurulması, anlaşmalar hukuku bağlamında anlaşmanın geçersizliğini ileri sürülmesi, WTO uyuşmazlık çözüm mekanizmasının harekete geçirilmesi siber espionaj faaliyetlerine karşı başvurulabilecek yollar olarak incelenmiştir.

Bu tez, ekonomik ve endüstriyel espionaj mağduru Devletlere ve şirketlere başvurabilecekleri etkili hukuki çözüm yolları araştırmakta ve siber güvenlik alanındaki hukuki literatüre ufak bir katkı sunmayı amaçlamaktadır.

INTRODUCTION

“The computer will condition every facet of human life in the future and so far as law is used to regulate that life it will affect the development of the law.”¹

Colin Tapper, 1973

Rapid developments in Internet and information technologies since 90s not only have changed our daily lives but also have transformed the way we perceive the world. Initial signs of this change can be traced back to 80's when the cost of storing data was reduced and personal computers began to be used widely.² The first computers were used mostly to process data and for calculation purposes. This traditional and limited relation between user and device demonstrated one-way interaction which was destined to evolve into a larger, comprehensive cyber environment together with the further developments in the field. Therefore; later with the launch of blogs and portals people started to interact with each other and every individual appeared to be an active player creating a multifaceted interactive platform. This shift to personal computers and Internet usage helped Internet and information technologies create massive economy. According to Boston Consulting Group, “By 2016, there will be 3 billion Internet users globally and the Internet economy will reach \$4.2 trillion in the G-20 economies.”³ In other words, Internet economy will rank among world's top five economies. As Murray stated we have experienced massive digitization process in every corner and have witnessed spread of computers in various areas from finance to

¹ Colin Tapper, **Computers and the Law**, Wiedenfeld and Nicolson, (1973), xv.

² In 1956 it cost \$50,000 to buy the world's first hard drive which stores 5MB of data. By 1980 a 26 MD HDD costs \$5,000. In 1987 a 40MB HDD was \$1,799. By the 1995 2.9 MB HDD becomes \$2,899 which cost 85 cent per MB. Nowadays the price per MD of HDD drops to 0.008 cent. For more information see: *Historical Notes about the Cost of Hard Drive Storage Space*, <http://ns1758.ca/winch/winchest.html>

³ The Boston Consulting Group Inc., ‘**The Internet Economy in the G-20**’ (2012), 1.

health, water management to electricity distribution lines/grids, personal messaging to diplomatic messaging and so on.⁴ Cate describe this phenomenon as “we are witnessing an explosion in digital data.”⁵ However, negative side of the coin began to speak on itself as these developments continue to occupy our individual and professional lives. Even though those changes have altered communication and information technologies and erased many challenges from our lives to a great extent, they also have paved the way for proliferation of new kind of threats and crimes.

As it is the fact that throughout the history, new technological developments empowered many people to the detriment of existing and traditional power structures.⁶ Likewise, given the nature of the cyberspace, cross border cyber-attacks and cybercrimes become new challenges which threatens our security. Many of the states mentioned cybercrimes and cyber-attacks in their national cyber strategy policy papers. Especially in the UK, cybercrime is one of the founding pillar of the national cyber strategy among highest priorities.⁷ This rising phenomenon creates several problems in terms of economy, politics, law, and technics and cooperation. Thanks to the easy and inexpensive access opportunities to computers and Internet connection, standalone criminals or stated backed entities can initiate cross border cyber-attacks successfully. They target national critical infrastructures such as finance and banking networks or flight control systems, which results in devastating harms to the states and individuals.

In addition to cybercrimes and cyber-attacks, today almost every nation suffers from cyberespionage, technically named as computer network exploitation.⁸ The underlying reason for that is the change in known patterns of espionage within a decade. Along with its methods and means, targets and its purpose have fundamentally changed. The ultimate purpose and target of the operations become to acquire

⁴ Andrew Murray, **Information Technology Law** (Oxford 2013) 5.

⁵ Fred H. Cate, **Privacy in the Information Age**, Brookings Institute Press, (1997), 16.

⁶ Eric Schmidt and Jared Cohen, **The New Digital Age: Reshaping the Future of People, Nations and Business**, (John Murray, 2013) 6-7; Moises Naim, **End of Power: From Boardrooms to Battlefields and Churches to States, Why Being in Charge isn't What it Used to be**, (Basic Books, 2013) 13-14; Henry Kissinger, **World Order**, (Penguin Books, 2014) 341-347.

⁷ UK government, **'A Strong Britain in an Age of Uncertainty: The National Security Strategy'** (2010) 27.

⁸ Katherine L. Herbig and Martin F. Wiskoff, **Espionage Against the United States by American Citizens 1947-2001**, Defense Personnel Security Research Center, (2002), 80: “Globalization is rapidly creating new international conditions based on global economics that will affect the allegiance of citizens. This development assures that economic espionage will become more important as dual-use Technologies blur the distinction between national defense and industrial applications.”

company data, which includes personal data, confidential data and intellectual property consist of business secrets, R&D documents, cutting edge technological plans etc. Secondly human based intelligence and espionage operations (HUMINT)⁹ have lost its importance, signal based intelligence and espionage operations (SIGINT and COMINT)¹⁰ has enormously proliferated given the changes of technological capabilities. Espionage is a grey and controversial area of international law, thus every nation regulates espionage under their criminal codes. However the matter of responding to or punishing the espionage, especially cyberespionage activities mostly based on APT (Advanced Persistent Threat) attacks, constitutes a remarkable aspect of the issue and there are more and more concrete, visible actions taken to prevent it. Due to radically increase of cyberattacks and espionage operations, states are looking for effective legal mechanisms to tackle with them. Victim states can condemn targeting state, initiate naming and shaming campaign against espionage operations but they are also looking for other legal mechanism such as invoking state responsibility, asserting violation of treaty obligations and seek for reparation and compensation.

This research analytically and legally examine and try to find an answer the question that how can states confront economic and industrial cyberespionage activities under existing international law mechanism. We do not have any claim emplace espionage under the boundaries of legal documents, however, we accepted economic and industrial cyberespionage as a fact and seek for legal mechanisms to tackle with. Our research covers the topic under two main chapters covering five headings: 1) Regulation of Cyberspace, Espionage and Its Changing Features and 2) Tackling with Cyberespionage.

Under the first main chapter, we aim to comprehend then analyze espionage activities and operations, regulations covering espionage operations under

⁹ EU Parliament, **Report on the Existence of A Global System for the Interception of Private and Commercial Communications (ECHELON interception system)** (2001/2098(INI)): “Protection of secret information is always organized in the same way: 1) only a small number of people, who have been vetted, have access to secret information 2) there are established rules for dealing with such information 3) normally the information does not leave the protected area, and if it does so, it leaves only in a secure manner or encrypted form. The prime method of carrying out organized espionage is therefore by gaining access to the desired information directly through people (‘human intelligence’). These may be: 4) plants (agents) acting on behalf of the service/business engaging in espionage 5) people recruited from the target area.

¹⁰ Ibid, “The form of espionage by technical means with which electromagnetic signals of any kind are intercepted and analyzed (‘signals intelligence’, SIGINT).”

international law and its changing features. Understanding the rationale behind espionage operations and activities will disclose its foundations and motivations. International law scholars discussed espionage operations according to a criteria which divides operations whether they are conducted on peacetime or wartime. Although espionage seems and has been long accepted that it is a tool adopted by parties of war in wartime, actually, espionage and its techniques, mechanisms and tools are dual-use in nature.¹¹ This nature is understood, observed and experienced within the past decade as a result of proliferation of technology which paves the way for cyber weapons, attacks, crimes and espionage. At this point we will explain the changing features of espionage in the face of proliferation of technology. Technology affected espionage in several ways; firstly purposes and targets are shifted. Military targets and gaining military supremacy was the primary purpose of the espionage operations for centuries. To illustrate, nowadays, accessing and acquiring assets, information, blueprints, patents which can be beneficial for industry and economy becomes primary purpose of the espionage operations. Secondly, methods and means of espionage operations have changed through human based intelligence to signal intelligence. Thirdly, actor and incidents of espionage operations have changed. To this end, we argued that theater of the espionage operations have been shifted from ground, physical space to cyber space; from wartime to peacetime and from military objectives to economic and industrial targets. Therefore we will argue that international, regional and domestic legal systems have to embrace that change and adopt it selves for this new phenomenon.

Under the second main chapter, we aim to clarify domestic, regional and international legal responses to and mechanism to tackle with cyberespionage. Turkish legal system and American legal system have been comparatively analyzed. We especially will focus on articles related with protection of trade secrets and commercial assets. European Cybercrime Convention has been examined as it is regional legal response to economic and industrial cyberespionage. Finally, international legal responses have been discussed. First response mechanism is responsibility of states for internationally wrongful acts. We will argue that cyberespionage operations provide a sufficient legal ground to invoke state responsibility and adopt counter measures compatible with internationally wrongful acts which as retorsion and

¹¹ Those that have both military and commercial applications.

countermeasures covering diplomatic and economic sanctions. Second response mechanism that we provide is international treaty law mechanisms. In case of conducting a cyberespionage before and during the treaty negotiations and after negotiations have been concluded, 1) principle of good faith constitute a legal base to terminate the treaty legally and 2) treaty can be deemed to be invalid by fraud due to cyberespionage. The last but not least, World Trade Organization (WTO) provide a legal forum for States to discuss and resolve their conflict relating to commercial and trade issues. Therefore, we argue whether economic and industrial cyberespionage can be addressed under the WTO litigation mechanism.

Within the conclusion part, we will provide final points which needs to be taken into account by victim States that seek for appropriate counter attack.

CHAPTER ONE

CYBERSPACE, ESPIONAGE AND CYBERESPIONAGE

“What are the social and private interest that the law should recognize and protect? Here technological change set new problems and gave new urgency to old ones. The law had to alter many definitions of what was private and what was public interest.

The law has almost always been acted upon by, or has responded to, technological change, rather than controlled it.”¹²

James Williard Hurst, 1950

“What was the most significant advancement that affected social, political, economic and legal systems fundamentally in the early 21st century?” This will be the question asked by 21st century historians. They will try to answer that question by looking at various developments that affect society, politics, economics and legal systems, but also their meaning, function and nature. They will possibly acknowledge the revolution in information technologies, which is defined as use of systems for storing, retrieving and sending information. This revolution is two-folded- firstly, the cost of storing information sharply decreases and secondly, connection speed and cost decrease dramatically.

Expanded access to information and the widespread usage of social media tools and the Internet have fundamentally affected the interaction between people and their environment. This accelerated and freed the dissemination of information, accurate or not, about any issue or fact. On the other hand, the protection of valuable information became more challenging due to the lack of security inherent to information

¹² James Williard Hurst, **The Growth of American Law: The Law Makers**, Boston, Little Brown and Company, (1950), 10.

technologies as they are not intended to provide security, but to create alternative communication challenges, which provide impregnable access.¹³

In this context, defining cyberspace and its components is significant in regards to regulation while protecting fundamental rights and freedoms, and to tackle criminals and threats effectively.

Although international law can be oblivious to espionage activities during times of peace, there are several incidents and attempts to regulate this area. Espionage activities have also undergone a fundamental transformation along with the above-mentioned revolution.¹⁴ Therefore, we will analyze and evaluate the change in purposes, means, targets and actors in this area. This quest will constitute a basis to analyze cyberespionage, define its legal characteristics and how to respond legally. In this chapter, we will present a definition of cyberspace and opinions on its regulation. Secondly, we will comparatively analyze positive and negative views on regulating peacetime espionage activities in order to provide a legal basis regarding international legal responses to peacetime cyberespionage activities.

¹³ David Sutcliffe, **What are the Current Grand Challenges of Internet Research**, Oxford Internet Institute Blog, (2016) “The technologies that affect us are changing far faster than at any previous time in the history; they are also being adopted at breakneck pace, i.e. faster than we can catch up, and this has unseen implications. The technology sector is used to asking ‘can we build it and make money?’ and dealing with the societal implications later.”

¹⁴ Katherine L. Herbig and Martin F. Wiskoff, **Espionage Against...**, 79: “The current revolution in information and communications Technologies is changing the scope and practices of espionage: spy’s method of collection, synthesis and transmission of information are shifting to take advantage of opportunities in these new technologies.”

A. Regulating Cyberspace and Espionage

1. Challenges Inherent to Regulating Cyberspace

a) Defining Cyberspace

“Relating to or characteristic of the culture of computers, information technology, and virtual reality”, is the definition of ‘cyber’ according to Oxford Dictionary.¹⁵ Cyberspace has become a widely-used notion, however the terminology to describe it is still developing. William Gibson, a science fiction writer, was the first to use the term “cyberspace” within his science fiction novel written in 1984.¹⁶

A review of government and scholarly literature reveals the difficulty of providing a conclusive and comprehensive definition of cyberspace that covers all of its functionality. In academics, Norbert Wiener first used the term cybernetics in 1948¹⁷, and in 1999, Lance Strate gave an early definition of cyberspace as a collective concept of “the diverse experiences of space associated with computing and related technologies”.¹⁸ Ottis and Lorents defined cyberspace as a “time-dependent set of interconnected information systems and the human users that interact where users, nodes and connections can appear and disappear and information is transformed over time”.¹⁹ A comprehensive definition was offered by Kuehl, according to which cyberspace is “a global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via

¹⁵ Oxford English Dictionary, Oxford University Press, 7, (2013), 173.

¹⁶ William Gibson, **Neuromancer**, Ace Publishing, (1984), 4. (“A year here and he still dreamed of cyberspace, hope fading nightly”)

¹⁷ Norbert Wiener, **Cybernetics, Second Edition: or the Control and Communication in the Animal and the Machine**, MIT Press, (1948).

¹⁸ Lance Strate, ‘**The Varieties of Cyberspace: Problems in definition and delimitation**’ Western Journal of Communication, 63 (1999) 383.

¹⁹ Ottis, R. & Lorents, P., ‘**Cyberspace: Definition and Implications**’, In Proceedings of the 5th International Conference on Information Warfare and Security, Dayton, Academic Publishing Limited, (2010), 267-270.

interdependent and interconnected networks using information communication technologies.”²⁰

Cyberspace is currently defined by the United States Department of Defense (US DOD) as a global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.²¹ It is also described in terms of three layers: 1) a physical network, 2) a logical network, and 3) a cyber-persona layer:

- The physical network is composed of the geographic and physical network components.
- The logical network consists of related elements abstracted from the physical network.
- The cyber-persona layer uses the rules of the logical network layer to develop a digital representation of an individual or entity identity.

According to Turkey’s National Cyber Security Strategy and 2013-2014 Action Plan, cyberspace is “the environment which consists of information systems that span across the world including the networks that interconnect these systems.”²² As for the National Institute of Standards and Technology (NIST), cyberspace is “a global domain within the information environment consisting of the interdependent network of information systems’ infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.”²³ According to the UK Cyber Security strategy, cyberspace is “an interactive domain made up of digital networks that is used to store, modify and communicate information. It includes the Internet, but also the other information systems that support our businesses, infrastructure and services.”²⁴ According to the l’Agence Nationale de la Sécurité des Systèmes d’Information (ANSSI) cyberspace is “espace de communication constitué par l’interconnexion mondiale d’équipements de traitement automatisé de données numériques”.²⁵ In other words, cyberspace is the communication space created by the

²⁰ Daniel T. Kuehl, ‘From cyber space to cyberpower: Defining the problem’ in Franklin D. Kramer, Stuart H. Starr, Larry K. Wentz, **Cyberpower and National Security**, National Defense University Press (2009) 28

²¹ Department of Defense Joint Publication 3-12, **Cyberspace Operations**, (2013).

²² Turkey’s National Cyber Security and 2013-2014 Action Plan, (2012).

²³ The White House Cyberspace Policy Review, (2009).

²⁴ The UK Cyber Security Strategy Protecting and promoting the UK in a digital world (2011).

²⁵ ANSSI Glossaire, see <https://www.ssi.gouv.fr/administration/glossaire/c/>

worldwide interconnection of automated digital data processing equipment. Therefore, key components of cyberspace can be defined and categorized as technology, complexity, human components along with its global nature.

In this regard, we simply prefer the definition of cyberspace as the “realm of computer networks (and the users behind them) in which information is stored, shared and communicated online”.²⁶ Although all of the above definitions except of given by US DOD, explain cyberspace as a virtual world, however, it is more than virtual and has a physical dimension. All human activity, this includes actions in cyberspace, takes place in the physical world. People log into computers and online services with regard to their geographical location; computers are addressed through domain names (such as www.abc.com) which gives no indication of physical location, but the knowledge containing that domain name is physically located in a server elsewhere.²⁷

b) Regulating Cyberspace

Ideas on regulating cyberspace have been changing since the 1990's, due to increasing risks and threats. Early scholars proposed the idea of cyber exceptionalism or cyber libertarianism, which defined cyberspace as transnational, far from regulations and a place where existing “legal concepts of property, expression, identity, movement, and context do not apply to.”²⁸ Other scholars opposed this idea, for example, Reed points out that there is fallacy behind cyber exceptionalism because “all the actors involved in an Internet transaction have a real-world existence and are located in one or more legal jurisdictions. It's inconceivable that a real world jurisdiction would deny that its laws potentially applied to the transaction”.²⁹ If traditional law enforcement bodies have faced the challenge of cross-border trade or

²⁶ P. W. Singer and Allan Friedman, **Cybersecurity and Cyberwar: What Everyone Needs To Know**, Oxford University Press, (2014) 13.

²⁷ Dorothy E. Denning, Peter F. MacDoran, ‘**Grounding Cyberspace in the Physical World**’, within Alan D. Campen, Douglas H. Deareh, R. Thomas Goodden (eds.), **Cyberwar: Security, Strategy and Conflict in the Information Age**, AFCEA International Press, (1996) 119.

²⁸ John Perry Barlow, “**A Declaration of the Independence of Cyberspace**” Electronic Frontier Foundation (1996) <https://projects.eff.org/~barlow/Declaration-Final.html> accessed on 18 July 2015; David Johnson and David Post, “**Law and Borders—The Rise of Law in Cyberspace**,” (1996) 48 Stanford Law Review 1367; Andrew Murray, **Information Technology Law** (Oxford 2013) 56.

²⁹ Chris Reed, **Internet Law: Text and Materials** (Cambridge, 2004), 175.

harm, the ordinary rules of private international law, jurisdiction and choice of law have proven effective in identifying the correct forum and legal rules to apply.³⁰

Even earlier, Goldsmith pointed out that cyber sceptics made three basic mistakes, which are overstatement of cyberspace transactions, disregarding “the distinction between default laws and mandatory laws”, and underestimation of the capability of existing legal tools and techniques.³¹ Besides Brown’s argument that “cyberspace is nowhere”³², according to the Dinnis and our view that “there does not exist some ‘matrix-like’ realm of cyberspace which bears no connection to the ‘real-world’. Actors still act in physical space; hardware and networks (even wireless and virtual ones) still require physical constructs.”³³

In the case of international law and cyberspace challenges, US State Department Legal Advisor Harold Koh also opposed the idea of cyber exceptionalism in 2012. In his speech, Koh stated that established norms and principles of international law are applicable to cyberspace and cyberspace is not a law free zone, but also set the fundamental question with regard to armed conflict, sovereignty, self-defense, cyber weapons, etc.³⁴ Even before Koh’s speech, some scholars underlined that existing international law norms and principles, especially designed for *jus ad bellum* and *jus in bello*, can provide a normative framework to cope with legal problems posed by cyberspace.³⁵ Nevertheless, even existing legal tools and techniques are needed to be revised, improved and interpreted so as to embrace the new challenges emerging due to technological advancement. For instance, the concept of war has undergone a transformation since the 1900’s. Its nature, definition, techniques, and elements have begun to change due to developments in technology. The often-quoted definition of war was underlined by L. Oppenheim, who stated several elements: “*war is contention*

³⁰ Reed, 176; Andrew Murray, *Information Technology Law* (Oxford 2013), 57.

³¹ Jack L. Goldsmith, “**Against Cyberanarchy**,” (1998) 65 *University of Chicago Law Review* 1200

³² Davis Brown, ‘A Proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict’, *HILJ* 47 (2006) 179.

³³ Heather Harrison Dinniss, **Cyber Warfare and the Laws of War**, (Cambridge, 2012) 28.

³⁴ Harold Hongju Koh, ‘**International Law in Cyberspace**’, The USCYBERCOM Inter-Agency Legal Conference (2012) <http://www.state.gov/s/l/releases/remarks/197924.htm> accessed on 18 July 2015.

³⁵ Michael N Schmitt, “**Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework**,” (1999) 37 *Columbia Journal of Transnational Law* 885; Heather Harrison Dinniss, *Cyber Warfare and the Laws of War*, (Cambridge, 2012) 9; see William M Stahl, ‘**The Uncharted Waters of Cyberspace: Applying The Principles of International Maritime Law to the Problem of Cybersecurity**’, 40, *GJICLR*, (2011), 247-273.

*between two or more states through their armed force, for the purpose of overpowering each other and imposing such conditions of peace as the victor pleases.”*³⁶

Within the last two decades, this definition has deteriorated and become limited only to one type of conflict³⁷ far from embracing the others.³⁸ For example, intra-state conflicts have increased in number, concepts like violent non-state actors or international foreign fighters have been proposed, and just as information warfare or cyber warfare, cyberespionage has come to light. Still, this does not mean that Oppenheim’s definition, likewise principles of armed conflict (*jus in bello*) or principles of *jus ad bellum*, is not adequate to cover new kinds of conflicts, but their elements should be interpreted in the light of new advancements.³⁹

In this context, on the one hand existing international law norms and principles should be interpreted with regards to cross border cyberespionage operations and activities, and new rules should be prepared to combat this new threat on the other.

³⁶ L. Oppenheim, **International Law, a Treatise** II (LONGMANS, first published 1912) 61.

³⁷ Yoram Dinstein, **War, Aggression and Self Defence**, Cambridge University Press 5th ed, (2011) 12 : “Oppenheim’s definition postulates what is termed nowadays a ‘total’ war. Many a war is unquestionably ‘total’ in that it is conducted with total victory in mind. Total victory consists of the capitulation of the enemy, following the overall defeat of its armed forces and/or the conquest of its territory, and if this is accomplished the victor is capable of dictating peace terms to the vanquished. Not every war is aimed at total victory. Oppenheim completely overlooked the feasibility of limited wars. Such wars are, in fact, of considerable frequency and import. In a limited war, the goal may be confined to the defeat of only some segments of the opposing military apparatus; the conquest of certain portions of the opponent’s territory (and no others); or the coercion of the enemy Government to alter a given policy without striving for total victory.”

³⁸ Further see: Rosa Brooks, **How Everything Became War and the Military Became Everything**, Simon and Schuster, (2016), 4 : “I sensed something disturbing: all our fine new technologies and fine new legal theories were blurring the boundaries of war, causing it to spread and ooze into everyday life. the U.S. government has also made it clear that it views cyber threats primarily through the lens of war.”; White House, **An International Strategy for Cyberspace** (2011), www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf : declaring that the United States would “respond to hostile acts in cyberspace as we would to any other threat to our country.” Harold H. Koh, **International Law in Cyberspace**, “cyber activities may in certain circumstances constitute uses of force, triggering the law of armed conflict and giving rise to a right to respond with traditional physical force.”

³⁹ See, Marco Roscini, **Cyber Operations and the Use of Force in International Law**, (Oxford, 2014); Marco Roscini, **World Wide Warfare—Jus ad bellum and the Use of Cyber Force** (2010) 14 Max Planck Yearbook of United Nations Law 96; Yoram Dinstein, **The Principle of Distinction and Cyber War in International Armed Conflicts**, (2012) 17 (2) Conflict Security Law 261-277; Yoram Dinstein, **Cyber War and International Law: Concluding Remarks at the 2012 Naval War College International Law Conference** (2013) 89 International Law Studies, 276.

2. Regulating Espionage

Although it is called the second oldest profession in the history⁴⁰ and practiced since the dawn of human history⁴¹, espionage is an evolving and dynamic concept, capable of adjusting itself to a changing environment. Apart from its application, methods and means, the legality of espionage activities is one of the disputed topics of law.

First of all, peacetime moral and legal rules are radically different from wartime rules. Therefore, international legal scholars have different opinions about deciding whether intelligence activities are permitted or restricted by international law as it's conducted in peacetime or wartime.⁴² Some scholars argued that these activities have been prohibited, others argued that it has been permitted, and a third group which described espionage activities as a gray area neither regulated nor permitted.

Along with the academics, in cases of wartime espionage activities, several international law documents set out limits and restrictions. Accordingly, the Geneva Convention of 1949⁴³ and Additional Protocol I of 1977 to the Geneva Conventions⁴⁴ embedded several articles imposing restrictions upon wartime espionage and penalties for captured spies.⁴⁵ Alternatively, in cases of peacetime espionage -as it is not defined by any international law instruments- international law treated espionage outside of the scope of law and does not impose any restrictions on peacetime espionage and intelligence collection activities.⁴⁶ However, it should be the other way around,

⁴⁰ Phillip Knightley, **The Second Oldest Profession: Spies and Spying in the Twentieth Century**, New York, W.W. Norton & Co., 1986.

⁴¹ Katharina Ziolkowski, 'Peacetime cyber espionage – new tendencies in public international law', in Katharina Ziolkowski (ed.), *Peacetime Regime for State Activities in Cyberspace: International Law, International Relations and Diplomacy* CCDCOE, (2013) 425.

⁴² See International law restrict espionage in peacetime: Quincy Wright, 'Espionage and the Doctrine of Non-Intervention in Internal Affairs' (1962) *Essays on Espionage and International LAW* 3 1. See International law allow espionage in peacetime: W. Hays Parks, 'The International Law of Intelligence Collection' (1999) *National Security Law* 433; Geoffrey B. Demarest, 'Espionage in International Law' (1996) 24 *DJILP* 321; A. John Radsan, 'The Unresolved Equation of Espionage and International Law', (2007) 28 *MJIL* 595; Jens David Ohlin, Kevin Govern, and Claire Finkelstein, **Cyber War: Law and Ethics for Virtual Conflicts**, (Oxford, 2015).

⁴³ Geneva Convention Relative to the Protection of Civilian Persons in Time of War (adopted on 12 August 1949, entered into force 21 October 1950) 75 U.N.T.S 287 art 5.

⁴⁴ Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflict (Protocol I) (Adopted June 8, 1977) 1125 U.N.T.S. 3 art 45, 46.

⁴⁵ Dieter Fleck, 'Individual and State Responsibility for Intelligence Gathering' (2007) 28 *MJIL* 687.

⁴⁶ John Kish and David Turns (ed.), **International Law and Espionage** (Kluwer Law International, 1995); John Yoo, 'Counterintuitive: Intelligence Operations and International Law' (2006) 28

because, “technically, the law of war is referred to using the Latin term *lex specialis*—special law. It is applicable in—and only in—special circumstances, but in those special circumstances, it supersedes ordinary law, or *lex generalis*, the “general law” that prevails in peacetime. We have one set of laws for “normal” situations, and another, more flexible set of laws for “extraordinary” situations, such as armed conflicts.”⁴⁷

In this sense, we will discuss the problems and challenges regarding regulation of espionage activities under international law.

a) Legality of Wartime Espionage Activities

Wartime espionage activities are allowed and regulated with several international legal documents. It is clearly state under Article 119 of HPCR Manual on International Law Applicable to Air and Missile Warfare that “Acts of espionage are not prohibited under the law of international armed conflict.”⁴⁸ Similarly, one of the early documents from the Hague Convention on respecting the Laws and Customs of War on Land states, “ruses of war and the employment of measures necessary for obtaining information about the enemy and the country are considered permissible.”⁴⁹ This convention also set rules for spies and espionage activities. According to Article 39 of the Protocol Additional (I) to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts⁵⁰, it is acknowledged that there are rules applicable to espionage:

1. *It is prohibited to make use in an armed conflict of the flags or military emblems, insignia or uniforms of neutral or other States not Parties to the conflict.*

MJIL, 626; Geoffrey B. Demarest, ‘**Espionage in International Law**’ (1996) 24 DJILP 321; Luke Pelican, ‘**Peacetime Cyberespionage: A Dangerous, but Necessary Game**’ (2012) 20 CommLaw Conspectus 363; Christopher S. Yoo, ‘**Cyber Espionage or Cyber War?: International Law, Domestic Law and Self-Protective Measures**’ Faculty Scholarship. Paper 1540 (2015) http://scholarship.law.upenn.edu/faculty_scholarship/1540 accessed 27 July 2015.

⁴⁷ Kristen Boon and Douglas Lovelace, **Terrorism: Commentary on Security Documents Volume 133. The Drone Wars of the 21st Century: Costs and Benefits**, Oxford, (2014) 140

⁴⁸ HPCR, **Manual on International Law Applicable to Air and Missile Warfare**, Harvard University, accessed <http://www.ihlresearch.org/amw/manual/section-r-espionage/r-general-rules/rule-119>

⁴⁹ **Hague Convention on respecting the Laws and Customs of War on Land**, entered into force 26.01.1910, art 24.

⁵⁰ Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I).

2. *It is prohibited to make use of the flags or military emblems, insignia or uniforms of adverse Parties while engaging in attacks or in order to shield, favour, protect or impede military operations.*

3. *Nothing in this Article or in Article 37, paragraph one (d), shall affect the existing **generally recognized rules of international law applicable to espionage** or to the use of flags.*

This article paves the way for applicability of generally recognized rules of international law to espionage through legal analogy. Based on this reasoning, we will try to examine the application of existing legal frameworks to new types of espionage activities. Furthermore, regarding Article 46 of the same protocol, named as ‘Spies’, specific provisions set out for regulating espionage activities:

1. *Notwithstanding any other provision of the Conventions or of this Protocol, any member of the armed forces of a Party to the conflict who falls into the power of an adverse Party while **engaging in espionage shall not have the right to the status of prisoner of war and may be treated as a spy.***

2. *A member of the armed forces of a Party to the conflict who, on behalf of that Party and in territory controlled by an adverse Party, gathers or **attempts to gather information shall not be considered as engaging in espionage** if, while so acting, he is in the uniform of his armed forces.*

3. *A member of the armed forces of a Party to the conflict who is a resident of territory occupied by an adverse Party and who, on behalf of the Party on which he depends, **gathers or attempts to gather information of military value within that territory shall not be considered as engaging in espionage** unless he does so through an act of false pretenses or deliberately in a clandestine manner. Moreover, such a resident shall not lose his right to the status of prisoner of war and may not be treated as a spy unless he is captured while engaging in espionage.*

4. *A member of the armed forces of a Party to the conflict who is not a resident of territory occupied by an adverse Party and **who has engaged in espionage in that territory shall not lose his right to the status of prisoner of war and may not be treated as a spy unless he is captured before he has rejoined the armed forces to which he belongs.***

Legal statutes of spies and espionage activities during times of war crystallized in these international legal documents. However, even before the enactment of these documents, several scholars argued about the legal status of spies and espionage activities. Pioneering international law scholar Hugo Grotius has mentioned spies and activities of espionage in his cornerstone book named *On the Law of War and Peace*. According to Grotius:

*“For so are Spies used, yet it is held lawful, by the general Consent of Nations, to send such, as Moses did, and such was Joshua himself and that justly sometimes, by such as have manifestly a lawful Cause to make War, by others with Impunity, which the Law of Arms grants.”*⁵¹

In the same book translated and published by another author, the same topic was explained by Grotius as,

*“...there is no doubt, but the law of nations allows anyone to send spies, as Moses did to the land of promise, of whom Joshua was one. Persons of that description may sometimes be lawfully employed by those, who are engaged in an evidently just war. Others too, who have not such evident proofs of the justice of their cause, may plead the rights of war as a vindication for employing such persons.”*⁵²

First of all, it is crucial to keep in mind while commenting on those paragraphs that Hugo Grotius has described this rule (allowance or consent of nations) at a time when human to human intelligence (human-based intelligence) is commonly employed and spying is a profession performed only by an individual without requiring any additional tools. However, today, almost all modern intelligence techniques require minimum human to human interaction, but are applied through technological devices.

Furthermore, according to Grotius, employing someone as a spy is lawful in the case of evidently just war situations, if there is not any evidence for justification of espionage, then the rights of war can be applied. There is only one option for employing a spy for Grotius, which is the state of being in war or intention of such. While Grotius stated *“For so are Spies used, yet it is held lawful, by the general Consent of Nations,”* he was clearly discussing the lawfulness of such general consent

⁵¹ Hugo Grotius, **The Rights of War and Peaces**, Book 3, Knud Haakonssen (ed.) Liberty Fund, (2005), 1295.

⁵² Hugo Grotius, **On the Law of War and Peace**, A.C. Campbell, Batoche Books, (2001) 289.

in the case of being in a state of war. Additionally, he made this explanation and discussed the topic under Chapter 4 titled as “*On the Right of Killing an Enemy in Lawful War and Committing Other Acts of Hostility*”. In other words, Grotius discussed espionage activities conducted during a time of war and categorized such activities as acts of lawful hostility. Therefore, Grotius considered lawful espionage activities during a time of war, but remained quiet for peacetime espionage activities and under which circumstances employing spies and conducting espionage activities can be perceived as lawful and just.

To this end, espionage activities and spying in times of war are regulated at an international level. There is little doubt whether these activities are subject to any kind of sanctions. However, legality and consequences of peacetime espionage activities is still controversial.

b) Legality of Peacetime Espionage Activities

According to Falk, “traditional international law is remarkably oblivious to the peacetime practice of espionage. As for the Radsan, espionage is operating in a sort of legal twilight.”⁵³ Leading treatises overlook espionage altogether or contain a perfunctory paragraph that defines a spy and describes his hapless fate in the event of capture. And yet espionage has always played a prominent role in international relations.⁵⁴ This statement indicates two points; first, there is not any rule or principle proposed by traditional international law. To illustrate, the doctrine - called the *Lotus Principle*- laid down by the Permanent Court of International Justice in the *Lotus* case, underlines that restrictions upon states cannot be presumed. In the absence of prohibitive rules, each state is free to adopt any approach or act accordingly.⁵⁵ Therefore, it is proposed that espionage is an area, where there is no prohibitive applicable law. *Non liquet* is the legal terminology used to describe this situation. However, we should emphasize that although *Lotus Principle* represent general

⁵³ A. John Radsan, ‘*The Unresolved Equation of Espionage...*’, 595.

⁵⁴ Richard A Falk, “Forward,” in Roland J. Stranger (ed), *Essays on Espionage and International Law* Ohio State University Press, (1962) 107.

⁵⁵ **PCIJ**, The Case of the S.S. *Lotus*, (France vs. Turkey) Series A. No. 10, (1927) accessed http://www.icj-cij.org/pcij/serie_A/A_10/30_Lotus_Arret.pdf

attitude towards peacetime espionage operations, this principle became questionable with regard to peacetime cyberespionage operations. Deeks explained this activity as international law agnosticism and stressed that we are experiencing a shift from agnosticism as a result of Snowden revelations.⁵⁶

In this regard, state practices⁵⁷ creating customary international law restricting such activities, are emerging on the one hand and legal documents other hand soft law is being at international and regional level (as it is the case in EU).

(1) Customary International Law and Espionage

In the early years of international law, customary law was the primary tool of creating norms, which gave treaties a secondary importance.⁵⁸ Despite the fact that it had to leave its prestigious prevailing status to law of treaties, considering international law has never been off the table.⁵⁹ In terms of the creation of a customary international law, there is evidence supporting peacetime espionage activities allowed between states. According to Article 38 of the ICJ Statute⁶⁰, the court shall follow and apply the below mentioned sources to decide disputes in accordance with international law;

- a. international conventions, whether general or particular, establish rules expressly recognized by the contesting states;
- b. ***international custom, as evidence of a general practice accepted as law***;
- c. the general principles of law recognized by civilized nations;
- d. subject to the provisions of Article 59, judicial decisions and the teachings of the most highly qualified publicists of the various nations, as subsidiary means for the determination of rules of law.

⁵⁶ Daniel Bodansky, Non Liqueur, **Max Planck Encyclopedia of Public International Law**, (2006)

⁵⁷ Infra p. 33. "We exemplify several incidents and operations, constituting a legal base for State practice in creation of customary international law". Infra p. 48 ff. "We exemplify domestic regulations constituting a *opinio juris* towards creation of customary international law for restricting cyberespionage operations."

⁵⁸ Akif Emre Öktem, **Uluslararası Hukuk**, Beta, (2013), 511.

⁵⁹ Ibid.

⁶⁰ **Statute of International Court of Justice**, art. 38, <http://www.icj-cij.org/documents/?p1=4&p2=2>

The Statue of International Court of Justice defines international custom as “evidence of a general practice accepted as law.”⁶¹ It can be said that milestones of the process of customary international law acquiring its contemporary basis of today are ICJ’s North Sea Continental Shelf decision and the 1986 Nicaragua decision.⁶² Although they have different aspects and dimensions, basically they defined and clarified the connections and relationship between, two fundamental sources of the international law, treaty and tradition.⁶³ According to the ICJ’s judgment on North Sea Continental Shelf case⁶⁴ for creation of a customary international law there are two distinctive elements as *state practice* and *opinio juris*. Similarly in the *Libya/Malta* case, ICJ stated that founding elements of customary law is “actual practice and *opinio juris* of states.”⁶⁵ While state practice should be general and consistent practice, *opinio juris* should be a “belief that a state activity is legally obligatory.”⁶⁶ Concerning this, while countries were signing the UN Charter at the San Francisco Conference, none of them believed that Article 2 and Article 51 included prohibition on peacetime espionage activities.⁶⁷ Thus, there was not an *opinio juris* at that time, but there was *state practice* providing evidence for supporting and allowing peacetime intelligence gathering activities. Nevertheless, inclination towards regulating peacetime espionage activities became a dominant trend at the end of the Cold War.

The circumstances inherent to international relations and perceptions towards international law changed during the Cold War era. On one hand, states persisted in conducting peacetime espionage activities, however on the other hand, states condemned other states which conducted espionage and looked for opportunities to retaliate. To illustrate, there was a general and persistent state practice for conducting a reconnaissance flight in so-called peacetime during the Cold War period. This period was dominated by countless reconnaissance flights conducted between competing powers. Whenever a reconnaissance flight was discovered, the targeted state has always reacted against this activity, declared this act as a violation of sovereignty and

⁶¹ Ibid, art. 38 (1) (b)

⁶² ICJ, Military and Paramilitary Activities in and Against Nicaragua (Nicaragua vs. US) 1986

⁶³ Akif Emre Öktem, *Uluslararası Teamül...*, 514

⁶⁴ North Sea Continental Shelf Case (Germany v. Denmark; Germany v. Netherland) (1969) 75 <http://www.icj-cij.org/docket/files/52/5563.pdf>

⁶⁵ Case Concerning The Continental Shelf (Libyan Arab Jamahiriya vs Malta) (1985) 29 <http://www.icj-cij.org/docket/files/68/6415.pdf> accessed 27 July 2015.

⁶⁶ Malcolm N. Shaw, *International Law*, Cambridge 6th edition, (2008) 84; O. Elias, ‘The Nature of the Subjective Element in Customary International Law’, 44 ICLQ, 1995, 501.

⁶⁷ John Yoo, ‘Counterintuitive: Intelligence Operations and International Law’ 28 MJIL, (2006) 628.

territorial integrity and accused the other state of conducting espionage. Regarding the norm generation process of international law, *opinio juris* and *state practice* has evolved and developed for years in order to propose an international treaty. Having said that, the Treaty on Open Skies, which was signed in 1992, and put into force in January 2002, established “the regime, to be known as the Open Skies regime, for the conduct of observation flights by States’ Parties over the territories of other States’ Parties.”⁶⁸ This regime was designed to be an instrument for confidence building between states. Pursuant to the treaty, 34 signatory parties can conduct unarmed observation flights over entire territories of another state. It should be noted that this final document was an outcome of Cold War experiences, especially practices, incidents and allegations regarding reconnaissance flights between US and Russia.

The most effective solution that will be implemented in the future is international cooperation and treaties.⁶⁹ As for a creation of custom in terms of cyberespionage or cyber attacks we may recall how they occur. First, the actions of states turn into recurrent practices, then the role of the custom is constituted by adding legal awareness to these behavioral patterns.⁷⁰ Likewise, an analogy can be established between cyberespionage and reconnaissance flights. States are irritated due to being targeted for cyberespionage, however they are not inclined to consent rules and principles regulating cyberespionage at the tip of such activities.

(2) Principles of International Law and Espionage

International legal scholars have consensus on the fact that peacetime espionage activities violate the principle of territorial integrity, sovereign equality, non-intervention and peaceful cooperation of states. According to Wright, peacetime espionage operations are illegal on the legal basis of showing “to respect the territorial integrity and political independence of other states” and such activities constitute an

⁶⁸ Treaty on Open Skies, art. 1/1, Entered into force: 1 January 2002,

http://disarmament.un.org/treaties/t/open_skies Turkey is one of party States signed the Treaty at Helsinki on 24 March 1992

⁶⁹ Arquilla, John. “Cyberwar Is Already Upon Us” Foreign Policy. N.p., 27 February 2012, http://www.foreignpolicy.com/articles/2012/02/27/cyberwar_is_already_upon_us

⁷⁰ Akif Emre Öktem, *Uluslararası Teamül...*, 521

intervention which “invades the territorial integrity and denies the political independence of another state.”⁷¹

The Montevideo Convention⁷² treaty discusses the definition and rights of statehood, and has provisions on the principles of territorial integrity and non-intervention. According to Article 8 of the Convention, “*no state has the right to intervene in the internal or external affairs of another*.” Article 11 of the Convention states the principle of territorial integrity as, “*the territory of a state is inviolable and may not be the object of military occupation nor of other measures of force imposed by another state directly or indirectly or for any motive whatever even temporarily.*”

Article 4 of the Convention underlined the sovereign equality by:

“States are juridically equal, enjoy the same rights, and have equal capacity in their exercise. The rights of each one do not depend upon the power which it possesses to assure its exercise, but upon the simple fact of its existence as a person under international law.”

The Montevideo Convention set out those principles as a right of and responsibility upon every state that should be respected and act accordingly. Similarly, the Charter of the United Nations has similar provisions. Article 2 of the Charter states that;

The Organization and its Members, in pursuit of the Purposes stated in Article 1 [Purposes of the United Nations], shall act in accordance with the following Principles.

1. *The Organization is **based on the principle of sovereign equality** of all its Members.*
2. *All Members, in order to ensure to all of them the rights and benefits resulting from membership, shall fulfil in good faith the obligations assumed by them in accordance with the present Charter.*
3. *All Members shall settle their international disputes by peaceful means in such a manner that international peace and security, and justice, are not endangered.*

⁷¹ Quincy Wright, ‘**Espionage and the Doctrine of Non-Intervention in Internal Affairs**’ Essays on Espionage and International Law OHIO State University Press, (2008) 4.

⁷² Montevideo Convention, signed December 26, 1933, entered into force on December 26, 1934 accessed http://avalon.law.yale.edu/20th_century/intam03.asp

4. *All Members shall refrain in their international relations from the **threat or use of force against the territorial integrity or political independence** of any state, or in any other manner inconsistent with the Purposes of the United Nations.*
5. *All Members shall give the United Nations every assistance in any action it takes in accordance with the present Charter, and shall refrain from giving assistance to any state against which the United Nations is taking preventive or enforcement action.*
6. *The Organization shall ensure that states which are not Members of the United Nations act in accordance with these Principles so far as may be necessary for the maintenance of international peace and security.*
7. *Nothing contained in the present Charter shall authorize the United Nations to intervene in matters which are essentially within the domestic jurisdiction of any state or shall require the Members to submit such matters to settlement under the present Charter; but this principle shall not prejudice the application of enforcement measures under Chapter VII.*

According to Kindred *et al*, “the dual concepts of sovereignty and equality are the cornerstone of public international law. Being sovereign and equal to others, a state has certain rights and corresponding duties. The rights include exclusive control over its territory, its permanent population [...] and other aspects of its domestic affairs. The necessary corollary is that there is a duty not to intervene overtly or covertly in the affairs of other states and thus not to interfere with their exclusive domestic jurisdiction.”⁷³

Similarly, Jonathan and Kovar stated that “l’espionnage fait appel à des moyens qui en eux-mêmes constituent des actes contraires au droit international.”⁷⁴ In other words, peacetime espionage activities violate international law because such espionage uses means or tools which themselves constitute acts contrary to international law. Additionally, it is acknowledged by Wright that “In time of peace, however, espionage and, in fact, any penetration of the territory of a state by agents of another state in violation of the local law, is also a violation of the rule of international

⁷³ H.M. Kindred, **International Law**, Chiefly as Interpreted and Applied in Canada (5th ed., 1993), 16.

⁷⁴ Gérard Cohen-Jonathan and Robert Kovar, **L’espionnage en Temps de Paix**, AFDIA 1960 Volume 6 N.1, 246.

law imposing a duty upon states to respect the territorial integrity and political independence of other states.”⁷⁵

Recently, in 2007, the Canadian Federal Court issued an exceptionally restrictive decision on cross-border intelligence activities. The Canadian Security Intelligence Service applied to the federal court for a warrant relating to investigative activities outside Canada pursuant to the Canadian Security Intelligence Service Act. The federal court interpreted domestic law in the light of international law norms and principles. Therefore, the federal court ruled that “binding customary principles of international law, which prohibit interference with the sovereignty and domestic affairs of other states. The intrusive activities clearly impinge upon the above-mentioned principles of territorial sovereign equality and non-intervention and are likely to violate the laws of the jurisdiction where the investigative activities are to occur. By authorizing such activities, the warrant would therefore be authorizing activities that are inconsistent with and likely to breach the binding customary principles of territorial sovereign equality and non-intervention, by the comity of nations. These prohibitive rules of customary international law have evolved to protect the sovereignty of nation states against interference from other states. Extraterritorial jurisdiction, prescriptive, enforcement or adjudicative, exists under international law and is subject to the strict limits under international law based on sovereign equality, non-intervention and the territorial principle.”⁷⁶

Violation of the above-mentioned principles of international law constitute a base for international responsibility of states. This responsibility is clearly stated by the United Nations General Assembly, as “*states are internationally responsible for the activities of their intelligence services and agents, and any private contractors they engage, regardless of where these activities take place and who the victim of internationally wrongful conduct is.*”⁷⁷ Additionally, the Montreux document extends this responsibility upon private contractors that perform intelligence functions on behalf of states.⁷⁸

⁷⁵ Q. Wright, “Espionage and the Doctrine of Non-Intervention in Internal Affairs” (1962) in R. Stanger ed., **Essays on Espionage and International Law**, 12.

⁷⁶ Canadian Security Intelligence Service Act (Re) (F.C.), 2008 FC 301, [2008] 4 F.C.R. 230 <http://reports.fja-cmf.gc.ca/eng/2008/2008fc301.pdf> accessed 22 June 2015.

⁷⁷ UNGA, “Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism” A/HRC/14/46 p.13 <http://www2.ohchr.org/english/bodies/hrcouncil/docs/14session/A.HRC.14.46.pdf>

⁷⁸ ICRC, **The Montreux Document on Private Military and Security Companies**, 2009, pp. 12, 35.

In this sense, from the 1945 signing of the UN Treaty to the end of Cold War in 1990, states have diplomatically, economically and sometimes militarily responded to peacetime espionage activities. The Open Skies Treaty is a good example of when states prefer regulated and foreknown activities. Alternatively, the Canadian Federal Court has underlined principles, founded in the Montevideo Convention and UN Charter, which may be used as a legal basis for illegality of peacetime espionage activities. Therefore, peacetime espionage activities can constitute as an international responsibility of attacker States.

B. Cyberespionage and Changing Features of Espionage

1. Defining Cyberespionage

Cyberespionage is defined by Oxford Dictionary as the use of computer networks to gain illicit access to confidential information, typically information held by a government or other organization.⁷⁹ Cyberespionage is defined by Tallinn Manual, under Rule 66, narrowly as “any act undertaken clandestinely or under false pretenses that uses cyber capabilities to gather or attempt to gather information with the intention of communicating it to the opposing party and that act must occur in a territory controlled by a party to the conflict.”⁸⁰ According to the UK Parliament, cyberespionage is a kind of cyber attacks that “have aimed to steal sensitive information and data from financial, government and utilities infrastructure targets.”⁸¹ Similarly, Cyber Security Strategy documents of Germany state, “cyber attacks directed against the confidentiality of an IT system, which are launched or managed by foreign intelligence services, are called cyberespionage.”⁸² These attacks can target intellectual property or sensitive/secret information about organizations or governments.

Technically speaking, within this research, computer network operations (CNO) are defined as an umbrella term which consists of computer network attacks (CNA),

⁷⁹ Oxford English Dictionary, Oxford University Press, 7, (2013) 234.

⁸⁰ Michael N. Schmidt (ed.), **Tallinn Manual on The International Law Applicable to Cyber Warfare**, Cambridge (2013) 158.

⁸¹ UK Houses of Parliament, **Cyber Security in the UK**, (2011) 2.

⁸² Federal Ministry of Interior, ‘**Cyber Security Strategy for Germany**’, (2011), 14.

computer network defense (CND) and computer network exploitation (CNE). Definitions given in the Dictionary of Military and Associated Terms are adopted within this research.⁸³ According to the Dictionary, CNA or cyber attack, refers to “actions taken via computer networks to disrupt, deny, degrade, or destroy information residing in computers and computer networks, or the computers and networks themselves.”⁸⁴ CND refers to “actions to protect information systems and computer networks, and to monitor for, analyze, detect, and respond to unauthorized activity within those networks.”⁸⁵ CNE concerns “actions to gather data from target information systems or networks or map target networks for future CNA operations.”⁸⁶

Herein after, cyberespionage will be used in the context of Computer Network Exploitation (CNE). In other words, CNE “refers to operations conducted through the use of computer networks to gather data from target or adversary automated information systems or networks.”⁸⁷ It is also defined as cyber exploitation, “a term that refers to the penetration of adversary computers and networks to obtain information for intelligence purposes.”⁸⁸ The International Group of Experts distinguished cyberespionage from CNE and cyber reconnaissance regarding its theatre of operation. While CNE occurs from beyond enemy territory, cyberespionage is conducted within enemy territory. However, such distinction is not practical, because technically it is difficult to make such distinction and it is easier to conduct such activities beyond enemy territory without jeopardizing any individual likewise espionage activities. Secondly, traditionally defined legal consequences attached to spies who are operating within enemy territory cannot be applicable to personnel conducting cyber exploitation or cyberespionage from beyond enemy territory. Therefore, at the end of this chapter it will become obvious that there is no technical difference between CNE and cyberespionage; it is only a terminological difference and there is no need for such a differentiation.

⁸³ U.S. Department of Defense, **Dictionary of Military and Associated Terms**, joint publication 1–02, April 12, 2001 (as amended through August 26, 2008), p. 113.

⁸⁴ Ibid

⁸⁵ Ibid

⁸⁶ Ibid

⁸⁷ William A. Owens, Kenneth W. Dam, and Herbert S. Lin, (Editors), **Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities**, National Academy of Sciences, 2009, s.161.

⁸⁸ Ibid, s. ix

Legally speaking, cyberespionage operations are a kind of cyber attack which targets commercial assets, trade secrets and provides unauthorized access to computers and networks. Therefore, those operations are punishable through criminal, civil and administrative channels.

2. Changing Features of Espionage

From the Cold War period to today, the purposes, targets, actors of espionage and the methods applied for espionage have been fundamentally changed. Targets of espionage activities have changed from military to economic and industrial secrets, to gain economic advantage against other states. Similarly, espionage activities are no longer conducted only by states and states' entities, but by a proliferation of especially civilian actors. Finally, methods and means for gathering intelligence have shifted from human intelligence to signal intelligence.

Additionally, the Internet has become a theater of conflicts and attacks between states. According to a report presented to the French Senate, *“à l'Internet est devenue facteur de vulnérabilité, si bien que le réseau est maintenant le théâtre de véritables attaques qui peuvent provenir d'Etats, d'organisations ou même d'individus: espionnage économique, déstabilisation, sabotage d'infrastructures critiques.”*⁸⁹ In other words, the Internet has become a factor of vulnerability, so that the network is now the scene of real attacks such as economic espionage, destabilization, and sabotage to critical infrastructure that can come from states, organizations or individuals. Therefore, it is acknowledged that dual use of the Internet and deployment of technology on espionage activities has accelerated as a result of the above-mentioned change or shift.

⁸⁹ Catherine Morin-Desailly, Rapport D'information fait au nom de la mission commune d'information Nouveau rôle et nouvelle stratégie pour l'Union européenne dans la gouvernance mondiale de l'Internet, 8 July 2014, Rapports Parlementaires No: 696, 307. <http://www.senat.fr/rap/r13-696-1/r13-696-11.pdf>

a) New Purpose and Targets

For centuries, wartime and peacetime espionage activities have been conducted for the purpose of gaining a military advantage. Spies infiltrated an army to disclose military secrets, collect information about size, capacity, and weapons of that army, reveal military plans, and sometimes tempt soldiers to revolt. Nowadays, although espionage activities with the purpose of gaining military advantage are still conducted, economic and industrial espionage activities have reached a wider scope of application.

Rapid developments in the areas of communication services and computer technologies, and with the digitalization of vast pieces of information, have assisted in the proliferation of economic and industrial espionage activities. Furthermore, not only state-owned critical infrastructures and networks, but also private networks and databases of companies are increasingly being targeted and becoming vulnerable to state-backed economic cyberespionage operations.⁹⁰ In 2009, a U.K. government security document revealed the shift in intelligence gathering operations and targets. “In the past, espionage activity was typically directed towards obtaining political and military intelligence. In today’s high-tech world, the intelligence requirements of a number of countries now include new communications technologies, IT, genetics, aviation, lasers, optics, electronics and many other fields. Intelligence services, therefore, are targeting commercial enterprises far more than in the past.”⁹¹ Thus, intelligence gathering activities are nowadays more about collecting financial and economic data, and business secrets and plans. The trend is shifting from military to commercial espionage, and human intelligence to signal intelligence.

Similarly, during her testimony before the U.S.-China Economic and Security Review Commission, FireEye, Inc. Threat Intelligence Department Manager Jen Weedon mentioned that several strategic sectors have been targeted by foreign actors. (See. Table 1)

⁹⁰ Craig Mundie, Speaking on The Future of Technology Conference Columbia University School of International and Public Affairs (08 November 2013) <http://www.youtube.com/watch?v=tnojfzVv7eA> accessed on 22 June 2015.

⁹¹ Sean Rayment, ‘Britain under attack from 20 foreign spy agencies including France and Germany’ (The Telegraph, 07 February 2009) accessed 22 June 2015.

Table 0-1: China-Based APT Group's Targeting of Strategic Emerging Industries⁹²

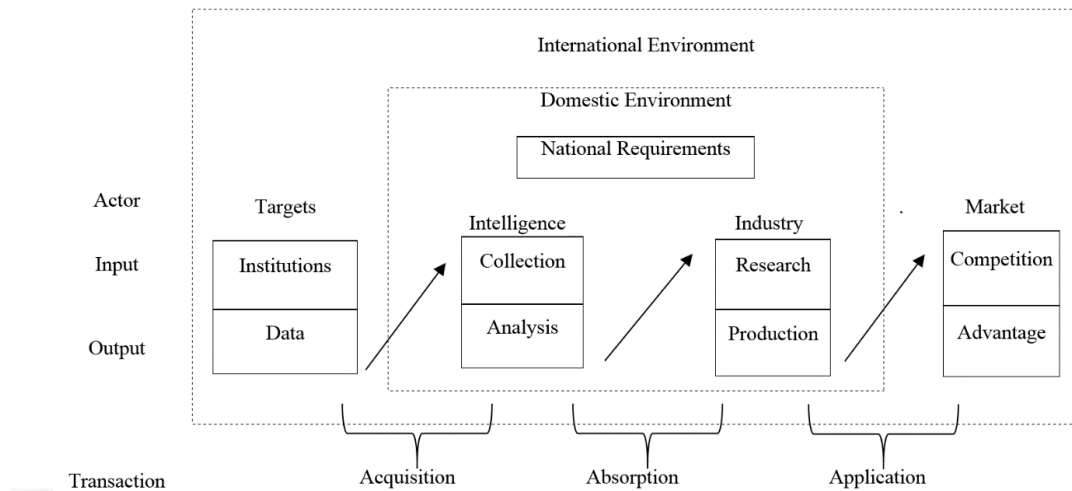
Strategic Emerging Industry	Number of China-Based APT Groups Targeting This Strategic Emerging Industry
Clean Energy Technology	3
Next-Generation IT	19
Biotechnology	6
High-End Equipment Manufacturing	22
Alternative Energy	7
New Materials	12
New Energy Vehicles	6

According to Weedon, along with the sectors mentioned above, electronics, telecommunications, robotics, data services, pharmaceuticals, mobile phone services, satellite communications and imagery, and business application software based sectors were also being targeted.⁹³ It is significant to collect highly sensitive and valuable information, but what is more significant is to apply them properly in market and industry. In particular, economic espionage has several stages from collection to innovation. The below model of espionage effectiveness provides a comprehensive illustration of those stages.⁹⁴ Collected information and data has to be analyzed and categorized in accordance with the domestic requirements and needs. At the later stage, industry will adopt those outputs and will turn into a product. These products will enable the domestic sector and products to gain competitive advantages in the international market against other domestic markets and like products.

⁹² U.S.-China Economic and Security Review Commission, **Hearing on Commercial Cyber Espionage and Barriers to Digital Trade in China**, testimony of Jen Weedon, (2015) 4. accessed <http://www.uscc.gov/sites/default/files/Weedon%20Testimony.pdf>

⁹³ Ibid. s.4-8.

⁹⁴ Jon R. Lindsay, Tai Ming Cheung, Derek S. Reveron (eds), **China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain**, Oxford University Press, (2015), 54.

Table 0-2: Economic and Industrial Cyberespionage Circle

Within the light of the foregoing, the focal point of economic cyberespionage activities and security technologies becomes company data, which includes personal data, confidential data and intellectual property.

b) New Methods and Means

The intelligence gathering methods and means have radically changed in the last two decades. States have always been in pursuit of adopting new approaches and improving their electronic capabilities to collect better information from targeted states. Throughout the 1990's and early 2000's, one phase cyber attacks (such as DDOS), malwares such as viruses, worms, and Trojan horses, were commonly applied. Later on, there has been the creation of tailored cyber weapons. According to Rid and McBurney, a cyber weapon is “a computer code that is used, or designed to be used, with the aim of threatening or causing physical, functional, or mental harm to structures, systems, or living beings.”⁹⁵

The Stuxnet is the first-known malicious computer worm tailored to target specific platforms such as PLC's (programmable logic controllers) and SCADA (Supervisory Control and Data Acquisition) systems. Stuxnet is a “cyber weapon

⁹⁵ Thomas Rid and Peter McBurney, **Cyber-Weapons**, The RUSI Journal, 157:1, (2012) 7.; Thomas Rid, **Cyber War Will Not Take Place**, Oxford University Press, (2013) 37.

created and deployed with the intent of degrading, disrupting, and destroying a specific information system.”⁹⁶ This malware was designed to collect information on industrial systems of Iranian nuclear facilities including either the Bushehr Nuclear Power Plant or the Natanz nuclear facility, and cause the fast-spinning centrifuges to tear themselves apart within the targeted uranium enrichment facility at Natanz. Three other major espionage tools have also been discovered that seem to link to Stuxnet. The pioneer of cyberespionage, Gauss, discovered in 2012, was designed to be a complex cyber weapon which steals passwords and other data. The second was Flame, which is able to take over drivers, screenshots, Skype, and Bluetooth functions, and can monitor a computer’s keyboard and network traffic. And the third was the DuQu, which operates in the background and collects data for years.

APT is one of the most significant cyber weapon which is applied commonly for conducting cyberespionage operations.⁹⁷ It stands for Advanced Persistent Threat, and is a sophisticated technique used by hackers to extract large amounts of data from targeted industries over a long period of time.⁹⁸ According to Cole, key terms that describes the APT are “stealthy, targeted, adaptive and data focused.”⁹⁹ This type of attack is well-tailored for targeted sector or computer networks and it has advanced capabilities to extract data and compromise the targeted entity. Such an adversary can spend years to exfiltrate the documents at a targeted entity without being spotted. According to the recent white paper published by McAfee, “APT differ from common botnets and malware type attacks because they target strategic users to gain undetected access to key assets.”¹⁰⁰

Throughout the history of espionage, none of the states accepted to regulate and restrict the use of tools and means of espionage activities. However, nowadays, commonly used tools and means for espionage activities have dual-use characteristics.

⁹⁶ Emilio Iasiello, **Are Cyber Weapons Effective Military Tools?**, Military and Strategic Affairs, Vol.7, No. 1, (2015) 32.

⁹⁷ Paul Taylor, **Industrial Espionage Cyber Style**, Financial Times, 8 November 2011 “Generally the term is used to designate a cybercrime category directed at business and political targets. Typically APTs require a high degree of stealthiness and the attack takes place over a prolonged period of time. Often they appear motivated by factors beyond immediate financial gain, and compromised systems continue to be of service even after key systems have been breached and initial goals reached. More often than not, the target organisation is unaware of the attack until alerted by a third party.”

⁹⁸ Mandiant, “**APT1: Exposing One of China’s Cyber Espionage Units**,” February 2013.

⁹⁹ Eric Cole, **Advanced Persistent Threat: Understanding the Danger and How to Protect Your Organization**, Elsevier, (2013) 20-21.

¹⁰⁰ McAfee, **Combating Advanced Persistent Threats**, (2011) accessed <http://www.mcafee.com/us/resources/white-papers/wp-combat-advanced-persist-threats.pdf>

These tools and means can be used to either protect citizens and digital assets or target individuals and steal digital assets and trade secrets. For instance, the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies¹⁰¹ is an international agreement designed to control the export of dual-use technologies. The agreement creates a special regime for controlling and regulating the export of guns, landmines and other weapons and their components. In December 2013, the list of controlled technologies was amended to include intrusion and surveillance items. According to the Wassenaar Agreement, “intrusion software” is defined as:

“Software” specially designed or modified to avoid detection by ‘monitoring tools’, or to defeat ‘protective countermeasures’, of a computer or network capable device, and performing any of the following:

- a. The extraction of data or information, from a computer or network capable device, or the modification of system or user data; or*
- b. The modification of the standard execution path of a program or process in order to allow the execution of externally provided instructions.*

The scope of restrictions has been widened with recent amendments and the below mentioned categories become subject to export control:

- 4. A. 5. Systems, equipment, and components therefor, specially designed or modified for the generation, operation or delivery of, or communication with, "intrusion software".*
- 4. D. 4. "Software" specially designed or modified for the generation, operation or delivery of, or communication with, "intrusion software".*
- 4. E. 1. c "Technology" for the "development" of "intrusion software".*
- 4. D. 1. a "Software" specially designed or modified for the "development" or "production" of equipment or "software" specified by 4.A. or 4.D.*
- 4. E. 1 "Technology" according to the General Technology Note, for the "development", "production" or "use" of equipment or "software" specified by 4.A. or 4.D.*

IP network surveillance systems

¹⁰¹ **The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies**, accepted on 11-12 July 1996, accessed: <http://www.wassenaar.org/wp-content/uploads/2015/08/WA-LIST-15-1-2015-List-of-DU-Goods-and-Technologies-and-Munitions-List.pdf>

5. A. 1. j. *IP network communications surveillance systems or equipment, and specially designed components therefore, having all of the following:*

1. *Performing all of the following on a carrier class IP network (e.g., national grade IP backbone):*

a. *Analysis at the application layer (e.g., Layer 7 of Open Systems Interconnection (OSI) model (ISO/IEC 7498-1));*

b. ***Extraction of selected metadata and application content (e.g., voice, video, messages, attachments); and***

c. ***Indexing of extracted data; and***

2. *Being specially designed to carry out all of the following:*

a. *Execution of searches on the basis of 'hard selectors'; and*

b. *Mapping of the relational network of an individual or of a group of people.*

ML11. *Electronic equipment, "spacecraft" and components, not specified elsewhere on the Munitions List, as follows:*

a. *Electronic equipment specially designed for military use and specially designed components therefor;*

Note ML11.a. includes:

c. ***Electronic systems or equipment, designed either for surveillance and monitoring of the electromagnetic spectrum for military intelligence or security purposes or for counteracting such surveillance and monitoring;***

i. ***Digital demodulators specially designed for signals intelligence;***

Although the agreement is not legally binding and signatory, countries should implement the changes in the agreement into their domestic legal systems; 31 of 41 countries have implemented the changes. Some scholars argued that this will hamper the efforts of oppressive regimes to monitor and profile their citizens. Other scholars opposed the changes that cover tools which enable states to improve their cybersecurity¹⁰² level. In any case, it reflects a tendency towards regulating cyber intrusion tools and later cyberespionage.

¹⁰² European Commission, **Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace**, 52013JC0001, (2013), "Cyber-security commonly refers to the safeguards and actions that can be used to protect the cyber domain, both in the civilian and military fields, from those threats that are associated with or that may harm its interdependent networks and information infrastructure. Cyber-security strives to preserve the availability and integrity of the networks and infrastructure and the confidentiality of the information contained therein."

c) New Actors and Incidents

Every state has authorized intelligent authorities and laws regulating foreign intelligence gathering.¹⁰³ In this regard, every state is trying to maintain optimum balance between national security needs and effective functioning of law enforcement authorities on the one hand, and right to privacy and personal data protection on the other. As right to privacy and personal data protection begin to be accepted as a part of international human rights and international legal documents relating to human rights, this currently existing balance has needed to be reconsidered and tailored not only by taking into account citizens, but also international society and citizens of other states. Invasive application of technologies and concerns related to that, pave the way for several high courts, such as the U.S Supreme Court and Canadian Supreme Court, to decide on restricting further the activities of foreign intelligence gathering. However, it is important to note that very foundation of those decision is to protect the basic rights of citizens and respect for international rules and principles.

Along with perpetrators of organized crime, hired-hand attackers¹⁰⁴, as well as industrial competitors or hacker groups such as Anonymous or RedHack, cyber-espionage attacks can come from national intelligence services.¹⁰⁵ SurfWatch Labs revealed the top trending cyberespionage actors in 2016. “Group 27, which is a cyber-espionage group linked with the Seven Pointed Dagger malware campaign that utilizes a remote access Trojan known as Trochilus, is the top trending espionage actor in 2016.”¹⁰⁶ There are also governmental agencies included in the list, such as the NSA, GCHQ and Russian Intelligence Agency.

¹⁰³ Peter Roudik, **Foreign Intelligence Gathering Laws**, The Law Library of Congress, December 2014, accessed <https://www.loc.gov/law/help/foreign-intelligence-gathering/foreign-intelligence-gathering.pdf>

¹⁰⁴ James Sperling (ed) **Handbook of Governance and Security**, Edward Elgar Publishing, (2014) 343.

¹⁰⁵ Ellen Messmer, ‘Cyber-espionage Attacks Threaten Corporate Data in New Unrelenting ways’ Network World, (2011) accessed 22 June 2015.

¹⁰⁶ Matt Lichtfuss, Cyber-Espionage Making Headlines Over Past Couple Weeks, SurfWatchLabs (2016), <https://blog.surfwatchlabs.com/2016/06/16/cyber-espionage-making-headlines-over-past-couple-weeks/>

Table 0-3: Top Trending Cyberespionage Actors in 2016

Group 27	Gaza Hacker Team
Scarlet Mimic	SandWorm Team
Poseidon APT Group	Russian Intelligence Agency
Firas Dardar	Codosa Team
Pawn Storm	Ahmad Umar Agha
APT 28	Peter Romar
GCHQ	Lazarus Group
Suckfly Group	NSA

It is acknowledged that activities of intelligent services are far more capable than other actors. Please be informed that the incidents and operations mentioned here are not pointing fingers or accusing any nation and its officials. These incidents are strong proof that states can perform such activities, although they are irritated from being targeted.¹⁰⁷ However, the aim is to show the fact that cyberespionage activities are commonly deployed, supported or backed by officials. As it is acknowledged under Tallinn Manual that “the mere fact that a cyber operation has been launched or otherwise originates from governmental cyber infrastructure is not sufficient evidence for attributing the operation to that state, but it is an indication that the state in question is associated with the operation.”¹⁰⁸

(1) Actors and Incidents Relating to China

In 2009, scholars from the University of Toronto and University of Cambridge published a report revealing field-based research and findings about the malware-based cyberespionage network named GhostNet.¹⁰⁹ According to the findings, this malware-based cyberespionage network infiltrated 1,295 computers in 103 countries. Scholars underlined that “up to 30 percent of the infected computers are considered high-value targets and include computers located at ministries of foreign affairs,

¹⁰⁷ See for some cases of industrial espionage and/or competitive intelligence which have been described in the press or in the relevant literature: EU Parliament, Report on the Existence of A Global System for the Interception of Private and Commercial Communications (ECHELON interception system) (2001/2098(INI))

¹⁰⁸ Michael N. Schmidt (ed.), **Tallinn Manual on The International Law Applicable to Cyber Warfare**, Cambridge (2013) 34.

¹⁰⁹ Ron Deibert and Rafal Rohozinski, ‘**Tracking GhostNet: Investigating a Cyber Espionage Network**’ (University of Toronto, Munk Centre for International Studies at Trinity College, 2009) <http://www.nsi.org/pdf/reports/Cyber%20Espionage%20Network.pdf> accessed on 22 June 2015.

embassies, international organizations, news media, and NGOs.”¹¹⁰ In 2010, David Drummond, Google’s Corporate Development and Chief Legal Officer, explained that highly sophisticated attacks, labelled as “Operation Aurora” by McAfee, targeting the Google infrastructure by China to infiltrate corporate properties.¹¹¹ However, this attack not only targeted Google. The Google investigation team discovered that at least twenty large companies including Yahoo, Symantec, Adobe, Northrop Grumman and Dow Chemical had also been among the targets.¹¹²

Technically named as Advanced Persistent Threats (APT), these threats are gaining access to privileged systems and maintaining their access until they are disclosed. GhostNet and Operation Aurora were both designed as advanced persistent threats. Along with GhostNet and Operation Aurora, in 2011, McAfee attributed a cyberattack to China they named as “Night Dragon” and stated in a report that attackers had exfiltrated computer systems of global oil, energy, and petrochemical companies.¹¹³ The “Night Dragon” attack caused the companies a loss of “proprietary operations and project-financing information that can make or break multibillion dollar deals.”¹¹⁴

Although the activities mentioned above have attribution problems, a report published by Mandiant in 2013 established the attribution link. According to the report, a special unit of the Chinese People’s Liberation Army (PLA) was targeting financial and industrial companies for large-scale thefts of intellectual property or industrial and economic espionage. The report underlined the fact that APT malware has been active since 2006, and compromises 141 companies in 20 major industries.¹¹⁵ Table I-4 illustrates other APT types attacks supposed to be originated China.

¹¹⁰ Ibid. 40.

¹¹¹ David Drummond, ‘A new approach to China’ (12 January 2010) <http://googleblog.blogspot.co.uk/2010/01/new-approach-to-china.html> accessed on 25 June 2015.

¹¹² Ariana Eunjung Cha and Ellen Nakashima, “Google China cyberattack part of vast espionage campaign, experts say” (14 January 2010) <http://www.washingtonpost.com/wp-dyn/content/article/2010/01/13/AR2010011300359.html> accessed on 25 June 2015.

¹¹³ McAfee, ‘Global Energy Cyberattacks: “Night Dragon”’ (10 February 2011) <http://www.mcafee.com/uk/resources/white-papers/wp-global-energy-cyberattacks-night-dragon.pdf> accessed on 25 June 2015.

¹¹⁴ Georger Kurtz, McAfee, Global Energy Cyberattacks: “Night Dragon”, 10 February 2011 <https://blogs.mcafee.com/business/global-energy-industry-hit-in-night-dragon-attacks/>; McAfee, Global Energy Cyberattacks: “Night Dragon”, Report 2011, <http://www.mcafee.com/us/resources/white-papers/wp-global-energy-cyberattacks-night-dragon.pdf>

¹¹⁵ Mandiant, “APT1 Exposing One of China’s Cyber Espionage Units” (18 February 2013) http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf accessed on 25 June 2015.

In 2015, several cyber intelligence research companies revealed that China-based cyber actors have carried out intrusion activities against targets across Southeast Asia, including ASEAN. ThreatConnect, in partnership with Defense Group Inc., published a report that “has attributed the targeted cyberespionage infrastructure activity associated with the Naikon APT group to a specific unit of the PLA.”¹¹⁶ It has been stated that, “Unit 78020 conducts cyberespionage against Southeast Asian military, diplomatic, and economic targets. The targets include government entities in Cambodia, Indonesia, Laos, Malaysia, Myanmar, Nepal, the Philippines, Singapore, Thailand, and Vietnam as well as international bodies such as United Nations Development Program (UNDP) and ASEAN.”¹¹⁷



¹¹⁶ ThreatConnect and Defense Group Inc., **Project Camerashy: Closing the Aperture on China’s Unit 78020**, 2015, accessed <http://www.threatconnect.com/camerashy/>; According to USCC 2015 ANNUAL REPORT; “Naikon is known as affiliated with PLA Unit 78020, the Second Technical Reconnaissance Bureau under the Chengdu Military Region”.

¹¹⁷ Ibid.7 See also, Josh Chin, ‘**Cyber Sleuth Track Hacker to China’s Military**’, The Wall Street Journal, (23 September 2015).

Table 0-4: Publicly Reported Cyberespionage Activities Attributed to China

Name of Attack	Date Identified	Target	Source of Attack
Titan Rain	2003-2006	10 most prominent U.S. defense contractors—including Raytheon, Lockheed Martin, Boeing and Northrop Grumman	Chinese military hackers (According to the SANS Institute)
F-35 JSF	2007-2009	BAE, Lockheed-Martin, Northrop-Grumman	APT compromised non-classified data on F-25, monitored meetings and technical discussions
Operation Aurora	2009-2010	Adobe Systems, Juniper Networks and Rackspace publicly confirmed that they were targeted. According to media reports, Yahoo, Symantec, Northrop Grumman, Morgan Stanley and Dow Chemical were also among the targets.	Series of cyber attacks conducted by a group based in Beijing, China, with ties to the People's Liberation Army. First publicly disclosed by Google on January 12, 2010, in a blogpost
Night Dragon	2009-2011	Multinational firms in oil/energy sector (sensitive internal documents, including proprietary information about oil- and gas-field operations, project financing and bidding documents)	Originated from China according to McAfee
RSA	2010	RSA, Lockheed	Compromise of industry standard RSA SecureID tokens enabled Lockheed intrusion
Nitro	2011	50 companies, including 29 chemical firms and 19 firms mostly in the defense industry; Fortune 100 companies that conduct chemical compound R&D	Symantec identifies author of the attacks and attributes the paternity to Chinese hackers. Attack traced back to single hacker in Hebei province
Operation Beebus	2011	The set of targets cover all aspects of unmanned vehicles, land, air and sea, from research to design to manufacturing of the vehicles and their various subsystems	FireEye Labs has linked the attacks to the China-based Comment Group hacker collective (a prolific actor believed to be affiliated with the Chinese government)
Telvent	2007	Telvent/Schneider Electric: Telvent said the attacker(s) installed malicious software and stole project files related to one of its core offerings — OASyS SCADA — a product that helps energy firms mesh older IT assets with more advanced “smart grid” technologies.	Attributed to China-based Comment Group
QinetiQ	2007	QinetiQ North America (NA) is a world leading defense technology and security company that provides technological equipment such as satellites, drones and software services to the U.S. Special Forces	Chinese hackers belonging to Comment Crew conducted an operation that started in 2009. Hackers compromised at least 151 machines of the company. The attacks lasted around 251 days during which they stole 20 gigabytes of data before being blocked

(2) Actors and Incidents Relating USA

The revelations of Edward Snowden¹¹⁸ about the NSA and other national intelligence services indicated that intelligence organizations are capable of collecting data through electronic means from around the world. The global reach of the Internet enables large scale techniques of surveillance as well as bulk data collection and extraction. It became possible to harvest data from submarines' Internet cables via different interceptors such as UPSTREAM, and QUANTUMISERT.¹¹⁹ However, this global data collection requires a transnational collaboration, because the NSA cannot control the data totally, absolutely and globally by itself. The well-known structure for such collaboration is the 5-Eyes Alliance, 9-Eyes and 14-Eyes programs.¹²⁰ The Five-Eyes Alliance was set up by UKUSA Agreement¹²¹, which gave authorization to the United States National Security Agency (NSA), the United Kingdom's Government Communications Headquarters (GCHQ), the Communications Security Establishment Canada (CSEC), the Australian Signals Directorate (ASD), and New Zealand's Government Communications Security Bureau (GCSB) to collect and share signal intelligence.

The signing parties agreed to exchange the products of the following operations relating to foreign communication:

1. collection of traffic
2. acquisition of communication documents and equipment
3. traffic analysis
4. cryptanalysis
5. decryption and translation
6. Acquisition of information regarding communication, organizations, practices, procedures and equipment.¹²²

¹¹⁸ Glenn Greenwald, Ewen MacAskill and Laura Poitras, 'Edward Snowden: the whistleblower behind the NSA surveillance revelations' (Guardian, 11 June 2013) accessed on 22 June 2015.

¹¹⁹ Edward Snowden, UPSTREAM and QUANTUMISERT see more: <https://search.edwardsnowden.com>

¹²⁰ The '9-eyes programme includes U.S., UK, Canada, Australia, New Zealand, Denmark, France, Norway and the Netherlands; the '14-eyes programme includes those countries and also Germany, Belgium, Italy, Spain and Sweden.

¹²¹ UKUSA Agreement, (adopted on 10 May 1955).

https://www.nsa.gov/public_info/declass/ukusa.shtml accessed on 22 June 2015.

¹²² UKUSA COMINT Agreement and Appendices Thereto, (adopted 26 June 1951) https://www.nsa.gov/public_info/_files/ukusa/ukusa_comint_agree.pdf accessed on 22 June 2015.

The NSA is doing nothing but collecting and analyzing data to hand over to national security agencies such as the CIA and FBI. The NSA was authorized to collect foreign intelligence due to national security concerns by the Foreign Intelligence Surveillance Act (FISA).¹²³ Revelations about the NSA indicated that the PRISM surveillance program was designed to collect e-mails, communications, texts and video chats of foreigners.¹²⁴ The main justifications or exceptions granted by law are 1) counter-terrorism, 2) organized crime and 3) national security interests.¹²⁵ Section 702 of the FISA provides legal basis for the collection of “foreign intel information” regarding persons who are “reasonably believed to be located outside of the US.”¹²⁶ Although the NSA’s surveillance program, such as PRISM, ignited debate on privacy and data protection in the U.S. related with human rights and protection mechanisms of the U.S. Constitution, there were other programs like Blarney and Rampart-T that serve the purpose of traditional espionage targeting foreign governments.¹²⁷ It was also revealed that through those programs the NSA could gain access to several diplomatic missions of the EU and the UN Headquarters in New York.¹²⁸ Apart from the international human rights concerns, the Vienna Convention on Diplomatic Relations protects diplomatic communications between capitals and missions whose norms are regarded as a custom accepted by all states. Article 27 of the Convention underlined that “the receiving State shall permit and protect free communication on the part of the mission for all official purposes.”¹²⁹ In this regard, basic tapping into communication of diplomatic premises constitutes a violation of international obligation.

Furthermore, alleged economic espionage activities of the NSA have been disclosed by documents showing that computer networks of Petrobras, the semi-state-owned Brazilian oil company, have been targeted and exfiltrated. Similarly, the Minister of Economy of France, Philippe Lemoine, in his speech during the hearing at

¹²³ Foreign Intelligence Surveillance Act 50 U.S.C. sec. 1881a <http://fas.org/irp/news/2013/06/nsa-sect702.pdf> accessed on 22 June 2015.

¹²⁴ Barton Gellman and Laura Poitras, ‘**U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program**’ (Washington Post, 7 June 2013) accessed on 22 June 2015.

¹²⁵ Oğuz Kaan Pehlivan, **İpin Ucunu Kaçırarak**: NSA, Analyst Journal, December 2013, v.34, 24-25

¹²⁶ Supra 103

¹²⁷ Edward Snowden, RAMPART-A Project Overview, <https://search.edwardsnowden.com/docs/RAMPART-AProjectOverview20140618> accessed on 22 June 2015.

¹²⁸ Laura Poitras, Marcel Rosenbach and Holger Stark, ‘Codename “Apalachee”’: How America Spies on Europe and the UN’ (Der Spiegel, 26 August 2013) accessed on 22 June 2015.

¹²⁹ **Vienna Convention on Diplomatic Relations**, (adopted 18 April 1961, entered into force 24 April 1964) 500 UNTS 95.

the French Senate stated that, “*Aux États-Unis, le contexte juridique, avec au premier chef le Patriot Act, s’est traduit, ainsi que le révèle le Washington Post, par une habilitation au secret-défense de 840 000 personnes, dont 135 000 seulement dans les agences de renseignement. Autrement dit, beaucoup sont dans les entreprises. Ces personnes ont deux employeurs, leur entreprise, et la NSA... Dans cet important appareillage, une part, très visible, se concentre sur la lutte contre le terrorisme, mais la plus grande part, beaucoup moins visible, se voue à l’espionnage économique.*” Lemoine said, according to information in the Washington Post, pursuant to the legal context created by the Patriot Act, only 135,000 personnel out of 840,000 have been working at intelligence agencies, but all 840,000 personnel have authorization to access state secrets. In other words, most of the personnel work at private companies. Those people have two employers: their companies and the NSA. In this context, the part which is more visible focuses on the fight against terrorism, but the other part, which is less visible, is dedicated to economic espionage.

Nevertheless, Vanee Vines, an NSA spokeswoman, denied any allegations for using foreign intelligence capabilities to “steal the trade secrets of foreign companies on behalf of U.S. companies to enhance their international competitiveness”, but rather explained economic espionage on the basis of national security.¹³⁰ Likewise, Mike Rogers, the chairman of the House Intelligence Committee, denied economic espionage activities of the NSA and stated that “economic espionage is against the law in the United States. If they [the NSA] do it, they are going to jail.”¹³¹ In spite of the denials from U.S. officials, Brazilian officials confirmed the interception and economic espionage activities of the NSA. H. E. Dilma Rousseff, former president of the Federative Republic of Brazil, underlined the industrial espionage activities targeting Petrobras, in her speech at the opening of the general debate of the 68th session of the United Nations General Assembly. In her speech, Rousseff stated that, “corporate information - often of high economic and even strategic value - was at the center of

¹³⁰ James Glanz and Andrew W. Lehren, ‘N.S.A. Spied on Allies, Aid Groups and Businesses’ (**The New York Times**, 20 December 2013) http://www.nytimes.com/2013/12/21/world/nsa-drag-net-included-allies-aid-groups-and-business-elite.html?_r=0 accessed on 23 July 2015.

¹³¹ Sam Jones, ‘US spies engaged in industrial espionage will be jailed, says lawmaker’ (Financial Times, 31 January 2014) accessed on 22 June 2015; Michael Rogers, ‘Panel Discussion “Rebooting Trust? Freedom vs. Security in Cyberspace”’ (**Munich Security Conference**, 31 February 2014) accessed on 22 June 2015 https://www.securityconference.de/media-library/videos/?tx_tvmediacenter_mediacenter%5Bcontroller%5D=Mediacenter&tx_tvmediacenter_mediacenter%5Bsearch_result%5D=320&cHash=b463f65bf1dae400bcd5f986133af1e0

espionage activity”, describing the activities as industrial espionage and “a breach of International Law.”¹³²

(3) Attribution Problem

There are ongoing discussions and speculations regarding the attribution problem. Attribution is basically about finding responsible individuals and entities then having reasonable clues to establish a causal link between perpetrators and state organs or governments. Therefore, it becomes possible to attribute illegal cyber activities to a government or state and label those activities as “state-sponsored, backed or financed.” However, the problem of attribution and the methods applied for attributing any cyber activity to officials is out of scope of this research. We have instead focused on illustrating the fact that states are conducting economic cyberespionage activities and try to find and adopt counter measures in which all attacking and defending activities provide a basis for state practice.

Unlike human-based intelligence gathering operations, signal-based intelligence gathering activities can be conducted covertly and without risk of being detected for a long time. Moreover, attributing any kind of cyber operations to states or states officials and bodies is a complex process, because proving the link between them is both technically and legally challenging. Detecting the source of an attack does not automatically provide a link between operations or support of a state. According to the Tallinn Manual Rule 7, “the mere fact that a cyber operation has been launched or otherwise originates from governmental cyber infrastructure is not sufficient evidence for attributing the operations to that State but is an indication that the State in question is associated with the operation.”¹³³ According to Roscini, “official state documents, such as national legislation, cyber doctrines, manuals, strategies, directives and rules of engagement, may become relevant in establishing state responsibility for cyber

¹³²Statement by H. E. Dilma Rousseff, President Of The Federative Republic Of Brazil, at the opening of the general debate of the 68th session of the **United Nations General Assembly** (New York, 24 September 2013) http://gadebate.un.org/sites/default/files/gastatements/68/BR_en.pdf accessed on 22 July 2015.

¹³³ Michael N. Schmidt (ed.), **Tallinn Manual on The International Law Applicable to Cyber Warfare** Cambridge, (2013), 39.

operations.”¹³⁴ This shows that actors are targeting both public and private networks for economic espionage purposes. Therefore a targeted state can apply certain legal mechanisms to tackle with these operations.

To this end, founding features of espionage activities have changed and states can be the victim and perpetrator of economic cyberespionage activities. Regarding the above mentioned explanations, economic espionage activities to gain strategic advantage has proliferated. There are several reasons for such a proliferation; first, the costs and externalities are low comparing to traditional espionage. To illustrate, according to the BlackOps Partners Corporation, which focus on counterintelligence and protection of trade secrets for Fortune 500 companies, \$500 billion in raw innovation is stolen from U.S. companies each year.¹³⁵ “Raw innovation includes trade secrets, research and development, and products that give companies a competitive advantage.”¹³⁶ Casey Fleming, CEO of BlackOps Partners Corporation, indicates that “when this innovation is meant to drive revenue, profit, and jobs for at least 10 years, we are losing the equivalent of \$5 trillion out of the U.S. economy every year to economic espionage. To put it into perspective, the U.S. will take in \$1.5 trillion in income taxes and \$2.7 trillion in all taxes in 2013.”¹³⁷

Secondly, determining the origin and attributing the attack to officials is difficult and complicated. Thirdly, it may take years to spot and detect cyberespionage activities, especially APT type attacks. Lastly, there is an underdeveloped legal framework to decide appropriate responses. Therefore, in order to respond to this change effectively and legally and to combat the rising economic espionage threat, we should look for opportunities to apply existing legal frameworks or expand their scope through covering this new situation. International legal documents do not provide any legal definition for economic and industrial espionage. Similarly, there is not any definition and legal framework to combat against cyberespionage, however, domestic legal systems describe espionage, industrial theft, and economic espionage as punishable crimes. Punishments envisaged for these crimes are applicable to those

¹³⁴ Marco Roscini, ‘Evidentiary Issues in International Disputes Related to State Responsibility for Cyber Operations’, **Texas International Law Journal**, 50:2, (2015) 256; Mark D. Young, ‘National Cyber Doctrine: The Missing Link in the Application of American Cyber Power’, **Journal of National Security Law & Policy** 173, (2010), 175–76.

¹³⁵ For more information BlackOps Partners, visit <https://blackopspartners.com/firm/>

¹³⁶ Joshua Philipp, **The Staggering Cost of Economic Espionage Against the US**, Epoch Times, 22 October 2013, <http://www.theepochtimes.com/n3/326002-the-staggering-cost-of-economic-espionage-against-the-us/>

¹³⁷ Ibid.

crimes which are committed by cyber means. Additionally, at the international level, it is a gray area whether espionage is subject to certain limitations and punishments. However, by adding cyber and economic elements to espionage, this gray area becomes less discrete, because huge amounts of economic and material damage occurs as a result of economic and industrial cyberespionage activities. In this regard, along with the domestic regulations, states are looking for possible responses allowed under international law.

The next chapter will focus on the theoretical basis of cyberespionage activities then discuss several domestic and international legal responses to economic and industrial cyberespionage activities.

C. Evaluation of Cyberespionage under International Legal Theory

The application of rational choice and game theory to international law offers comprehensive results in order to explain the rationale behind economic cyberespionage activities. It is crystal clear that states are conducting cyberespionage activities as a result of cost-benefit analysis. The benefits which are gained and expected to be gained are greater than the cost and externalities of conducting cyberespionage.

Previous researches have proven that weaker parties have been eager to challenge stronger parties and those weaker parties have been inclined to win the conflicts.¹³⁸ The underlying reason for such an outcome is because of the strategy adopted by parties. While the stronger party focuses on and designs its strategy on attacking, the weaker party adopts direct defense and guerilla warfare strategies, which paves the way for victory.¹³⁹ In the case of cyberespionage, infiltration and attack activities, strategies of the parties change. The weaker party adopts direct attacking and guerilla warfare strategies simultaneously, while the stronger party, in order to protect its valuable assets, adopts a direct defense strategy. It is generally a better

¹³⁸ Ivan Arreguin-Toft, *How the Weak Win Wars, A Theory of Asymmetric Conflict*, **Cambridge Studies in International Relations**, 2005; T.V. Paul, *Asymmetric Conflicts: War Initiation by Weaker Powers* **Cambridge University Press**, (1994).

¹³⁹ *Ibid*, 39.

strategy to focus one's efforts on cyber offense, rather than defense.¹⁴⁰ The weaker party in this regard, is small group of experts conducting operations and infiltration activities against the stronger parties, which are well protected servers and networks of state entities and companies. Therefore, actors have adopted certain protective measures called “active cyber defense” which is to enable the targeted actors to identify, target and counterattack. In addition, the weaker party is likely to take advantage of the stronger party's dependence on cyberspace for four significant reasons.¹⁴¹ First, the costs of cyber operations are low in comparison with traditional espionage or military activities. Second, determining the origin of cyber operations and attributing them to the weaker party is difficult. Therefore, the strong party would be hindered in responding conventionally to such an attack. Third, cyber attacks can confuse the enemy. Fourth, there is an underdeveloped legal framework to guide responses. Those four significant reasons provide an asymmetric advantage for the weaker party and may reduce conventional military dominance and superiority of the stronger party.

Table 0-5: Strategies of Stronger and Weaker Parties

Stronger Party	Weaker Party
Direct Defense	Direct Attack
Active Defense	Guerilla Warfare

In some respect, there is an equilibrium on deciding and conducting cyberespionage activities. States can conduct or refrain to conduct cyberespionage activities under certain circumstances. Such decision is subject to internal and external variables. Capabilities of states, effective use and allocation of resources and legal restrictions on the one hand, while the capabilities of the target, benefits to be gained from the activity, international relations between states and legal consequences of the

¹⁴⁰ Pierluigi Paganini. “FireEye World War C report – Nation-state driven cyber attacks.” Security Affairs RSS., 3 October 2013, <http://securityaffairs.co/wordpress/18294/security/fireeye-nation-state-driven-cyber-attacks.html>

¹⁴¹ U.S.-China Economic and Security Review Commission, Report to Congress, access https://docs.google.com/document/d/1FbrhjU0ztFWTX7n-xU2rf_eV4lsA-qYFyVsK3cSgAds/edit (2008) 9.

activity affect the targeting process. Furthermore, the below scenarios illustrate the possible equilibrium while deciding to deploy cyberespionage activities.

First, a state might not want to perpetrate cyberespionage because it can use its capacity for more beneficial purposes for example, by attacking another target. This is also related with the strategic allocation of resources. Either through cost-benefit analysis or allocation of resources strategically, states can refrain from attacking a specific target. This equation is called coincidence of interest. “In this situation states are acting independently to achieve their best outcomes regardless of the behaviors of other state.”¹⁴² To illustrate, whether sponsored by state or non-hacker groups inside China are attacking other state’s critical infrastructure and targeting strategic sectors to collect, infiltrate and gain economic advantage. In this sense, they are absolutely oblivious to any possible reaction or behavior of a targeted state and they have only motivated to gain advantage in any kind without considering the reaction.

Second, many states receives no benefit from perpetrating cyberespionage and the few states that would benefit from cyberespionage are deterred from doing so by powerful states that want to prevent being attacked. In other words, many states refrain from attacking non-strategic targets due to its inefficiency or strategic targets due to being targeted by a strong opponent. This inactivity derives from the concept of coercion. This coercion can be any kind, such as cyber, diplomatic, economic and military. In this regard, detecting pressure points and adopting appropriate measures hinder other state’s capabilities to perform those activities.

Third, two states decline to attack each other’s systems in a bilateral repeated prisoner’s dilemma and all the other states decline to do so because of coincidence of interest of coercion. Or it may be that the other states also face each other in bilateral prisoner’s dilemmas and therefore refrain from attacking systems because they fear retaliation from their (single) opponent.

As it is underlined by Deeks, “clear and objective surveillance norms that restrict current foreign surveillance practices can improve inter-state relationships.”¹⁴³ Therefore, legal norms and principles regulating and restricting surveillance and cyber

¹⁴² Jack L. Goldsmith and Eric Posner, **Limit of International Law**, Oxford University Press, (2005) 35.

¹⁴³ Ashley Deeks, **An International Legal Framework for Surveillance**, Virginia Journal of International Law, Vol. 55:2, (2015) 325.

infiltration activities will eventually contribute to inter-state relations. Similarly, Baker states that “mutual trust between treaty parties increases when espionage affirms that the assurances provided are accurate. States will be more willing to cooperate with other states in the future if their espionage confirms that the assurances provided by these parties are truthful.”¹⁴⁴ Contrary to Baker and Deeks, Buchan states that “espionage represents a threat to the maintenance of international peace and security.”¹⁴⁵

D. Concluding Remarks

Challenges inherent to regulating cyberspace can also be observed for regulating espionage operations. While espionage operations have radically changed considering its targets, purposes, actors, methods and means; we have encountered that traditional espionage activities evolved into a cyberespionage.

As it is discussed in details above, cyberespionage operations¹⁴⁶ conducted by various actors consist a solid legal base for State practice which is one of the constituting elements of the customary international law. We exemplify several incidents and operations, constituting a legal base for State practice in creation of customary international law. However State practice is not solely sufficient for creation of customs where we seek for *opinio juris*. Next chapter under domestic regulations we aimed to exemplify that such regulations constituting a *opinio juris* towards creation of customary international law for restricting cyberespionage operations on international level. It is still early to assert but such domestic regulations will eventually pave the way for codification or creation of customary international law

Secondly, due to its nature of information technologies and cyberespionage operations, they are inclined to be an extraterritorial. For example, in many cases, States or corporations keep their data into cloud systems which most of the time placed

¹⁴⁴ Christopher. D. Baker, ‘**Tolerance of international espionage: A functional approach**’ 19 American University International Law Review (2003) 1105.

¹⁴⁵ Russel Buchan, ‘**Cyber espionage and international law**’, in Nicholas Tsagourias and Russell Buchan (eds.), **Research Handbook on International Law and Cyberspace**, Edward Elgar Publishing, (2015) 177.

¹⁴⁶ Supra p. 33.

physically in the third country. Therefore, attacker State target not only the owner of the data but also a third country hosting physically the data in concern. In such cases, the attributing attack to a certain State and establishing the legal and factual link between attack and the suspected States becomes challenging. In this regard, attribution methods and techniques should be studied and researches should be conducted, where the scope of this study is narrow to discuss further this issue.



CHAPTER TWO

TACKLING WITH ECONOMIC AND INDUSTRIAL CYBERESPIONAGE

“Widespread employment of espionage in recent decades gives rise to fears the traditional methods of conducting international affairs and defending territory are inadequate.”¹⁴⁷

Wesley L. Gould & Michael Barkun, 1970

In the lights of explanations made in the first chapter, it is acknowledged that cyberespionage activities, motivated by acquiring commercial and industrial assets, not only pose significant threats to economic and financial systems, but also governmental networks. It is acknowledged by Tallinn Manual that a state may exercise its jurisdiction, 1) over persons engaged in cyber activities on its territory, 2) over cyber infrastructure on its territory and 3) extraterritorially, in accordance with international law.¹⁴⁸ In this regard, states criminalize both certain activities and some activities according to the outcome of cyberespionage.

Many states do not have specific regulations dedicated to tackle cyberespionage, so, traditional legal approach offers to apply intellectual property crimes for such activities. In other words, traditional legal approach considers the target of those activities and propose a punishment accordingly. Therefore, regulations related with protection of trade secrets and cybercrimes are domestic legal tools, if any private network is targeted by cyberespionage. There are also specific regulations to penalize economic and industrial espionage. Those regulations exist only under the American legal system, so we will analyze these regulations as well.

¹⁴⁷ Wesley L. Gould & Michael Barkun, **International Law and the Social Sciences**, Princeton, “Some Regulatory Problems of the Contemporary World: Peacetime Espionage”, (1970) 255.

¹⁴⁸ Michael N. Schmidt (ed.), **Tallinn Manual ...**, 27.

In the case of extraterritorial responses, states may adopt certain measures in accordance with international law such as; declaring such activities as internationally wrongful acts and deploy countermeasures; seek for treaty law responses accordingly such as terminating bilateral treaties due to fraudulence; or apply international forums such as the WTO. In order to give response to cyberespionage activities legally, we should look at legal documents for definitions, criminalization and punishments for individuals and legal entities. In the case of state responsibility, we should look at international legal documents restricting such activities or state practices according to appropriate legal responses and international forums to tackle economic cyberespionage. Although there are limited restrictions imposed on espionage activities by international norms, there are still several legal bases for targeted states to assert illegality of economic cyberespionage and to adopt legal arguments, under domestic and international law.

A. Legal Responses to Economic and Industrial Cyberespionage

1. Domestic Legal Responses

C.I.A, which stands for Confidentiality, Integrity and Availability, is a key information security principle which should be guaranteed in any kind of secure system.¹⁴⁹ 1) Confidentiality is the ability to hide information from those people unauthorized to view it, 2) Integrity is the ability to ensure that data is an accurate and unchanged representation of the original secure information, 3) Availability is about accessibility of the information concerned by an authorized viewer at all times.¹⁵⁰ First of all, economic and industrial cyberespionage violates confidentiality, integrity of a secured system and sometimes its availability. Therefore, states criminalize and punish any kind of violation of the above-mentioned principle. Confidentiality is the prevention of unauthorized disclosure of information. Rules and regulations relating to protection of trade and commercial secrets cover the confidentiality part. Integrity aims at ensuring that information is protected from unauthorized or unintentional

¹⁴⁹ Sattarova Feruza Y., Prof.Tao-hoon Kim, 'IT Security Review: Privacy, Protection, Access Control, Assurance and System Security' International Journal of Multimedia and Ubiquitous Engineering, 2, 2, (2007) 18-19.

¹⁵⁰ Oğuz Kaan Pehlivan, *Siber Dünya: Gerçekler ve Reel Tehditler*, Analist Journal, 31, (2013) 62.

alteration, modification, or deletion. Rules and regulations restricting any unauthorized access to a computer or a secure network cover the integrity part.

Espionage activities are regulated through domestic legal systems all over the world. These activities are described under criminal codes where various punishments such as imprisonment and fines are proposed. It is significant to be aware that tools enabling espionage have changed fundamentally over a decade. In this sense, existing legal documents and provisions covering espionage are designed and enacted at a time when human-based intelligence is prioritized. However, today's business environment is profoundly different from the 1990's. Therefore, new rules and crimes have been developed and enacted for preventing cyberespionage operations. Domestic laws provide trade secret protection and cybercrimes as legal mechanisms to tackle cyberespionage.

Article 39 of the TRIPS Agreement requires member states of the WTO to provide protection for trade secrets against their unlawful acquisition, use or disclosure by third parties. There is no unitary law or approach dealing with trade secrets, in other words the protection varies from member state to member state¹⁵¹ Civil actions are adopted frequently against the misuse of trade secrets. In the late 1990's, criminalization of the misuse of trade secrets was proposed. The UK Law Commission consultation paper presents several arguments, which are embraced by other countries in support of criminalization of the misuse of trade secrets and breach of confidentiality.¹⁵² According to the paper:

1. there is no distinction in principle between the harm caused by such misuse and the harm caused by theft;
2. the imposition of legal sanctions is necessary in order to protect investment in research;
3. civil remedies alone are insufficient to discourage trade secret misuse (and would continue to be insufficient even if exemplary damages were made more widely available), because many wrongdoers are unable to satisfy any judgment against them;

¹⁵¹ Joe Lang, **The Protection of Commercial Trade Secrets**, European Intellectual Property Review, Vol 25/10 (2003), 462.

¹⁵² UK Law Commission, '**Legislating the Criminal Code: Misuse of Trade Secrets**', Law Commission Consultation Paper 15, (1997) 30.

4. it is inconsistent for the law to prohibit the infringement of copyright and registered trademarks but not the misuse of trade secrets; and
5. criminalization would help to preserve standards in business life.

Nevertheless, even if the misuse of trade secrets is not criminalized that does not mean that perpetrators will escape criminal liability. For instance, “it is possible that the industrial spy, in the course of acquiring the trade secrets of another, might commit the criminal offence of burglary, or of gaining unauthorized access to a computer or of intercepting communication illegally.”¹⁵³ In addition, a distinction is made in the legal literature between technical trade secrets and other trade secrets. Technical trade secrets concern information that is within patentable subjects, traditionally defined not to include business methods; non-technical trade secrets, on the other hand, refer to everything else, including compilation of information and improved methods of organizing and conducting businesses.¹⁵⁴

a) Turkish Legal System

There is not any specific regulation on economic and industrial cyberespionage under the Turkish legal system. However, provisions related with protection of trade secrets, especially with unauthorized access and interception, have covered cyberespionage activities as well. Therefore, we will examine these provisions and their relation to prevention of cyberespionage activities.

(1) Protection of Trade Secrets

There is not any specific law or legislation in effect regarding trade secrets and their protection. In Turkish legal literature, it is acknowledged that several requirements/conditions have to exist for information or documents to be considered

¹⁵³ Joe Lang, **The Protection of ...**, 464.

¹⁵⁴ Elizabeth A. Rowe and Sharon K. Sandeen, **Trade Secrecy And International Transactions Law and Practice**, Edward Elgar Publishing, (2015), 10.

¹⁵⁴ Ibid.

as a trade secret. According to the Usluel, confidentiality and having commercial value makes commercial information or knowledge a trade secret.¹⁵⁵ The confidentiality feature of a trade secret should be considered as such information that should not be known by other rivals operating in the same industry, the owner of the trade secret should take appropriate measures to protect that secret, and finally, the trade secret should not be acquired legally.¹⁵⁶ According to Öztekin, a trade secret is “any nondisclosed information related to a commercial entity’s business and that is intentionally kept secret by its owner, which creates a commercial advantage for its owner in terms of competition and have an independent commercial value.”¹⁵⁷ The main conditions of trade secrets are 1) a trade secret is to be non-disclosed information, 2) a trade secret must have commercial value, 3) the information should be secret, and 4) the owner of the information should have the intention not to disclose the relevant information.¹⁵⁸

Additionally, the Court of Cassation stated that, “the most significant features of trade secret are to be confidential and unknown by society or other colleagues or enterprises in the same sector.”¹⁵⁹ Along with this requirement, a trade secret “must not be generally/publicly known. Secondly, the owner of the secret must be aware of the value of this information and willing to keep it confidential. Finally, the secret must be based on real facts, persons or information.”¹⁶⁰ In other words, a trade secret should possess such qualities as: the existence of confidential information, the will to keep it secret, the interest of the owner in keeping it secret, and veracity. There is a long-awaited draft law on Trade Secrets, Banking Secrets and Client Secrets, which is now before the Parliamentary Commission. The draft law gives the definition of a trade secret as:

“the information and documents relating to the field of operations of a commercial enterprise or company, that are and that can be known and acquired only by a specific number of members and other officials that is exposed to the risk of the emergence of losses particularly if they are learnt by the rivals and

¹⁵⁵ Aslı E. Gürbüz Usluel, *Anonim Şirketlerde Ticari Sırrın Korunması*, Vedat, (2009) 29.

¹⁵⁶ Ibid, 32-38.

¹⁵⁷ Selçuk Öztekin, ‘**Protection of Trade Secrets through IPR and Unfair Competition Law**’, AIPPIA, (2010), 3.

¹⁵⁸ Ibid, 4.

¹⁵⁹ Yargıtay, 11. HD., E.2004/7827; K.2007/5755.

¹⁶⁰ Uğur Aktekin, Deniz Doğan Alkan, ‘**Trade Secret Protection Turkey Chapter**’ within Trevor Cook (ed), *Trade Secret Protection: A Global Guide*, Globe Law and Business, (2016), 418.

*that should not be disclosed to the third parties, that are extremely vital for the enterprise and for the success and efficiency in the economic life of the company, that contain important information **internal structure or organization of enterprise, its financial, economic, credit and cash status, its research and development studies, its operation strategy, its resources for raw materials, the technical characteristics of productions, its pricing policies, its marketing tactics and expenses, its market share, its client potential and client networks on wholesale and retail sale basis**, as well as its contractual contacts for items are subject to permission and that are not subject to permission and other relevant information and documents.”*

In other words, the draft law listed several types of trade secrets as such: organizational structure, financial and cash position, creditworthiness, research and development activities, activity strategies, raw material resources, employee information, technical details of a means of production, pricing policies, marketing tactics and costs, market shares, connected retailers and wholesalers, customer lists and information, contractual links, databases and working methods. However, these are examples provided for illustration and do not comprise an exhaustive list.

(a) Civil Remedies

Turkish legislation proposes civil and criminal remedies to the violations of trade secrets. First of all, the main legal instrument for addressing violations of trade secrets are the “unfair competition” provisions of the Turkish Commercial Code (TCC). Unfair competition is regulated under chapter four (from Article 54 to Article 63) of the TCC with no.6103 (TCC).¹⁶¹ Article 54 states, 1) purpose of the provisions regarding unfair competition is to create, for the benefit of all participants, a just and undamaged competition, 2) acts or commercial practices which are deceptive or in any other manner against good faith effecting the relationship between competitors or between the suppliers and customers are unfair and against the law.” Article 55 listed out acts against good faith and commercial practices; subsection (d) states that acquiring business secrets without permission constitute unfair competition:

¹⁶¹ Turkish Commercial Code with n.6102, (accepted on 13.01.2011, Official Gazette No. 27846 dated on 14.02.2011).

- a) *Advertisements and sales methods against good faith and other unlawful acts,*
- b) *To direct to infringe or to terminate an agreement;*
- c) *To benefit from others' business products without authorization;*
- d) ***To divulge manufacturing and business secrets illegally, in particular one who utilizes and makes known to others information and business secrets of a manufacturer which he has acquired secretly and without permission or in any other illegal manner shall be acting against goodwill.***
- e) *Not to abide by the rules of business; in particular persons who do not abide by the business rules which have been set as a responsibility of his competitors as well through a law or an agreement or who do not abide by the business rules common in a profession branch or a business environment shall be acting against goodwill.*
- f) *To use transactional conditions that are against goodwill; in particular persons who use previously written transactional conditions against the other party in a deceiving manner*

Pursuant to Article 56, anyone who, through unfair competition, suffers injury as regards his customers, his credit, his professional reputation, his commercial activities or other economic interests or is exposed to such a danger may demand:

- a) ***the establishment of the of the unfairness of the act;***
- b) ***the prevention of unfair competition;***
- c) *the suppression of the material conditions resulting from unfair competition and, if unfair competition rests on untrue or deceitful statements, the rectification of these statements;*
- d) ***compensation of loss and damages, if there is a fault;***
- e) ***payment of moral damages*** in case of existence of the circumstances indicated in Article 58 of the Law of Obligations. The judge may, as damages in favour of the plaintiff and in accordance with the provision of paragraph (d), also order the equivalent of the advantages which the defendant might secure through unfair competition

In other words, the right owner can ask through the court for the violations to be determined, stopped and prevented, request an interlocutory injunction, request the restitution of the material status/facts resulting from the unfair competition, and payment of compensation for material and moral damages sustained because of the violations.

Article 63 of the TCC held liable legal entities if an act of unfair competition has been committed during the performance of such legal entities' work. In case the unfair competition act is committed within the frame of a legal entity's activities, application of cautionary measures special to such legal entities may also be ruled. The trade secrets obtained by means of fraud, espionage or other improper means are covered by the provisions of TCC and there are no limitations as to the remedies in such cases.¹⁶²

(b) Criminal Remedies

Criminal remedies for accessing trade secrets illegally are regulated under the Turkish Penal Code (TPC).¹⁶³ Disclosure of business secrets, banking secrets log or information relating to customers are punishable activities according to the TPC. Wording of Article 239 explains the conditions for punishment as follows:

1. *Any person who delivers information or documents which he holds by virtue of office about the customers, or **discloses business secrets, banking secrets log** is sentenced to **imprisonment from one year to three years**, and also imposed punitive fine up to five thousand days upon complaint. In case of **delivery or disclosure of this information or documents to unauthorized individuals by the persons who unlawfully acquired such information/documents**, the offender is punished according to the provision of this subsection.*
2. *Provisions of first subsection are applicable also for the information relating to **scientific researches or discoveries or industrial practices**.*
3. *Punishment to be imposed is increased by one third in case of disclosure of these secrets **to the foreigners or their personnel domiciled outside of Turkey**. In that case, no complaint is sought.*

¹⁶² Selçuk Öztekin, **Protection of ...**, 8.

¹⁶³ Turkish Criminal Code, Law Nr. 5237 (passed on 26.09.2004, Official Gazette No. 25611 dated 12.10.2004).

4. *Any person who leads another person to disclose the information or documents within the scope of this article by using force or threat is punished with imprisonment from three years to seven years.*

Article 239 of the Penal Code states that persons holding information or documents containing commercial secrets, banking secrets or client secrets because of their job or job title, who are then found, upon complaint, to have disclosed the information or documents to unauthorized persons, are liable to be sentenced to imprisonment from one to three years and to have a judicial fine.¹⁶⁴ The persons who obtain the information and documents through unlawful means and give or disclose them to unauthorized persons will be sentenced likewise. If these secrets are disclosed to a foreigner residing abroad or his officers, the penalty will be increased by one third of the principal penalty.

Subsection (2) widens the scope of this article through scientific researches , discoveries, or industrial practices. Pursuant to subsection one and two, persons who unlawfully acquired this information or documents and delivered or disclosed this information or documents to unauthorized individuals are also defined as offenders. In addition to that, if persons who unlawfully acquired such information/documents, deliver or disclose these secrets to foreigners or their personnel domiciled outside of Turkey, punishment to be imposed is increased by one third. In the case that a trade secret has been acquired through computer network operations, this unauthorized access is separately punishable under the TPC.

(2) Cyber Crimes

(a) Unauthorized Access

Given the fact that almost every bit of business, legal, personal information has been digitalized, it is acknowledged that crime can be committed through digital platforms and tailored tools for accessing such information. Therefore, the Turkish

¹⁶⁴ It is estimated that the judicial fine may corresponds to up to 5,000 days at a rate of TRY20 to TRY100 per day, according to the decision of judge in the case.

Penal Code has special provisions on unauthorized access to data processing systems. Wording of Article 243 gives details of the crime as:

1. *Any person who **unlawfully enters a part or whole of data processing system or remains there** is punished with imprisonment up to one year, or imposed punitive fine.*
2. *In case the offenses defined in above subsection involve systems which are **benefited against charge**, the punishment to be imposed is increased up to one half.*
3. *If such **act results with deletion or alteration of data within the content of the system**, the person responsible from such failure is sentenced to imprisonment from six months up to two years.*
4. *Any person who **unlawfully traces data transmissions with technical devices in a data processing system or between data processing systems without accessing the system**, is punished with imprisonment from one year to three years.*

Within this article, unlawfully or unauthorized access to a part or whole of a network becomes punishable, without any condition such as to acquire the data within that network.¹⁶⁵ Therefore, this crime has been committed when unauthorized access has happened. Similarly, the Court of Cassation ruled that “suspect has accused of accessing a commercial bank account while he did not make any transaction using this system. Therefore, it is contrary to the law, ruling in accordance with the article 243/4 while disregarding article 243/1.”¹⁶⁶

According to subsection 1, the *actus reus* element of this crime consists of “unlawfully access” and “remaining” activities. The term “remaining” covers APT, or Advanced Persistent Threats. The *means rea* element of this crime is accessing and remaining activities should be done intentionally. In addition, the recently enacted subsection 4 proposes an imprisonment from one to three years for whom unlawfully traces data transmissions with technical devices in a data processing system, or between data processing systems, without having authorization.

¹⁶⁵ Murat Volkan Dülger, **Bilişim Suçları ve İnternet İletişim Hukuku**, Seçkin (2012) 313.

¹⁶⁶ Yargıtay 11.C.D., 26.03.2009, E.2008/18190 K. 2009/3058.

Article 244 of the TPC proposes a crime for hindrance or destruction of the system, deletion or alteration of data within that system. The article is written as following;

- (1) *Any **person who hinders or destroys operation of a data processing system is punished with imprisonment from one year to five years.***
- (2) *Any person **who garbles, deletes, changes or prevents access to data, or installs data in the system or sends the available data to other places is punished with imprisonment from six months to three years.***
- (3) *The punishment **to be imposed is increased by one half in case of commission of these offenses on the data processing systems belonging to a bank or credit institution, or public institutions or corporations.***
- (4) *Where the execution of above mentioned acts does not constitute any other offense apart from **unjust benefit secured by a person for himself or in favor of third parties**, the offender is sentenced to imprisonment from two years to six years, and also imposed punitive fine up to five thousand days.*

Pursuant to Article 246/4, security precautions specific to legal entities are imposed in the case of commission of the offenses listed in this section and within the frame of activities or benefit of legal entities. Therefore, in cases of conviction of a crime through participation of the organs or representatives of a legal entity, security precautions stipulated under Article 60 become applicable. As a security precaution, the court may decide on the cancellation of an authorization license or confiscation of their property.

(b) Illegal Interception of Data and Systems

Intercepting communication network and traffic data is prohibited under the Turkish Constitution and Turkish Penal Code. According to Article 22 of the Turkish Constitution, in regulating freedom of communication it is accepted that:

“Everyone has the freedom of communication.

Privacy of communication is fundamental. Unless there exists a decision duly given by a judge on one or several of the grounds of national security, public order, prevention of crime, protection of public health and public morals, or protection of the rights and freedoms of others, or unless there exists a written order of an agency authorized by law in cases where delay is prejudicial, again on the above-mentioned grounds, communication shall not be impeded nor its privacy be violated. The decision of the competent authority shall be submitted for the approval of the judge having jurisdiction within twenty-four hours. The judge shall announce his decision within forty-eight hours from the time of seizure; otherwise, seizure shall be automatically lifted.”

Penal Code under section 9 regulates the offenses against privacy and secrecy of life. Pursuant to Article 132;

1. ***Any person who violates the confidentiality of communication between persons shall be sentenced to a penalty of imprisonment of a term of 1 to 3 years. If the violation of confidentiality occurs through the recording of the content of the communication, the penalty to be imposed shall be increased by one fold.***
2. ***Any person who unlawfully publicizes the contents of a communication between persons shall be sentenced to a penalty of imprisonment for a term of 2 to 5 years.***
3. ***Any person who unlawfully discloses the content of a communication between himself and others without obtaining their consent, shall be sentenced to a penalty of imprisonment for a term of 1 to 3 years. (Sentence added on 2 July 2012 - by Article 79 of the Law no. 6352) Where such conversation is published in the press or broadcasted, the penalty to be imposed shall be the same.***

In the case of commission of the offenses defined in the above articles, the punishment is increased by one half, if the offence is committed by abusing his or her position or profession. Moreover, security precautions specific to legal entities are imposed in cases of commission of offenses, defined in the above articles, by legal entities.

In addition, law no 6698, regarding Personal Data Protection, was enacted and published in the Official Gazette.¹⁶⁷ Article 30 of the law has envisaged certain provisions to be amended and new provisions to be added. In this context, article 243/4 of the Turkish Penal Code, “*monitoring data transfer which occur within an information system or between information systems by technical tools without entering the system is punishable by 1 to 3 years of imprisonment.*” The purpose of this article is to punish illegal monitoring and interception.

Likewise, the articles of the Wassenaar Agreement regulate and restrict the trade of intrusion and surveillance items, as in article 245/A/1 of the TPC which regulates the prohibited devices and programs. According to article 245/A/1, “creating or producing a device, computer program, password or other security code for committing a crime; individuals who manufacture, import, deliver, convey, store, accept, sell, prepare them to be sold, deliver to others or who owned them shall be punished by one to three years of imprisonment or judicial fine up to five thousand days.”

The provisions above are not specifically designed to answer the rising problem of intrusions and espionage, but these are available tools designed for combating cyberespionage. Nevertheless, despite being proposed and applied under the domestic legislations, these provisions contribute to ease the mutual legal assistance process and other kind of cooperation between law enforcement and judiciary officials regarding the cross-border nature of cyber attacks and activities related to cyberespionage.

b) American Legal System

Under the American legal system, the Economic Espionage Act is *lex specialis* and the primary legal mechanism to tackle cyberespionage. This act criminalizes certain economic and industrial espionage acts with penalties up to 10 years. Along with the Espionage Act, the U.S. legal system regulates theft of trade secrets, which is the precursor to the Espionage Act and Computer Fraud Act that criminalizes unauthorized access to a computer or network.

¹⁶⁷ Turkish Law on Personal Data Protection with Nr.6698 (accepted on 24.03.2016 Official Gazette No. 29677 dated on 07.04.2016)

(1) Economic and Industrial Espionage

Contrary to the Turkish legal system, the U.S. Economic Espionage Act of 1996 (“The Act”) gives detailed definitions of economic and industrial espionage.¹⁶⁸ The Act criminalizes two kinds of activities- the theft of trade secrets to benefit a foreign actor¹⁶⁹ and theft for commercial or economic purposes.¹⁷⁰ Each crime is subject to different penalties and fines.

According to the Act, economic espionage occurs when someone is intending or knows that the offense will benefit any foreign government, foreign instrumentality, or foreign agent, knowingly: (1) steals, or without authorization appropriates, carries away, conceals, or obtains by deception or fraud a trade secret; (2) copies, duplicates, reproduces, destroys, uploads, downloads, or transmits that trade secret without authorization; or (3) receives a trade secret knowing that the trade secret had been stolen, appropriated, obtained or converted without authorization.

Industrial espionage occurs when someone knows that his or her offense will injure the owner of a trade secret of a product produced for or placed in interstate or foreign commerce, or acts with the intent to convert that trade secret to the economic benefit of anyone other than the owner by: (1) stealing, or without authorization appropriating, carrying away, concealing, or obtaining by deception or fraud information related to that secret; (2) copying, duplicating, reproducing, destroying, uploading, downloading, or otherwise transmitting that information without authorization; or (3) receiving that information knowing that that information had been stolen, appropriated, obtained or converted without authorization.¹⁷¹

According to those definitions, the *mens rea* element for this crime is intending or knowing whether his or her action will benefit any foreign government or will injure the owner of a trade secret. The *actus reus* element for committing this crime is acquiring trade secret to the economic benefit of anyone other than the owner.

¹⁶⁸ Economic Espionage Act 1996 sec 101, 18 USC § 1831-1839.

¹⁶⁹ Ibid, 18 U.S.C. § 1831(a).

¹⁷⁰ Ibid, 18 U.S.C. § 1832.

¹⁷¹ Economic Espionage Act 1996 sec 101, 18 USC § 1832.

The Act also defines foreign powers/actors, or “foreign instrumentality”, as any agency, bureau, ministry, component, institution, association or any legal, commercial or business organization, corporation, firm, or entity that is substantially owned, controlled, sponsored, commanded, managed, or dominated by a foreign government.

The Economic Espionage Act penalizes any above mentioned activities, if a foreign power/actor gains benefit from them. According to the U.S. Code § 1839 3 *“the term “foreign agent” means any officer, employee, proxy, servant, delegate, or representative of a foreign government.”* Regarding economic espionage, “benefit means not only economic benefit but also reputational, strategic, or tactical benefit.”¹⁷² There is a distinction made between individuals and organizations.¹⁷³ Individuals who commit this crime will be subject to 15 years imprisonment or a five million USD fine. In cases of organizations, there is not any imprisonment, but the fine will not be greater than 10 million USD or 3 times the value of the stolen trade secret.

Although it is rarely applicable, the Act was applied in May 2014 against five Chinese military hackers responsible for economic espionage. This was the first ever case filed against state actors. Grand Jury of Western District of Pennsylvania (WDPA) indicted the hackers with allegations;

1. ***“...conspired to hack into American entities, to maintain unauthorized access to their computers and to steal information from those entities that would be useful to their competitors in China, including state-owned enterprises (SOEs)***
2. ***...stole trade secrets that would have been particularly beneficial to Chinese companies at the time they were stolen***
3. ***...stole sensitive, internal communications that would provide a competitor, or an adversary in litigation, with insight into the strategy and vulnerabilities of the American entity.”***¹⁷⁴

¹⁷² Charles Doyle, **Stealing Trade Secrets and Economic Espionage: An Overview of 18 U.S.C. 1831 and 1832**, Congressional Research Service Report, accessed <https://www.fas.org/srg/crs/secretary/R42681.pdf> (2014) 11.

¹⁷³ Title 18 U.S.C., Section 1831 Economic Espionage.

¹⁷⁴ Department of Justice, U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage, 19 May 2014, accessed <https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor>

In the indictment, it is stated that “the conspirators trade secrets that would have been particularly beneficial to Chinese companies at the time they were stolen.”¹⁷⁵ According to the indictment, “conspirators also stole sensitive, internal communications that would provide a competitor, or adversary in litigation, with insight into the strategy and vulnerabilities of the American entity.”¹⁷⁶ The attackers alleged to steal “1.4 gigabytes of data, the equivalent of roughly 700,000 pages of email messages and attachments” from Westinghouse’s computers between 2010 to 2012.¹⁷⁷ Westinghouse is a civilian nuclear power plant developer and constructor, and at that time they were constructing a nuclear power plant in China. Similarly, U.S. Steel, the largest steel company in the U.S., was targeted when it had significant business interests with China. While the company was participating in several international trade disputes with Chinese steel manufacturers, 1,753 U.S. Steel computers were infiltrated by spear-phishing e-mails.

(2) Theft of a Trade Secret

Although it is commonly referred to as industrial espionage, the U.S. legal system has separate provisions to regulate the theft of trade secrets. A trade secret is defined under the Uniform Trade Secrets Act 1985 (UTSA) as;

“the term “trade secret” all forms and types of financial, business, scientific, technical, economic or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically or in writing, if –

(A) the owner thereof has taken reasonable measures to keep such information secret; and

¹⁷⁵ United States v. Wang Dong, Sun Kai Liang, Wen Xinyu, Huang Zhenyu, Gu Chunhi, Criminal No 14-118, District Court West District of Pennsylvania, (1 May 2014) accessed <https://www.justice.gov/iso/opa/resources/5122014519132358461949.pdf>

¹⁷⁶ Ibid, 3.

¹⁷⁷ Ibid, 16.

(B) the information derives independent economic value, actual or potential, from being generally known to and not being readily ascertainable through proper means by public.”

Therefore, one of the key elements of the crime is that the trade secret should derive “independent economic value... from not being generally known to ... the public.” In the case of *Lansig Linde Ltd. vs. Kerr*, it is argued that trade secrets are defined as;

*“What are trade secrets and how do they differ (if at all) from confidential information? Mr. Poulton suggested that a trade secret is information which, if disclosed to a competitor, would be liable to cause real or significant harm to the owner of the secret. I would add first, that it must be information used in a trade or business, and secondly that the owner must limit the dissemination of it or at least not encourage or permit widespread publication.”*¹⁷⁸

According to Toren, the definition given by UTSA is setting a very minimal standard and courts have held information which affords only a slight advantage to the holder, may qualify as a trade secret.¹⁷⁹ To illustrate, in *Sheridan v. Mallinckrodt, Inc.* case, the court stated that “although the advantages of a trade secret may be slight, they are responsible for helping to control production costs, and do, therefore provide the owner with a competitive edge (advantage)”.¹⁸⁰ The court can adopt numerous methods to prove a competitive edge (advantage) that trade secret may provide to the owner. In the *United States v. Bottone* case, the court ruled that “value of these papers (stolen formulae) secret processes for which European drug manufacturers were willing to pay five and six figures.”¹⁸¹ Calculation of the independent economic value of the information may be based on open market indicators or the court may use “thieves’ market” as a proper means of valuing stolen goods or property. The court allows the use of a thieves’ market and ruled that “the valuation of stolen goods

¹⁷⁸ *Lansig Linde Ltd. vs. Kerr*, **Weekly Law Report** 1, (1991), 251.

¹⁷⁹ Peter J. Torren, **Intellectual Property and Computer Crimes**, Law Journal Press, (2016) Chapter 5, 17.

¹⁸⁰ *Sheridan v. Mallinckrodt, Inc.*, 568 F. Supp. 1347, U.S. District Court for the Northern District of New York - 568 F. Supp. 1347 (N.D.N.Y 1983).

¹⁸¹ *United States v. Caesar Bottone, Seymour Salb, and Nathan Sharff*, 365 F.2d 389 (2d Cir. 1966).

according to the concept of a thieves' market is an appropriate method for determining the market value of goods.”¹⁸²

In some respect, collecting intelligence in the market-place is essential for companies to survive. For instance, as it is legally grounded in the *Mars UK Ltd. vs. Technowledge Ltd* case,¹⁸³ purchasing a competitor's product and analysis of that product through reverse-engineering is plausible. However, in a case of industrial espionage, the U.S. Court of Appeals concluded that aerial photographing of a plant under construction is “an improper method”¹⁸⁴ of discovering the trade secrets.”¹⁸⁵

Pursuant to the Act, theft of trade secrets is (1) whoever knowingly performs targeting or acquisition of trade secrets or (2) intends to convert a trade secret to knowingly benefit anyone other than the owner. This indicates the *means rea* element of the crime. On the other hand, the *actus reus* element of this crime is defined as (1) steal, conceal, or carry away by fraud, artifice, or deception; (2) copy, duplicate, sketch, draw, photograph, download, upload, alter, destroy, photocopy, replicate, transmit, deliver, send, mail, communicate, or convey; (3) receive, buy, or possess a trade secret, knowing the same to have been stolen or appropriated, obtained, or converted without authorization.

In 2012, the High Court narrowed the jurisdictional scope of the Act in the *United States v. Aleynikov* case.¹⁸⁶ The Court interpreted the wording of the provision, as the Economic Espionage Act, is only applicable to the trade secret if it relates to products that a company sells, and not those related to products that a company uses internally. A year later, the Theft of Trade Secrets Clarification Act was enacted. This act amended the scope of the Economic Espionage Act through including trade secrets related to “a product or service used in or intended for use” in commerce.¹⁸⁷

¹⁸² *United States v. Michael J. Oberhard*, No. 89-1503. United States Court of Appeals, Seventh Circuit (1989) ; *United States v. Stegora*, 849 F.2d 291, 292 (8th Cir. 1988).

¹⁸³ *Mars UK Ltd. vs. Technowledge Ltd*, Fleet Street Reports 18, Sweet and Maxwell, (1999).

¹⁸⁴ Under the Trade Secret Law of most of the States in US defines “improper means” includes theft, bribery, misrepresentation, breach or inducement of a breach of a duty to maintain secrecy, or espionage through electronic or other means. Reverse engineering or independent derivation alone shall not be considered improper means. (Trade Secret Law California).

¹⁸⁵ *E. I Du Pont de Nemours & Company vs. Rolfe Christopher*, No. 28254, (US Court of Appeals, 5th Circuit) (1970).

¹⁸⁶ *United States v. Aleynikov*, No. 11-1126 (2d Cir. 2012).

¹⁸⁷ Warrington Parker, President Obama Signs into Law the Theft of Trade Secrets Clarification Act, Orrick News Alert, 01-03-2013, accessed <https://www.orrick.com/Events-and-Publications/Pages/President-Obama-Signs-into-Law-the-Theft-of-Trade-Secrets-Clarification-Act.aspx>

Unlike economic espionage, the beneficiary of the theft of trade secrets must be anyone other than the owner of the misappropriated trade secret(s). The maximum sentence for individuals who committed the theft is 10 years imprisonment, 250,000 USD or an alternative fine based on gain/loss figures. In the case of committing the crime through an organization, there is only a maximum five million USD organizational fine.¹⁸⁸

Theft of trade secrets involves the intent to harm the owner, however, an intent to benefit a foreign actor/power or a knowledge of that result is required for economic espionage. Economic espionage covers all trade secrets “notwithstanding the absence of any connection to interstate or foreign commerce.”¹⁸⁹ Therefore, imprisonment and fines are more severe comparing to the theft of trade secrets.

In addition to that, there are ongoing negotiations on free trade agreements between the U.S. and (1) the Trans-Pacific Partnership (TPP), which involves 11 countries in the Asia-Pacific region, and (2) the Transatlantic Trade and Investment Partnership (TTIP) with the European Union. According to the U.S. Chamber of Commerce,

*“Some TPP countries, such as Canada, Australia, Malaysia, and Singapore, have no laws criminalizing traditional trade secret disclosure or misappropriation. Many of these countries have criminal laws targeting computer-related crimes, which may sweep some forms of trade secret infringement into their purview but do not address trade secrets directly. Among those countries that do criminalize trade secret misappropriation or disclosure, the penalties often vary from those that would not provide sufficient deterrent effect to those that would but only if applied consistently. ... The low criminal penalties or lack thereof in some TPP jurisdictions are particularly troublesome, as criminal penalties are believed to provide a greater deterrent to the would-be trade secret thief than the prospect of a civil penalty alone.”*¹⁹⁰

Therefore, the U.S. aims to harmonize criminal laws penalizing the violation of trade secrets or undisclosed information.

¹⁸⁸ Title 18 U.S.C., Section 1832 Theft of Trade Secrets.

¹⁸⁹ Doyle, Supra 105, 8.

¹⁹⁰ U.S. Chamber of Commerce, The Case for Enhanced Protection of Trade Secrets in the Trans-Pacific Partnership Agreement, (2013) 23.

(3) Computer Fraud

Another domestic legal tool to combat cyberespionage under the American legal system is the Computer Fraud and Abuse Act. According to the act, unauthorized access to a computer and obtaining an information is a punishable crime. Title 18, , Section 1030(a) of the United States Code provides that:

(a)Whoever—

(1) ***having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph y. of section 11 of the Atomic Energy Act of 1954, with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it;***

(2) ***intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains—***

(A) *information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);*

(B) *information from any department or agency of the United States; or*

(C) *information from any protected computer;*

- (3) *intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct affects that use by or for the Government of the United States;*
- (4) *knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than \$5,000 in any 1-year period;*

The crime of computer fraud consists of three essential elements. First of all, the defendant should intentionally access a computer without authorization or by exceeding authorized access. This behavior constitutes the *actus reus* part of the typology of the crime. Secondly, the defendant should obtain information (1) contained in a financial record of a financial institution or an issuer of a credit card or, (2) on a costumer contained in a file of a consumer reporting agency, (3) from any department/agency of the United States, or (4) from any protected computer. The defendant should have specific intentions to perpetrate such activities. In other words, one should act (1) for the purposes of commercial advantage or private personal gain, (2) in furtherance of a described criminal or tortious act, or (3) obtained information having a value exceeding \$5,000.00. In this regard, the above-mentioned *mens rea* element should coexist with the *actus reus* element for crimes to be committed.

Title 18, Section 1030(a) of the United States Code proposes the punishment for the above-mentioned crime as follows:

- (b) *Whoever conspires to commit or attempts to commit an offense under subsection (a) of this section shall be punished as provided in subsection (c) of this section.*
- (c) *The punishment for an offense under subsection (a) or (b) of this section is—*
- (1)
- (A) *a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(1) of this section which does not*

occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and

(B) a fine under this title or imprisonment for not more than twenty years, or both, in the case of an offense under subsection (a)(1) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

(2)

(A) except as provided in subparagraph (B), a fine under this title or imprisonment for not more than one year, or both, in the case of an offense under subsection (a) (2), (a) (3), or (a) (6) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

(B) a fine under this title or imprisonment for not more than 5 years, or both, in the case of an offense under subsection (a)(2), or an attempt to commit an offense punishable under this subparagraph, if—

(i) the offense was committed for purposes of commercial advantage or private financial gain;

(ii) the offense was committed in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or of any State; or

(iii) the value of the information obtained exceeds \$5,000; and

(C) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(2), (a)(3) or (a)(6) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

(3)

(A) a fine under this title or imprisonment for not more than five years, or both, in the case of an offense under subsection (a)(4) or (a)(7) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and

(B) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(4), or (a)(7) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph.

Section 1030(a) (2) does not impose fines. Although there is no “monetary threshold for establishing a misdemeanor offense under section 1030(a) (2), the value of the information obtained during an intrusion can elevate the crime to a felony.”¹⁹¹ Violations of section 1030(a) (2) are misdemeanors punishable by a fine or a one-year prison term unless aggravating factors apply. A violation or attempted violation of section 1030(a) (2) is a felony (otherwise it is a misdemeanor) if: (1) committed for commercial advantage or private financial gain, (2) committed in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or of any state, or (3) the value of the information obtained exceeds \$5,000.

Merely obtaining information worth less than \$5,000 is a misdemeanor, unless committed after a conviction for another offense under section 1030, in which case the maximum prison term is 10 years.

Briefly, section 1030 requires that the defendant actually accesses a computer without or in excess of authorization. Merely viewing information is sufficient to be understood as “obtaining information” even without downloading or copying a file. Department or agency includes any federal government entity, including the legislature, judiciary, and all parts of the Executive Branch. Whether a company working as a private contractor for the government constitutes a “department or agency of the United States” for purposes of prosecution under subsection (a) (2) (B) are intended to be covered by this section.¹⁹² Any reasonable method can be used for fulfilling the requirement to determine the value of the information. For example, the research, development, and manufacturing costs or the value of the property “in the thieves’ market” can be used to meet the \$5,000 valuation.¹⁹³

Until 2008, a violation of section 1030(a) (2) (C) required actual interstate or foreign communication.¹⁹⁴ This limitation precluded prosecution in serious cases

¹⁹¹ H. Marshall Jarrett, Michael W. Bailie, **Prosecuting Computer Crimes**, Office of Legal Education Executive Office for United States Attorneys, (2015) ,17.

¹⁹² Ibid.

¹⁹³ Title 18 U.S.C., Section 1831 Economic Espionage.

¹⁹⁴ See 18 U.S.C. § 1030(a)(2)(C) (2007).

where sensitive or proprietary information was stolen from within a single state, as is often the case with “insider” thefts. Through the Identity Theft Enforcement and Restitution Act, Congress deleted the portion of section 1030(a) (2) (C) that required interstate or foreign communication. Accordingly, the government may now prosecute those who steal information from a computer without regard to how or where the criminal gained access to the victim’s computer, so long as that computer constitutes a “protected computer.”

Due to the complex and long bureaucratic characteristic of the extradition process or lack of any bilateral agreement, domestic legal actions against criminals or perpetrators outside of the territories of states, are mostly ineffective. Even if states signed and mutual legal assistance agreement,¹⁹⁵ the success of domestic criminal actions are low. However, as a part of naming-shaming campaign, which is a political action, governments apply to courts for obtaining arrest warrants or bringing a criminal case against perpetrators. For instance, in order to confront Chinese economic and industrial espionage activities, a grand jury in the western district of Pennsylvania indicted five Chinese military hackers for economic espionage against the U.S. nuclear power, metals, and solar products industries for commercial advantage.¹⁹⁶ The U.S. Department of Justice's indictment of these hackers was actually a domestic response, but also politically a part of naming and shaming campaign against China’s economic and industrial espionage activities.¹⁹⁷

To conclude, domestic legal systems offer several provisions enabling ways to combat cyberespionage. However, these provisions are targeting individuals or organizations who are responsible for cyberespionage activities. The next chapter will cover appropriate legal responses under international law and provisions applicable to states rather than individuals and organizations.

¹⁹⁵ **Agreement on Mutual Legal Assistance in Criminal Matters**, U.S.-China (19 June 2000) <http://www.state.gov/documents/organization/126977.pdf> accessed on 25 June 2015.

¹⁹⁶ U.S. Department of Justice, ‘U.S. Charges Five Chinese Military Hackers with Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage’ (19 May 2014). <https://www.fbi.gov/pittsburgh/press-releases/2014/u.s.-charges-five-chinese-military-hackers-with-cyber-espionage-against-u.s.-corporations-and-a-labor-organization-for-commercial-advantage> accessed on 25 June 2015.

¹⁹⁷ Scott J. Shackelford, **Managing Cyber Attacks in International Law, Business, and Relations In Search of Cyber Peace** (Cambridge, 2014) 11.

2. Regional Legal Responses

a) European Trade Secret Protection

The EU and its member states are signatory to the WTO Agreement including the TRIPS Agreement, therefore they are obligated to comply with Article 39 of the TRIPS Agreement, requiring the adoption of legislation for protection of trade secrets, and to notify the WTO whenever they issued such protection. Following a proposal of the European Council, on 8 June 2016, the European Parliament and the Council adopted Directive 2016/943 (The Directive)¹⁹⁸ that aims to standardize the national laws in EU countries against the unlawful acquisition, disclosure and use of trade secrets. In contrary to the EU Regulations, directives are not self-executing and direct EU member states to adopt laws that comply with each directive.¹⁹⁹ In this sense, every member state can adopt a protection in accordance with principles enshrined under the Directive.

According to the European Commission, the Directive aims to harmonize “the definition of trade secrets in accordance with existing internationally binding standards. It also defines the relevant forms of misappropriation and clarifies that reverse engineering and parallel innovation must be guaranteed, given that trade secrets are not a form of exclusive intellectual property right.”²⁰⁰ There are several underlying reasons for enacting the Directive. According to the Directive, “innovative businesses are increasingly exposed to dishonest practices aimed at misappropriating trade secrets, such as theft, unauthorized copying, *economic espionage* or the breach of confidentiality requirements, whether from within or from outside of the Union.”²⁰¹

Considering *economic espionage*, the European Union has significant experience which paves the way for taking necessary precautions against economic

¹⁹⁸ European Parliament and The Council, **Directive 2016/943**, “On The Protection of Undisclosed Know-How and Business Information (Trade Secrets) Against Their Unlawful Acquisition, Use And Disclosure”, 8 June 2016.

¹⁹⁹ Paul Craig, Gráinne de Búrca, **EU Law: Text, Cases and Materials**, 6th Edition, Oxford, (2015) 108

²⁰⁰ European Commission, Trade Secrets, https://ec.europa.eu/growth/industry/intellectual-property/trade-secrets_en

²⁰¹ Directive 2016/943, par. (4)

cyberespionage. In 2000, a report published by the European Parliament claiming and arguing that the U.S. was using the communications interception system, known as ECHELON, to intercept European businesses and passing on the “competitive intelligence” collected through this system to U.S. firms.²⁰² The report states that as the gathering of economic data, such as details of developments in individual sectors of the economy, trends on commodity markets, compliance with economic embargoes, observance of rules on supplying dual-use goods, etc. is a part of the remit of foreign intelligence services and firms are often subject to surveillance.²⁰³

Furthermore, according to the report, “the U.S. intelligence services do not merely investigate general economic facts but also intercept detailed communications between firms, particularly where contracts are being awarded, and they justify this on the grounds of combating attempted bribery. Therefore, detailed interception poses the risk that information may be used for the purpose of competitive intelligence-gathering rather than combating corruption, even though the U.S. and the United Kingdom state that they do not do so.”²⁰⁴ The report also asserts that “authoritative sources confirmed the U.S. Congress Brown Report, indicating that 5% of intelligence gathered via non-open sources is used as economic intelligence; whereas it was estimated by the same sources that this intelligence surveillance could enable the U.S. industry to earn up to 7 billion USD in contracts.”²⁰⁵ In addition to that, the report underlined that:

“the situation becomes intolerable when intelligence services allow themselves to be used for the purposes of gathering competitive intelligence by spying on foreign firms with the aim of securing a competitive advantage for firms in the home country, and whereas it is frequently maintained that the global interception system has been used in this way, although no such case has been substantiated,

*whereas sensitive commercial data are mostly kept inside individual firms, so that **competitive intelligence-gathering in particular involves efforts** to obtain information through members of staff or through people planted in the firm for*

²⁰² EU Parliament, Report on the Existence of A Global System for the Interception of Private and Commercial Communications (ECHELON interception system) (2001/2098(INI))

²⁰³ Ibid, par. (O)

²⁰⁴ Ibid, par. (P)

²⁰⁵ Ibid., par. (S)

*this purpose or else, more and more commonly, **by hacking into internal computer networks;***

whereas risk and security awareness in small and medium-sized firms is often inadequate and the dangers of economic espionage and the interception of communications are not recognized.”²⁰⁶

The report concluded its findings that “if an ECHELON type system is used purely for intelligence purposes, there is no violation of EU law, since operations in the interests of state security are not subject to the EC Treaty, but would fall under Title V of the Treaty on European Union (CFSP). However if such a system is misused for the purposes of gathering competitive intelligence, such action is at odds with the Member States’ duty of loyalty and with the concept of a common market based on free competition, so that a Member State participating in such a system violates EC law.”²⁰⁷

Several recommendations are proposed to ensure effective protection regarding 1) the amendment of international agreements on the protection of citizens and firms, 2) national legislative measures to protect citizens and firms, 3) specific legal measures to combat industrial espionage, 4) measures concerning the implementation of the law and the monitoring of that implementation, 5) measures to encourage self-protection by citizens and firms, and 6) measures to improve security in the institutions and other measures. Under the specific legal measures to combat industrial espionage, the report addressed the member states;

“The Member States are called upon to consider to what extent industrial espionage and the payment of bribes as a way of securing contracts can be combated by means of European and international legal provisions and, in particular, whether WTO rules could be adopted which take account of the distortions of competition brought about by such practices, for example by rendering contracts obtained in this way null and void. The USA, Canada, Australia and New Zealand are called upon to join this initiative.

The Member States are called upon to give a binding undertaking neither to engage in industrial espionage, either directly or behind the front offered by a

²⁰⁶ Ibid., par. (R, T, U)

²⁰⁷ Ibid., par 13.1 Conclusions

foreign power active on their territory, nor to allow a foreign power to carry out such espionage from their territory, thereby acting in accordance with the letter and spirit of the EC Treaty.

The Member States and the U.S. Administration are called upon to start an open US-EU dialogue on economic intelligence-gathering.

The Member States are called upon to ensure that their intelligence services are not misused for the purposes of obtaining competitive intelligence, since this would be at odds with the Member States' duty of loyalty and the concept of a common market based on free competition.”²⁰⁸

According to Article 2 of the Directive, trade secret means “information which meets all of the following requirements:

- (a) it is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question;*
- (b) it has commercial value because it is secret;*
- (c) it has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret.”²⁰⁹*

Without establishing criminal sanctions, harmonizing the civil means through which victims of trade secret misappropriation can seek protection are: (a) stopping the unlawful use and further disclosure of misappropriated trade secrets, (b) the removal from the market of goods that have been manufactured on the basis of a trade secret that has been illegally acquired, or (c) the right to compensation for the damages caused by the unlawful use or disclosure of the misappropriated trade secret.

According to Article 10, member states shall ensure that the competent judicial authorities may, at the request of the trade secret holder, order any of the following provisional and precautionary measures against the alleged infringer:

²⁰⁸ Ibid.

²⁰⁹ Directive 2016/943, Art. 2

- (a) *the cessation of or, as the case may be, the prohibition of the use or disclosure of the trade secret on a provisional basis;*
- (b) *the prohibition of the production, offering, placing on the market or use of infringing goods, or the importation, export or storage of infringing goods for those purposes;*
- (c) *the seizure or delivery up of the suspected infringing goods, including imported goods, so as to prevent their entry into, or circulation on, the market.*²¹⁰

Pursuant to Article 14 of the Directive, member states shall ensure that the competent judicial authorities, upon the request of the injured party, order an infringer who knew or ought to have known that he, she or it was engaging in unlawful acquisition, use or disclosure of a trade secret, to pay the trade secret holder damages appropriate to the actual prejudice suffered as a result of the unlawful acquisition, use or disclosure of the trade secret.²¹¹

To this end, after the ECHELON incident, there was not any progress to restrict industrial espionage activities. However, it was publicly announced that there should be a limit setting rules, regulations, and administrative procedures on industrial espionage activities. The Directive on the protection of trade secrets is an outcome of such a campaign; supporting a production of international norm that industrial espionage is not acceptable. Within the framework of the Directive Article 4/2-3, we can identify two types of cybercrime offences laid down in the European Convention on Cybercrime and the EU Directive 2013/40 namely, illegal access and illegal interception. These offences fulfil the conditions of (i) intentionally, (ii) unauthorized access to information (iii) held on electronic files.²¹²

²¹⁰ Directive 2016/943, Art. 10

²¹¹ Directive 2016/943, Art. 14

²¹² Marco Alexandre Saias, **Unlawful Acquisition of Trade Secrets by Cyber Theft: between the Proposed Directive on Trade Secrets and the Directive on Cyber Attacks**, JIPLP, Vol.9/9, (2015), 724.

b) European Cybercrime Protection

The Cybersecurity Strategy of the European Union,²¹³ published in 2013, states that cyberspace should be protected from incidents, malicious activities and misuse; and governments have a significant role in ensuring a free and safe cyberspace. The EU economy is already affected by cybercrime²¹⁴ activities against the private sector and individuals. According to the document, “cybercriminals are using ever more sophisticated methods for intruding into information systems, stealing critical data or holding companies to ransom. The increase of economic espionage and state-sponsored activities in cyberspace poses a new category of threats for EU governments and companies.”²¹⁵ The document underlined that the EU does not call for the creation of new international legal instruments for cyber issues.²¹⁶

Within the document there are references to cyberespionage with regard to EU support in case of a major cyber incident or attack. Pursuant to the document:

*“If the incident seems to relate to **cyber espionage or a state-sponsored attack**, or has national security implications, national security and defense authorities will alert their relevant counterparts, so that they know they are under attack and can defend themselves. Early warning mechanisms will then be activated and, if required, so will crisis management or other procedures. **A particularly serious cyber incident or attack could constitute sufficient ground for a Member State to invoke the EU Solidarity Clause (Article 222 of the Treaty on the Functioning of the European Union).**”²¹⁷*

²¹³ European Commission, **Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace**, 52013JC0001, (2013).

²¹⁴ This definition is accepted by Cybersecurity Strategy document of EU: cybercrime commonly refers to a broad range of different criminal activities where computers and information systems are involved either as a primary tool or as a primary target. Cybercrime comprises traditional offences (e.g. fraud, forgery, and identity theft), content-related offences (e.g. on-line distribution of child pornography or incitement to racial hatred) and offences unique to computers and information systems (e.g. attacks against information systems, denial of service and malware).

²¹⁵ European Commission, **Cybersecurity Strategy...**, (2013).

²¹⁶ European Commission, **Cybersecurity Strategy...**, (2013): “To address cybercrime, the Budapest Convention is an instrument open for adoption by third countries. It provides a model for drafting national cybercrime legislation and a basis for international co-operation in this field. If armed conflicts extend to cyberspace, International Humanitarian Law and, as appropriate, Human Rights law will apply to the case at hand.”

²¹⁷ According to the Article 222 of the **Treaty on the Functioning of the European Union**:

1. The Union and its Member States shall act jointly in a spirit of solidarity if a Member State is the object of a terrorist attack or the victim of a natural or man-made disaster. The Union shall

The European Convention on Cybercrime²¹⁸ (The Convention) and the EU Directive 2016/943 on Attacks against Information Systems are key significant legal documents at the EU level, aim to tackle cyber attacks and foster cooperation between signatory states.

(1) European Convention on Cybercrime

Signed in 2001, The Convention is the first binding international legal document regulating cybercrimes in particular, infringement of copyrights, computer related fraud, child pornography, hate crimes and violations of network security.²¹⁹ 49 states have ratified the Convention from the date the treaty opened for signature.²²⁰ The purpose of the Convention enshrined in the Preamble as; “Convention is necessary to deter action directed against the confidentiality, integrity and availability of computer systems, networks and computer data as well as the misuse of such systems, networks and data by providing for the criminalization of such conduct, as described in this Convention, and the adoption of powers sufficient for effectively combating such criminal offences, by facilitating their detection, investigation and prosecution at both

mobilise all the instruments at its disposal, including the military resources made available by the Member States, to:

- (a) - prevent the terrorist threat in the territory of the Member States;
 - protect democratic institutions and the civilian population from any terrorist attack;
 - assist a Member State in its territory, at the request of its political authorities, in the event of a terrorist attack;
 - (b) assist a Member State in its territory, at the request of its political authorities, in the event of a natural or man-made disaster.
2. Should a Member State be the object of a terrorist attack or the victim of a natural or man-made disaster, the other Member States shall assist it at the request of its political authorities. To that end, the Member States shall coordinate between themselves in the Council.

²¹⁸ Council of Europe, **Convention on Cybercrime**, European Treaty Series - No. 185, (signed 23 November 2001, in effect 1 July 2004); “it is also called Budapest Convention on Cybercrime or the Budapest Convention.” Turkey signed the Convention on 10 November 2010 and ratified 22 April 2014.

²¹⁹ Views on legal nature of the Convention see: Marco Gercke, ‘**Understanding cybercrime: phenomena, challenges and legal response**’, ITU, (2012) www.itu.int/ITU-D/cyb/cybersecurity/legislation.html; Micheal Vatis, ‘**The Council of Europe 's Convention on Cybercrime**’, Berkeley Technology Law Journal, 18, (2014), 212; Amalie Weber, ‘**The Council of Europe Convention on Cybercrime**’, Berkeley Technology Law Journal, 18, (2014) 441; Mike Keyser, ‘**The Council of Europe Convention on Cybercrime**’, Journal of Transnational Law and Policy, 12, (2003), 287; Shannon Hopkins, ‘**Cybercrime Convention: A Positive Beginning to a Long Road Ahead**’, Journal of High Technology Law, 2, (2003), 107.

²²⁰ Nine of them are non-member States of Council of Europe (Australia, Canada, Dominican Republic, Israel, Japan, Mauritius, Panama, Sri Lanka, United States of America), see other States: <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=1&DF=20/02/2015&CL=ENG>.

the domestic and international levels and by providing arrangements for fast and reliable international co-operation.”

In this regard, the Convention propose cybercrimes which can be adopted against cyberespionage namely, (1) offences against the confidentiality, integrity and availability of computer data and systems and (2) computer-related offences. Article 2 of the Convention regulates illegal access, in other words, unauthorized access to the whole or any part of a computer system. This offense should be committed intentionally. Moreover, the Article envisaged that the offense can be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.

Article 3 of the Convention regulates the illegal interception, which covers APT type attacks. The Convention criminalize the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. This crime should be committed intentionally. Similar to Article 2, this offence can be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.

Article 4 and 5 of the Convention regulate the interference of data and system. Pursuant to Article 4, data interference offense is committed by damaging, deletion, deterioration, alteration or suppression of computer data without right. This offense again should be committed intentionally. With regard to Article 5, system interference is committed by serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

Likewise, the articles of the Wassenaar Agreement regulating and restricting trade of intrusion and surveillance items, the Convention regulates the misuse of devices under article 6. Pursuant to the article, it is envisaged as a criminal offenses when committed intentionally and without right:

- a) ***the production, sale, procurement for use, import, distribution or otherwise making available of:***

- i) **a device, including a computer program**, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Articles 2 through 5;
 - ii) **a computer password, access code, or similar data** by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and
- b) **the possession of an item referred to in paragraphs a.i or ii above**, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5.

Computer related offences, especially computer related forgery and fraud, are regulated under Articles 7 and 8 of the Convention. Computer related fraud is relevant to cyberespionage. Article 8 establishes a criminal offense when committed intentionally and without right, the causing of a loss of property to another person by (1) any input, alteration, deletion or suppression of computer data, (2) any interference with the functioning of a computer system with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person. Therefore, “causing of a loss of property”, “procuring, without right, an economic benefit” are covering economic and industrial cyberespionage activities.

(2) EU Directive 2016/943 on Attacks against Information Systems

The Cybercrime Convention is the legal framework of reference for combating cybercrime, including attacks against information systems. This Directive²²¹ builds on that Convention. This Directive aims to amend and expand the provisions of the Council Framework Decision.²²²

²²¹ European Parliament and The Council, Directive 2013/40, “**On Attacks Against Information Systems and Replacing Council Framework Decision 2005/222/JHA**”, Official Journal of European Union L218/8 (2013).

²²² Council Framework Decision, 2005/222/JHA of 24 February 2005 on attacks against information systems.

The objectives of the Directive 2016/943 are explained as: 1) to approximate the criminal law of the member states in the area of attacks against information systems by establishing minimum rules concerning the definition of criminal offenses and the relevant sanctions and 2) to improve cooperation between competent authorities, including the police and other specialized law enforcement services of the member states, as well as the competent specialized Union agencies and bodies, such as Eurojust, Europol and its European Cyber Crime Centre, and the European Network and Information Security Agency (ENISA). Common definitions and approaches to the constituent elements of criminal offenses, such as illegal access to an information system, illegal system interference, illegal data interference, and illegal interception aim to ensure this approximation.

In the preamble, the Directive 2016/943 underlined that “large-scale cyber attacks can cause substantial economic damage both through the interruption of information systems and communication and through the loss or alteration of commercially important confidential information or other data.”²²³ Article 1 of the Directive 2016/943 states that the Directive establishes minimum rules concerning the definition of criminal violations and sanctions in the area of attacks against information systems. It also aims to facilitate the prevention of such violations and to improve cooperation between judicial and other competent authorities.²²⁴ In addition, Article 9 underlined that the offenses referred to in Articles 3 to 8 are punishable by effective, proportionate and dissuasive criminal penalties. Therefore, the Directive determines the minimum limit of punishment for offenses laid down under Articles 3 to 8.

On the contrary to the Convention, the Directive defines term “without right” as a conduct referred to in this Directive, including access, interference, or interception, which **is not authorized by the owner or by another right holder of the system** or of part of it, or not permitted under national law.²²⁵

Pursuant to Article 3, it is criminalized when committed intentionally or accessed without right, to the whole or to any part of an information system, and is

²²³ European Parliament and The Council, Directive 2013/40, “**On Attacks Against Information Systems**.., par. (6).

²²⁴ Ibid., art. 1.

²²⁵ Ibid., art. 2

punishable as a criminal offense when committed by infringing a security measure, at least for cases which are not minor.²²⁶

Articles 4 and 5, which are almost identical to articles 4 and 5 of the Convention, criminalized illegal system and data interference. Pursuant to Article 4, seriously hindering or interrupting the functioning of an information system by inputting computer data, by transmitting, damaging, deleting, deteriorating, altering or suppressing such data, or by rendering such data inaccessible, intentionally and without right, is punishable as a criminal offense.²²⁷ According to Article 5, deleting, damaging, deteriorating, altering or suppressing computer data on an information system, or rendering such data inaccessible, intentionally and without right, is punishable as a criminal offense.²²⁸ Offenses referred to in Articles 4 and 5, when committed intentionally, are punishable by a maximum term of imprisonment of at least three years where a significant number of information systems have been affected through the use of a tool, referred to in Article 7, designed or adapted primarily for that purpose. Offenses referred to in Articles 4 and 5 are punishable by a maximum term of imprisonment of at least five years if:

- (a) they are committed within the framework of a criminal organization, as defined in Framework Decision 2008/841/JHA, irrespective of the penalty provided for therein;*
- (b) they cause serious damage; or*
- (c) they are committed against a critical infrastructure information system*

Article 6 is related with illegal interception. Although it is not defined under the article, interception is defined under the preamble. Accordingly, the preamble states that interception includes, but is not necessarily limited to, the listening to, monitoring or surveillance of the content of communications and the procuring of the content of data either directly, through access and use of the information systems, or indirectly through the use of electronic eavesdropping or tapping devices by technical means.²²⁹ Furthermore, pursuant to Article 6, intercepting, by technical means, non-public transmissions of computer data to, from or within an information system,

²²⁶ Ibid., art. 3

²²⁷ Ibid., art. 4

²²⁸ Ibid., art. 5

²²⁹ Ibid., par. (9)

including electromagnetic emissions from an information system carrying such computer data, intentionally and without right, is punishable as a criminal offense.²³⁰

Article 7 focuses on the tools used for committing offenses. Accordingly, the intentional production, sale, procurement for use, import, distribution or otherwise making available, of one of the following tools, without right and with the intention that it be used to commit any of the offenses referred to in Articles 3 to 6, is punishable as a criminal offense at least for cases which are not minor:

(a) a computer programme, designed or adapted primarily for the purpose of committing any of the offences referred to in Articles 3 to 6;

(b) a computer password, access code, or similar data by which the whole or any part of an information system is capable of being accessed.

According to Article 9, offenses referred to in Articles 3, 6, 7 and 8 are punishable by a maximum term of imprisonment of at least two years. More importantly, the Directive regulates the liability of and sanctions against legal persons. Pursuant to Article 10, legal persons can be held liable for offences referred to in Articles 3 to 8, committed for their benefit by any person, acting either individually or as part of a body of the legal person, and having a leading position within the legal person, based on one of the following:

(a) a power of representation of the legal person;

(b) an authority to take decisions on behalf of the legal person;

(c) an authority to exercise control within the legal person.²³¹

Regarding sanctions against legal persons, Article 11 states that a legal person held liable pursuant to Article 10 (1) is punishable by effective, proportionate and dissuasive sanctions, which shall include criminal or non-criminal fines and which may include other sanctions, such as:

(a) exclusion from entitlement to public benefits or aid;

(b) temporary or permanent disqualification from the practice;

²³⁰ Ibid., art. 6

²³¹ Ibid., art. 10

of commercial activities;

(c) placing under judicial supervision;

(d) judicial winding-up;

*(e) temporary or permanent closure of establishments which have been used for committing the offence.*²³²

In the light of above explanations, we concluded that, continental legal systems have adopted an approach to tackle with economic and industrial cyberespionage where regulating cyber crimes and trade secrets. However, common law system has proposed and adopted *lex specialis* dealing only with economic and industrial cyberespionage. In this regard, common law system offers heavy fine and imprisonment for actors of such operations.

3. International Legal Responses

a) Cyberespionage during Wartime

In addition to the explanations made under the chapter named Legality of Wartime Espionage, this part will analyze the legality of cyberespionage during wartime. According to the Manual on International Law Applicable to Air and Missile Warfare, Rule 119, “acts of espionage are not prohibited under the law of international armed conflict.”²³³

It is an accepted rule that “cyberespionage and other forms of information gathering directed at an adversary during an armed conflict do not violate the law of armed conflict.”²³⁴ The Tallinn Manual stated that “cyber espionage and other forms of information gathering directed at an adversary during an armed conflict do not violate the law of armed conflict. A member of the armed forces who has engaged in cyber espionage in enemy controlled territory loses the right to be a prisoner of war and may be treated as a spy if captured before re-joining the armed forces to which he

²³² Ibid., art. 11

²³³ HPCR, **Manual on International Law Applicable to Air and Missile Warfare**, (2009); US Commander’s **Handbook On The Law Of Naval Operations**, COMDTPUB P5800.7A, (2007) par. 12.9

²³⁴ Schmidt, **Tallinn Manual...**, 158

or she belongs.”²³⁵ The International Group of Experts explicitly states that topics such as “cyber espionage, theft of intellectual property and a wide variety of criminal activities” is not addressed in the Tallinn Manual due to “application of the international law on uses of force and armed conflict plays little or no role.”²³⁶ Similarly, the International Group of Experts underlined the fact that “network intrusions, the deletion or destruction of data (even on a large scale), computer network exploitation, and data theft do not amount to and the blocking of certain Internet functions and services would not suffice to trigger a non-international armed conflict.”²³⁷

Nevertheless, the International Group of Experts agreed that cyberespionage operations can only target the information relating to a party of the conflict. “It is not cyberespionage for the purpose of this rule for a corporation located in the territory of a part to the conflict to use cyber means to surreptitiously gather information about the commercial activities of a corporation in the territory of another party to the conflict.”²³⁸ In other words, this rule does not cover activities out of scope of the conflict in question.

b) Cyberespionage during Peacetime

As it is explained under the previous chapter, namely Legality of Peacetime Espionage Activities, espionage activities during peacetime constitute a violation of several principles of international law. This rationale is also accepted in the case of peacetime cyberespionage activities. A state targeted by cyber operations which are attributable to another state and constitute an internationally wrongful act, but do not amount to an armed attack, may respond with acts of retorsion or non-forcible countermeasures.

Keep in mind the explanations made by the Canadian Federal Court in 2007, “binding customary principles of ... international law prohibit interference with the

²³⁵ Ibid.

²³⁶ Schmidt, **Tallinn Manual**..., 18

²³⁷ Schmidt, **Tallinn Manual**..., 78.

²³⁸ Ibid.

sovereignty and domestic affairs of other states.”²³⁹ Equivalent attitude is embedded by the Tallinn Manual, under article 4, which states that “any interference by a state with cyber infrastructure aboard a platform, wherever located, that enjoys sovereign immunity constitutes a violation of sovereignty.”²⁴⁰

As it is stated under article 6 of the Tallinn Manual, “a state bears international legal responsibility for a cyber operation attributable to it and which constitute a breach of an international obligation.”²⁴¹ Similarly, according to article 9 of the Tallinn Manual, “a state injured by an internationally wrongful act may resort to proportionate countermeasures, including cyber countermeasures, against the responsible State.”²⁴²

Those principles of international law constitute a legal basis for invoking the breach of an international obligation and responsibility of states for internationally wrongful acts due to being targeted by cyberespionage activities.

(1) Prohibition on Use of Force

Pursuant to Article 2/4 of the UN Charter, “all members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations.” This prohibition is prescribed to achieve the purpose of the United Nations as it is laid down under article 1, by stating that “to maintain international peace and security.” The UN Charter did not provide any criteria to define such kinds of acts that amount to a use of force. The scale and effects test, proposed in the Nicaragua Case of ICJ, is considered to be an appropriate tool for determining whether an act amounts to an armed attack or not.²⁴³

Regarding whether cyberespionage or cyber attacks can be considered an armed attack, there are two different views. The first view accepts that cyber operations cannot amount to an armed attack since Article 2/4 has been interpreted restrictively to only prohibit conduct that produces human casualties and destruction

²³⁹ Supra n.56.

²⁴⁰ Schmidt, *Tallinn Manual*..., 23.

²⁴¹ Schmidt, *Tallinn Manual*..., 29.

²⁴² Schmidt, *Tallinn Manual*..., 36.

²⁴³ ICJ, *Military and Paramilitary Activities in and Against Nicaragua*..., par. 195

of property.²⁴⁴ In other words, although the ordinary meaning of “force” is clearly broad enough to include both armed and unarmed forms of coercion, use of force is traditionally understood as “to imply a military attack an armed attack by the organized military, naval or air forces of a state.”²⁴⁵ However, cyber operations are short of producing human casualties and physical harm. Secondly, The *travaux préparatoires* of the UN Charter indicates that the prohibition of use of force was not intended to include economic coercion and political pressures.²⁴⁶ Additionally, article 41 of the UN Charter refers to “interruption of ... communication” as a “measure not involving armed force”, thus, certain type of cyber operations cannot be assessed under the prohibition of article 2/4. In the light of above reasons, cyber operations cannot be regarded as a use of force.

On the contrary, the second view accepts that “cyber operations fall under the prohibition of article 2/4 of the UN Charter once *their effects* are comparable to those likely to result from kinetic, chemical, biological or nuclear weaponry.”²⁴⁷ This approach has also been accepted by International Group of Experts under the Tallinn Manual as it is stated that “a cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force.”²⁴⁸ Support of this view is proposed by two arguments. Firstly, Article 2/4 states only “threat or use of force”, but does not specifically mention the kind of threat or force.²⁴⁹ As highlighted by the International Court of Justice, in its Advisory Opinion on the Legality of the Threat or Use of Nuclear Weapons²⁵⁰, “Article 51 does not refer to specific weapons: it applies to any armed attack, regardless of the weapon

²⁴⁴ See Yoram Dinstein, **War, Aggression and Self Defence** ..., 208 : “an armed attack presupposes a use of force producing (or liable to produce) serious consequences, epitomized by territorial intrusions, human casualties or considerable destruction of property.”

²⁴⁵ Ian Brownlie, **International Law and the Use of Force by States**, Clarendon, (1963) 362

²⁴⁶ A Brazilian proposal to extend the prohibition to “the threat or use of economic measures in any manner inconsistent with the purposes of the United Nations” was rejected at the San Francisco Conference; Documents of the United Nations Conference on International Organization, vol. VI, 1945, pp. 559, 720–721.

²⁴⁷ Ibid, Yoram Dinstein, **War, Aggression and Self Defence**..., 80

²⁴⁸ Michael N. Schmidt (ed.), **Tallinn Manual**..., 47

²⁴⁹ Albert Randelzhofer, ‘Use of Force’ in Rudolf Bernhardt, **Encyclopedia of International Law** Vol. 4 North Holland Publishing (1982) 268; “Corresponding to the prevailing and correct view, force in Art. 2/4 is limited to armed forces. It must be admitted that the wording of Art. 2(4) of the Charter alone gives no clear answer to this dispute. But para. 7 of the Preamble of the Charter states one of the aims of the United Nations to be “that armed force shall not be used, save in the common interest”, and Art. 44 supports the view that the Charter also uses the notion of force in cases where it apparently means armed force. The prevailing view is further supported by the teleological interpretation of Art. 2(4).

²⁵⁰ ICJ, Advisory Opinion on Legality of the Threat or Use of Nuclear Weapons, (1996) ICJ Reports 226, 254.

employed²⁵¹, it does not matter what specific means kinetic or electronic are used to bring it about, but the end result must be that violence occurs or is threatened.”²⁵²

In addition to that, Brownlie asked whether use of weapons such as bacteriological, biological and chemical devices which do not involve any explosive effect” can be amount to use of force?²⁵³ Although academics thought at that time that they should be employed with more orthodox weapons to be qualified as use of force, Brownlie argued that “use of such weapons could be assimilated to the use of force as they are employed for the destruction of life and property.”²⁵⁴ Likewise, Dinniss argues that in order to apply the prohibition of use of force in Charter, unique characteristic of computer network attacks, should be taken into account, as ICJ adopted the same approach in Nuclear Weapons advisory opinion.²⁵⁵ Considering STUXNET as a tailored cyberweapon to target specific SCADA systems, it should be acknowledge that it is designed to be employed destruction of a property. Therefore, “the use of cyber operations as an offensive or defensive tool designed to cause death or injury to persons or the destruction of objects and infrastructure, irrespective of whether such destruction involves physical damage, functional harm, or a combination of both,”²⁵⁶ can be accepted as a use of force.

Secondly, if a cyber attack can create “severe damage to property or even human fatalities (as a result, e.g., of the shutdown of computers controlling waterworks and dams, leading to the flooding of inhabited areas), it would qualify as an armed attack.”²⁵⁷ Therefore, some legal scholars argued that if a cyber attack does not cause harm to persons or physical damage to property, but creates catastrophic, severe

²⁵¹ See Y. Dinstein, ‘Computer Network Attacks and Self-Defense’, *International Law Studies*, Vol 76, (1999) 103.

²⁵² Yoram Dinstein, *War, Agression and Self Defence* ..., 88.

²⁵³ Brownlie, *International Law*..., 362

²⁵⁴ Ibid.

²⁵⁵ Heather Harrison Dinniss, *Cyber Warfare*..., 65.

²⁵⁶ Nils Melzer, *Cyberwarfare and International Law*, UNIDIR, (2011), 7. “Conspicuous examples of a use of “force” within the meaning of article 2(4) of the UN Charter, therefore, would be cyber operations manipulating target computers systems so as to cause a meltdown in a nuclear power station, or opening the floodgates of a dam above a densely populated area, or disabling a busy airport’s air traffic control during bad weather conditions, each with potentially horrendous consequences in terms of death, injury and destruction.”

²⁵⁷ Yoram Dinstein, *War, Agression and Self Defence* ..., 212.

effects²⁵⁸, extremely adverse effects²⁵⁹, such an attack should be qualified as an armed attack. Similarly, according to Melnitzky, “prior to the Internet, looting on such a scale could only have been accomplished by a military occupation. The effects-based approach requires that a cyber attack must cause damage only previous possible by traditional military force is therefore satisfied.”²⁶⁰ In this sense, cyberespionage, which violates confidentiality and integrity of a network as a cyber attack, but also violates commercial secrets, can be categorized as a use of force. In addition to that, it should be underlined that article 2/4 of the UN Charter prohibits the use of force regardless of its gravity, magnitude, scale or duration”.²⁶¹ ICJ has noted this fact in Nicaragua Case, by stating that even minor act of interstate force is prohibited under the article 2/4 of the UN Charter.²⁶²

It should also be noted that the militarization of cyberspace is a well-known fact.²⁶³ Due to strategic or military concerns, many States have or want to acquire

²⁵⁸ Schmidt, **Tallinn Manual...**, 55-56: “The classical scenario illustrating the division of opinion (among experts on this issue) is a cyber incident directed against the New York Stock Exchange that causes the market to crash. Experts were divided over the characterisation of such an event. Some of the Experts were unprepared to label it as an armed attack because they were not satisfied that mere financial loss constitutes damages for this purpose. Others emphasized the catastrophic effects such a crash would occasion and therefore regards them as sufficient to characterise the cyber operation as an armed attack. By the same approach, a cyber operation directed against major components of a State’s critical infrastructure that causes severe, albeit not destructive, effects would qualify as an armed attack.”

²⁵⁹ Marco Roscini, **Cyber Operations and the Use of Force...**, 55.

²⁶⁰ Alexander Melnitzky, ‘**Defending America Against Chinese Cyber Espionage Through The Use Of Active Defenses**’ 20 *Cardozo Journal of International Comparative Law* (2012) 566; Fort he opposing view that cyberespionage cannot be qualified as use of force, because there is insufficient State practice see: Russell Buchan, ‘**Cyberattacks: Unlawful uses of force or prohibited interventions?**’ 17 *Journal of Conflict and Security Law* (2012) 211. Russel Buchan, ‘Cyber espionage and international law’, in Nicholas Tsagourias and Russell Buchan (eds.), **Research Handbook on International Law and Cyberspace**, Edward Elgar Publishing, (2015) 187; David Fidler, ‘**Tinker, Tailor, Soldier, Duqu: Why cyber espionage is more dangerous than you think**’ 5 *International Journal of Critical Infrastructures*, (2012) 28 “no government regards cyber espionage of any kind as a prohibited use of force”.

²⁶¹ Ian Brownlie, **International Law...**, 214 and 432; Yoram Dinstein, **War, Aggression and Self-Defence...**, 175; ICJ, **Corfu Channel** (United Kingdom of Great Britain and Northern Ireland v. Albania) (Merits), **Separate Opinion by Judge Alvarez**, 1949, 47. “the minesweeping operation undertaken by British ships in the Corfu Strait, was in fact a violation of Albanian sovereignty. The Court must reaffirm, as often as the occasion arises, that intervention and all kind of forceable action are not permissible, in any form or on any pretext in relations between States.”

²⁶² ICJ, **Military and Paramilitary Activities in and against Nicaragua**, par. 195: “sending by or on behalf of a State of armed bands, groups, irregulars or mercenaries, which carry out acts of armed force against another State of such gravity as to amount to” (inter alia) an actual armed attack conducted by regular forces, “or its substantial involvement therein. *Court does not believe that the concept of “armed attack” includes not only acts by armed bands where such acts occur on a significant scale but also assistance to rebels in the form of the provision of weapons or logistical or other support.* Such assistance may be regarded as a threat or use of force, or amount to intervention in the internal or external affairs of other States. It is also clear that it is the State which is the victim of an armed attack which must form and declare the view that it has been so attacked.

²⁶³ Myriam Dunn Cavelty, **The Militarisation of Cyberspace: Why Less May Be Better**, NATO CCD COE Publications, (2012); Myriam Dunn Cavelty, “**The Militarisation of Cyber Security as a Source**

offensive cyber weapons, have set up cyber commands within their military organization and adopt cyber warfare programs or manuals.²⁶⁴ In this regard, in the presence of such practices of States, arguing legally cyber operations can be considered as use of force has solid basis. We support and side with second view the recognition of cyber operations as a form of use of force, as Dinstein states that, “from a legal perspective, there is no reason to differentiate between kinetic and electronic means of attack. A premeditated destructive CNA can qualify as an armed attack just as much as a kinetic attack bringing about the same-or similar-results. The crux of the matter is not the medium at hand (a computer server in lieu of, say, an artillery battery), but the violent consequences of the action taken. If there is a cause and effect chain between the CNA and these violent consequences, it is immaterial that they were produced by high rather than low technology.”²⁶⁵

A cyber operations need not amount to use of force within the meaning of article 2/4 of the UN Charter to be internationally wrongful, such operations can violate certain obligations and principles of customary international law either.

(2) Internationally Wrongful Act

States are considered responsible for their internationally wrongful acts.²⁶⁶ In 2001, the International Law Commission adopted draft articles on the responsibility of

of Global Tension”, Strategic Trends Analysis, Center for Security Studies, 2012. Kristin Bergtora Sandvik, **Towards a Militarization of Cyberspace? Cyberwar as an Issue of International Law**, PRIO Papers, (2012); Jens Ringsmose and Karsten Friis, **Conflict in Cyber Space**, Routledge, (2016).

²⁶⁴ Countries having cyber command so far, United States, United Kingdom, South Korea, China, NATO based in Tallinn, Germany, India, Iran, Russia, Israel, Netherlands, France, Turkey. Jennifer Valentino-Devries and Danny Yadron, **Cataloging the World’s Cyberforces**, Wall Street Journal, 11 October 2015 : The Journal’s research shows: 29 countries now have formal military or intelligence units dedicated to offensive cyberefforts. 49 countries have bought off-the-shelf hacking software. 63 countries use cybertools for surveillance, either domestically or internationally.

²⁶⁵ Yoram Dinstein, **Computer Network Attacks and Self-Defense**, International Law Studies Vol 76, US Naval War College, (2002), 103.

²⁶⁶ US Department of State, **Digest of United States Practice in International Law**, Chapter 18, (2014), 19 “A State is responsible for an internationally wrongful act when there is an act or omission that is attributable to it under international law that constitutes a breach of an international obligation of the State. *Cyber activities may constitute internationally wrongful acts if they are inconsistent with a primary rule of international law and are attributed to a State under the secondary rules on State responsibility.* A State is legally responsible for cyber activities undertaken through “proxy actors” who act on the State’s instructions or under its direction or control. If a State exercises a sufficient degree of control over a person or group of persons committing an internationally wrongful act, the State assumes responsibility for the act just as if the State had committed the act itself. These rules apply to conduct

states for internationally wrongful acts. Although it is not a binding document, it set out the principles and norms on this topic. The very first articles defined the elements of internationally wrongful acts. There is an internationally wrongful act of a state when conduct consisting of an action or omission 1) is attributable to the state under international law and 2) constitutes a breach of an international obligation of the state.²⁶⁷

Moreover, cyberespionage activities can be legally categorized under internationally wrongful acts due to contradiction between well-established international law principles, territorial sovereign equality and non-intervention.²⁶⁸ Illegality of the cyberespionage may result from violation of any obligation under international law. “Interstate computer network exploitation for the purposes of intelligence gathering, electronic dissemination of hostile propaganda, or denial of service attacks”²⁶⁹ can be considered as a violation of the sovereignty of the targeted State and the customary principle of non-intervention, even if they do not qualify as a use of force within the meaning of article 2(4) of the UN Charter. Similarly, “nondestructive cyber operations intruding into computer-based archives, documents and correspondence of a foreign diplomatic mission, or interfering with the mission’s free communication,”²⁷⁰ is violate international obligations of the receiving state under Vienna Convention on Diplomatic Relations.²⁷¹

Both the Permanent Court of International Justice (PCIJ) and the International Court of Justice (ICJ) applied the principles of the Responsibility of States for Internationally Wrongful Acts as that which “every internationally wrongful act of a State entails the international responsibility of that State.”²⁷² For instance, in the

online just as they do offline, and they ensure that States cannot hide behind putatively private actors in engaging in internationally wrongful conduct.”

²⁶⁷ Yearbook of the International Law Commission, **Draft articles on Responsibility of States for Internationally Wrongful Acts**, with commentaries, (2001) Vol. 2 part 2 art 2.

²⁶⁸ Catherine Lotrionte, **Countering State-Sponsored Cyber Economic Espionage Under International Law**, North Carolina Journal of International Law (2014) 496 “economic espionage, as a highly intrusive coercive act into the economic and political freedoms of a state, may constitute a wrongful act of intervention in violation of the customary norm” The use of countermeasures can provide states with a legal basis for effective responses to economic espionage, buying time for the potential establishment of international consensus to prohibit cyber methods of IP theft for competitive advantage through a new treaty, state practice, or new interpretations of WTO agreements as applicable to economic espionage.

²⁶⁹ Nils Melzer, **Cyberwarfare...**, 9

²⁷⁰ Ibid

²⁷¹ Vienna Convention on Diplomatic Relations, arts. 24, 27 and 45(a).

²⁷² Yearbook of the International Law Commission, **Draft articles on Responsibility of States for Internationally Wrongful Acts**, with commentaries, (2001) Vol. 2 part 2 art 1.

Phosphates in Morocco case, the PCIJ underlined the fact of an internationally wrongful act against another state.²⁷³ The *Corfu Channel* case is significant for cyberespionage because the ICJ stated that “nothing was attempted by the Albanian authorities to prevent the disaster. These grave omissions involve the international responsibility of Albania.”²⁷⁴ Attributing an omission and its legal consequences to a state is providing a viable analogy for cyberespionage operations, because most of the time states are acting reluctantly to take preventive measures against criminal networks responsible for cyber attacks.

In the *Rainbow Warrior* case, the arbitral tribunal concluded that “in the international law field there is no distinction between contractual and tortious responsibility, so that any violation by a State of any obligation, of whatever origin, gives rise to State responsibility and consequently, to the duty of reparation.”²⁷⁵ This interpretation also covers the general principles of international law such as territorial integrity and non-intervention. The interpretation of international wrongful acts by the ICJ was widened in later years. In the *Barcelona Traction* case, the ICJ noted that “an essential distinction should be drawn between the obligations of a State towards the international community as a whole and those arising *vis-à-vis* another State. By their very nature the former are the concern of all States. In view of the importance of the rights involved, all States can be held to have a legal interest in their protection; they are obligations *erga omnes*.”²⁷⁶

Apart from attribution problems, if a state engages in activities neither prohibited nor regulated by international law such as espionage, state responsibility can only be asserted if such activities violate other norms of international law, such as, protection of diplomatic communication, good faith while concluding a treaty, etc. Thus, the legal base for asserting illegality of espionage should be linked to existing international law principles, norms and values either *jus cogen* norms or *erga omnes* obligations.

The breach of international obligation has two distinctive legal consequences. First of all, “the State responsible for the internationally wrongful act is under an

²⁷³ PCIJ., *Phosphates in Morocco*, (Judgment), (1938), Series A/B, No. 74, 10 http://www.icj-cij.org/pcij/serie_AB/AB_74/01_Phosphates_du_Maroc_Arret.pdf accessed 21 July 2015

²⁷⁴ ICJ, *Corfu Channel Case* (UK vs. Albania), (1949) par. 23.

²⁷⁵ *Rainbow Warrior* (New Zealand v France) (1990) 278 http://legal.un.org/riaa/cases/vol_XX/215-284.pdf accessed 21 July 2015.

²⁷⁶ The *Barcelona Traction* (Belgium v. Spain) (1970) 32 <http://www.icj-cij.org/docket/files/50/5387.pdf> accessed 21 July 2015.

obligation: (1) to cease that act, if it is continuing; (2) to offer appropriate assurances and guarantees of non-repetition, if circumstances so require.”²⁷⁷ Secondly, “the responsible State is under an obligation to make full reparation for the injury caused by the internationally wrongful act. Injury includes any damage, whether material or moral, caused by the internationally wrongful act of a State.”²⁷⁸ Furthermore, the responsible state is under obligation to “re-establish the situation which existed before the wrongful act was committed”²⁷⁹ and the responsible state is under obligation to “compensate for the damage caused thereby, insofar as such damage is not made good by restitution.”²⁸⁰ Finally, if restitution or compensation becomes adequate, the responsible state is under obligation to “give satisfaction for the injury.”²⁸¹

On the other hand, internationally wrongful acts create new rights on behalf of injured states. The injured or targeted states have the right to invoke responsibility,²⁸² but limited rights to take countermeasures.²⁸³ Article 46 is well-tailored especially for global mass surveillance or espionage activities conducted without any limitations; “where several States are injured by the same internationally wrongful act, each injured State may separately invoke the responsibility of the State which has committed the internationally wrongful act.”²⁸⁴

This legal ground can be invoked by other states which faced the same internationally wrongful act. For instance, in relation to mass surveillance communications’ content and metadata, intelligence gathering activity, “amounts to a systematic interference with the right to respect for the privacy of communications, and requires a correspondingly compelling justification.”²⁸⁵ As stated in the Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, “bulk access technology is

²⁷⁷ Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries, YILC (2001) Vol. 2 part 2 art 30.

²⁷⁸ Ibid. art 31.

²⁷⁹ Ibid. art 35.

²⁸⁰ Ibid. art 36.

²⁸¹ Ibid. art 37.

²⁸² Ibid. art 42-48.

²⁸³ Ibid. art 49-53.

²⁸⁴ Ibid. art 46.

²⁸⁵ UN Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism (23 September 2014) A/69/397 para 59 <http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N14/545/19/PDF/N1454519.pdf?OpenElement> accessed 15 July 2015.

indiscriminately corrosive of online privacy and impinges on the very essence of the right guaranteed by the UN's International Covenant on Civil and Political Rights.”²⁸⁶

To this end, Article 49 of the draft articles of the Responsibility of States for Internationally Wrongful Acts states that “an injured State may only take countermeasures against a State which is responsible for an internationally wrongful act in order to induce that State to comply with its obligations.” In this regard, countermeasure and retorsion will be discussed in the next part.

(a) Countermeasures against Cyberespionage

Considering industrial and economic cyberespionage activities as economic warfare,²⁸⁷ cyber-based countermeasures or non-cyber based countermeasures can be adopted against states that constitute internationally wrongful acts.²⁸⁸

Pursuant to Article 51 of the draft articles of the Responsibility of States for Internationally Wrongful Acts, “countermeasures must be commensurate with the injury suffered, taking into account the gravity of the internationally wrongful act and the rights in question.” Therefore, countermeasures must meet the requirements of necessity and proportionality, but also must be designed to induce the state to return to compliance with its international obligations. According to Article 52, before taking countermeasures, an injured state shall: (a) call on the responsible State, to fulfil its obligations, (b) notify the responsible state of any decision to take countermeasures and offer to negotiate with that state. However, even before following the above procedure, the injured state may take such urgent countermeasures as are necessary to preserve its rights. With regard to Article 53, countermeasures shall be terminated as soon as the responsible state has complied with its obligations.

The International Law Commission categorized countermeasures as sanctions, retorsion and reprisal. While retorsion is a lawful response to a wrongful act, reprisal

²⁸⁶ Ibid. para 59.

²⁸⁷ Karl Zemanek, ‘Economic Warfare’ in Rudolf Bernhardt, **Encyclopedia of International Law** Vol. 3 North Holland Publishing (1981) 158: “Generally speaking, the term economic warfare indicates a hostile relationship between two or more States in which at least one endeavours to damage the economy of the other(s) for economic, political or military ends. The term is further used to describe the sum of measures and countermeasures which the States involved take in this context.”

²⁸⁸ US Department of State, **Digest of United States Practice**..., 20.

is a reaction to an internationally wrongful act by the injured party against the offending state and generally involves the use of force.²⁸⁹ Applying a cyber blockade or cyber containment in order to paralyze whole IT systems and related infrastructures can qualify as cyber bases countermeasures.

(b) Retorsion against Cyberespionage

As Shaw explained “retorsion is the adoption by one state of an unfriendly and harmful act, which is nevertheless lawful, as a method of retaliation against the injurious legal activities of another state.”²⁹⁰ In other words retorsion remains within the boundaries of law.²⁹¹ According to the ILC, any kind of action categorized as retorsion aims to deprive the responsible state of advantages from its offense.²⁹² To illustrate, retorsion can be breaking diplomatic relations, reducing economic support, imposing trade restrictions, or visa requirements.²⁹³ The ILC illustrated acts of retorsion as “limitation upon normal diplomatic relations, or other contacts, embargoes of various kind or withdrawal of voluntary aid programmes.”²⁹⁴ Schachter mentions that typical examples of retorsion include “rupture of diplomatic relations, cessation of trade in general or in specific areas, non-recognition of acts of the offending government, denial of benefits of available to the offending government, curtailment of migration from offending government.”²⁹⁵

After the Snowden revelations, many countries passed new regulations or amended existing laws to oblige U.S. technology firms to comply with provisions

²⁸⁹ **Yearbook of International Law Commission**, Vol. II (1) Third Report on State Responsibility, A/CN.4/440 (1991) par. 24-25

²⁹⁰ Malcolm N. Shaw, **International Law**, (Cambridge 6th edition, (2008) 1128

²⁹¹ Jan Klabbers, **International Law**, Cambridge, (2013) 168

²⁹² **Yearbook of International Law Commission**, Vol. II (1) Third Report on State Responsibility, A/CN.4/440 (1991) par. 16-17,

²⁹³ Malcolm N. Shaw, **International Law**., 1128 “...expulsion or restrictive control of aliens, as well as various economic and travel restriction.”

²⁹⁴ Commentaries on the Draft Articles on Responsibility of States for Internationally Wrongful Acts, **Yearbook of International Law Commission**, Vol. II (2) (2001) 128.

²⁹⁵ Oscar Schachter, **International Law in Theory and Practice**, Martinus Nijhoff Publishers, (1991), 198. See also, Antonio Cassese, **International Law**, Oxford University Press (2001), 244: According to the Cassese retorsion is “any retaliatory act by which a State responds, by an unfriendly act not amounting to a violation of international law, to either (a) a breach of international law or (b) an unfriendly act by another State.” He gives examples of “the breaking off of diplomatic relations, discontinuance or reduction of trade/ investment, withholding economic assistance, expulsion of nationals, heavy fiscal duties on goods from the offending State, strict passport regulations”.

prohibiting data about their citizens from being transferred to other countries. According to Castro, “new regulations could cost U.S. IT services companies up to \$35 billion in revenue over the next three years.”²⁹⁶ To illustrate, Brazil, initially announced that the Microsoft Outlook service will not be used anymore, and then a German company decided to use Deutsche Telekom rather than a U.S.-based company for cloud computing services.²⁹⁷

(c) Legal Rationale

The fundamental question with regard to internationally wrongful acts and economic cyberespionage and setting up the legal rationale between them, whether economic espionage is sufficient and effective for invoking the principles of states’ responsibility. The basic legal argument to invoke state responsibility with regard to economic cyberespionage is state sovereignty, which also covers the very concept of economic sovereignty. Whether the operation targets public or private infrastructure, states enjoy sovereignty on both of them. According to Schmidt, a target state can invoke the principle of sovereignty if only “*the cyber operation destroys or alters data or somehow makes the cyber infrastructure operate in a manner in which it is not intended to operate.*”²⁹⁸ In other words, if physical damage or injury occurs, then the targeted state can invoke the principle of sovereignty against the targeting state. However, cyberespionage activities, even if such activities was conducted only for monitoring networks, it creates damage to targeted state.

²⁹⁶ Daniel Castro, **How Much Will PRISM Cost the U.S. Cloud Computing Industry?**, Information Technology & Innovation Foundation, August 2013; Michael Hickins, **Spying Fears Abroad Hurt U.S. Tech Firms**, Wall Street Journal, 3 February 2014, <http://online.wsj.com/news/articles/SB10001424052702303743604579350611848246016>; Elizabeth Dwoskin, New Report: Snowden Revelations Hurt U.S. Companies, Wall Street Journal Digits Blog, 30 July 2014 <http://blogs.wsj.com/digits/2014/07/30/new-report-snowden-revelations-hurt-u-s-companies/>

²⁹⁷ Claire Cain Miller, Revelations of N.S.A. Spying Cost U.S. Tech Companies, New York Times, 21 March 2014, <http://www.nytimes.com/2014/03/22/business/fallout-from-snowden-hurting-bottom-line-of-tech-companies.html>

²⁹⁸ Michael N. Schmidt, ‘Cyber Responses “By The Numbers” in International Law’ (2015) EJIL <http://www.ejiltalk.org/cyber-responses-by-the-numbers-in-international-law/> accessed 15 July 2015; (according to Findler, economic espionage do not constitute internationally wrongful acts at all to trigger state responsibility. See, David P. Fidler, ‘Economic Cyber Espionage and International Law: Controversies Involving Government Acquisition of Trade Secrets through Cyber Technologies’ 17 (10) ASIL (2013) <http://www.asil.org/insights/volume/17/issue/10/economic-cyber-espionage-and-international-law-controversies-involving> accessed 15 July 2015.

A targeted state should implement additional protection mechanisms because all of the existing cyber defense structures have been breached. For instance, after data breaches, *Petrobras* initiated a new data protection program costing “R\$3.9bn in security with 3000 employees engaged in the area.”²⁹⁹ Additionally, according to the report published by the Center for Strategic and International Studies, it is estimated that cybercrime and economic espionage cost \$445 billion annually to the world economy.³⁰⁰ Secondly, economic costs and effects of a breach occur sometimes in the long run. For instance, the F-35 Lightning II Joint Strike Fighter program of was seriously damaged and costs were increasing steadily over time due to alleged Chinese economic cyberespionage operations.³⁰¹

To this end, economic cyberespionage operations actually create damage to the targeted state and provide enough legal basis for asserting violation of state sovereignty, which triggers state responsibility under internationally wrongful acts. Lastly, economic cyberespionage operations might violate treaty law obligations which allow the targeted state to invoke legal mechanisms under treaty law.

(3) International Treaty Law and Cyberespionage

In 2013, Timor-Leste lodged a complaint against Australia and claimed that Australia was conducting espionage during the negotiations of a treaty between Australia and the Democratic Republic of Timor-Leste on Certain Maritime Arrangements in The Timor Sea (CMATS) in 2004.³⁰² Timor-Leste argued that Australia bugged cabinet offices of the Timor-Leste government during the

²⁹⁹ Joe Leahy, ‘Brazil’s Petrobras to invest heavily in data security’ (Financial Times, 18 September 2013) <http://www.ft.com/cms/s/0/f3195d0a-2081-11e3-9a9a-00144feab7de.html#axzz3hzSQnxdS> accessed 15 July 2015.

³⁰⁰ McAfee, ‘Net Losses: Estimating the Global Cost of Cybercrime’ (June 2014) <http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf> accessed 15 July 2015.

³⁰¹ David Alexander, ‘Theft of F-35 design data is helping U.S. adversaries – Pentagon’ (Reuters, 19 Jun 2013) <http://www.reuters.com/article/2013/06/19/usa-fighter-hacking-idUSL2N0EV0T320130619> accessed 15 July 2015; Pierluigi Paganini, ‘Snowden reveals that China stole plans for a new F-35 aircraft fighter’ (19 January 2015) <http://securityaffairs.co/wordpress/32437/intelligence/china-stole-plans-f-35-aircraft.html> accessed 15 July 2015; Plans of F-35, Der Spiegel <http://www.spiegel.de/media/media-35687.pdf> accessed 15 July 2015.

³⁰² **Treaty between Australia and The Democratic Republic of Timor-Leste on Certain Maritime Arrangements in The Timor Sea** (adopted 12 January 2006, entry into force, 23 February 2007) ATS 12; Austl. Minister for For. Aff. & Spec. Minister of State, ‘Arbitration under the Timor Sea Treaty’ (3 May, 2013) http://foreignminister.gov.au/releases/2013/bc_mr_130503.html.

negotiations for a petroleum and gas treaty in 2004, so the treaty should be declared void or invalid. However, shortly after the declaration of independence of Timor-Leste, the government of Australia declared that, “it recognizes as compulsory ipso facto and without special agreement, in relation to any other State accepting the same obligation, the jurisdiction of the International Court of Justice in conformity with paragraph 2 of Article 36 of the Statute of the Court.”³⁰³ In this context, Timor-Leste could not initiate a case before the ICJ, but Timor-Leste instituted arbitral proceedings at the Permanent Court of Arbitration³⁰⁴ in accordance with the Timor Sea Treaty.³⁰⁵

In 2010, it was revealed that the NSA granted the legal authority to intercept communications of 193 governments, intergovernmental organizations and other entities for foreign intelligence purposes, including Timor-Leste.³⁰⁶ Similarly, in 2013, the Australian Security Intelligence Organization (ASIO) seized electronic and paper files from the office of the lawyer representing East Timor in the arbitration tribunal and a key witness in the Timor case, a former spy turned whistle-blower, has been arrested in a separate raid.³⁰⁷

Timor-Leste’s Canberra-based legal adviser, Bernard Collaery stated that:

*“the documents reveal that the Director-General of the Australian Secret Intelligence Service and his deputy instructed a team of ASIS (Australian Secret Intelligence Service) technicians to travel to East Timor in an elaborate plan using Australian aid programs relating to the renovation and construction of the cabinet offices in Dili, East Timor, to insert listening devices into walls to be constructed under an Australian aid program.”*³⁰⁸

³⁰³ **Statute of the International Court of Justice**, <http://www.icj-cij.org/jurisdiction/?p1=5&p2=1&p3=3&code=AU> accessed 21 June 2015.

³⁰⁴ **PCA**, Timor-Leste v. Australia, 2013-16 (2013).

³⁰⁵ Timor Sea Treaty between the Government of East Timor and the Government of Australia, ATS 13 (adopted 20 May 2002 entered into force Apr. 2, 2003).

³⁰⁶ NSA, In the Matter of Foreign Governments, Foreign Factions, Foreign Entities and Foreign-Based Political Organizations (16 July 2010) <https://search.edwardsnowden.com/docs/ExhibitF20140630> accessed 21 July 2015.

³⁰⁷ Mark Colvin, ‘Lawyer representing E. Timor alleges ASIO agents raided his practice’ (ABC, 3 December 2013); Katharine Murphy and Lenore Taylor, ‘Timor-Leste spy case: ‘witness held, and lawyer’s office raided by ASIO’ (Guardian, 3 December 2013) <http://www.theguardian.com/world/2013/dec/03/timor-leste-spy-witness-held-lawyers-office-raided-asio> accessed 21 July 2015. The senior retired Australian Secret Intelligence Service (ASIS) agent, who is a prime witness in the Timorese espionage case against Australia in the international courts, was detained and searched. Whistleblower intended to provide “credible direct evidence” of the bugging of the Timorese cabinet rooms in 2004.

³⁰⁸ Ibid.

On 12 December 2013, Timor-Leste lodged an application before the ICJ and requested the ICJ to declare, “the seizure by Australia of the documents and data violated (1) the sovereignty of Timor-Leste and (2) its property and other rights under international law and that Australia must immediately return the documents and data.”³⁰⁹

A year later, the ICJ declared by twelve votes to four that “Australia shall ensure that the content of the seized material is not in any way or at any time used by any person or persons to the disadvantage of Timor-Leste until the present case has been concluded.”³¹⁰ Furthermore, the ICJ stated that “Australia shall not interfere in any way in communications between Timor-Leste and its legal advisers.”³¹¹

According to this subject, this is the first case which includes cyberespionage, economic espionage and application of international treaty law provisions. Thus, Timor-Leste has several legal grounds while asserting the CMATS treaty is void or invalid, but also illegality of cyberespionage or economic espionage conducted by Australia to gain advanced position in negotiations of the oil and petroleum treaty.

Although there is not any specific reference to cyberespionage or cyber attacks under Vienna Convention, we consider that existing principles under Convention can be violated due to such operations.

(a) Violation of Good Faith Principle

Governing international law principles on treaties, whether bilateral or multilateral, are enshrined under the Vienna Convention on the Law of Treaties (VCLT or the Convention) which concluded in Vienna on 23 May 1969. The Convention set the basic principles to determine what is a treaty, how to conclude, terminate, amend etc.; the scope of the convention was only about the treaties between

³⁰⁹ ICJ, (Timor-Leste v. Australia) (Application) (2013) 5,6. <http://www.icj-cij.org/docket/files/156/17962.pdf> accessed 21 June 2015.

³¹⁰ ICJ, (Timor-Leste v. Australia) (Judgement) (2013) 8. <http://www.icj-cij.org/docket/files/156/18090.pdf> accessed 21 June 2015.

³¹¹ Daniel Hurst, ‘Australia has violated Timor-Leste’s sovereignty, UN court told’ (Guardian, 20 January 2014) <http://www.theguardian.com/world/2014/jan/21/australia-has-violated-timor-lestes-sovereignty-un-court-told> accessed 21 June 2015.

states, not with international other subjects of international law.³¹² According to the Convention:

“Treaty means an international agreement concluded between States in written form and governed by international law, whether embodied in a single instrument or in two or more related instruments and whatever its particular designation.”

This definition indicates several elements for documents to become a treaty. First of all, a treaty has to be international. Secondly, treaties should be concluded between states, which excludes treaties between states and other subjects of international law. The International Court of Justice in the *Anglo-Iranian Oil Company* case, submitted to the court by the U.K. government in 1951, stated that “the text of the Iranian Declaration is not a treaty text resulting from negotiations between two or more States. It is the result of unilateral drafting by the Government of Iran, which appears to have shown a particular degree of caution when drafting the text of the Declaration.”³¹³ Thirdly, treaties should be concluded in written form, which excludes oral agreements. For a text to become a treaty, the Convention set criteria that a treaty should be governed by international law. According to the International Law Commission’s Commentary, the phrase “governed by international law” includes the element of “intention to create obligations under international law.”³¹⁴ Apart from its name, a treaty employs terminology to create legal rights and obligations and expresses the intention of parties to create obligations under international law.

While concluding a treaty, states initiate several rounds of official meetings in order to express their terms and conditions and negotiate on those terms to find common ground. Good faith in negotiations and willingness to conclude a treaty is an international norm. According to D’Amato, the good faith principle requires parties to deal honestly and fairly, represent their motives truthfully, and refrain from taking unfair advantage.³¹⁵ Moreover, there are specific aspects of good faith as *pacta sunt servanda*, abuse of rights and discretion, estoppel and acquiescence, and negotiations

³¹² Anthony Aust, **Modern Treaty Law and Practice** (Cambridge, 2013) 6; **Vienna Convention on the Law of Treaties** (adopted on 22 May 1969, entered into force on 27 January 1980) 1155 UNTS 331 art 1.

³¹³ *Anglo-Iranian Oil Co. Case (United Kingdom v Iran) (Preliminary Objection)* [1951] <http://www.icj-cij.org/docket/files/16/1997.pdf> accessed (2015) 105.

³¹⁴ **ILC, Draft Articles on the Law of Treaties** with commentaries, (1966) 189 http://legal.un.org/ilc/texts/instruments/english/commentaries/1_1_1966.pdf accessed 21 June 2015

³¹⁵ Anthony D’Amato, ‘Good Faith’ in **Encyclopedia of Public International Law** (1992) 599.

in good faith.³¹⁶ Negotiations in good faith are well applicable, especially for pre-contractual espionage activities.

The Vienna Convention obliged parties to perform treaties in good faith³¹⁷ and interpret treaties in good faith.³¹⁸ In addition, the ILC commentary extended the scope of good faith to the period of negotiations stating that “in the case of treaties, there is the special consideration that the parties by negotiating and concluding the treaty have brought themselves into a relationship in which there are particular obligations of good faith.”³¹⁹ The question in this context is whether parties have an obligation to act in good faith in creation of the rights and obligation. In the *Nuclear Tests Case*, the ICJ put an end to this question and stated, “one of the basic principles governing the creation and performance of legal obligations, whatever their source, is the principle of good faith.”³²⁰

Apart from the Vienna Convention, the ICJ strictly underlined the principle of good faith in the *North Sea Continental Shelf* case. In this case, the court declared that “...they were so to conduct themselves that the negotiations were meaningful.”³²¹ Later on, in the *Fisheries Jurisdiction* case, the court underlined that the parties should conduct their negotiations on the basis of good faith.³²² Furthermore, in the *Gabcikovo-Nagymaros Project* case, the ICJ stressed the significance of the good faith principle, especially in negotiations;

“Articles 65 to 67 of the Vienna Convention on the Law of Treaties, if not codifying customary law, at least generally reflect customary international law and contain certain procedural principles which are based on an obligation to act in good faith.”³²³

³¹⁶ Steven Reinhold, ‘*Good Faith in International Law*’, (2013) Paper No 2/2013 7.

³¹⁷ **Vienna Convention on the Law of Treaties** (adopted on 22 May 1969, entered into force on 27 January 1980) 1155 UNTS 331 art 26.

³¹⁸ *Ibid.* art 31.

³¹⁹ **International Law Commission**, Draft Articles on the Law of Treaties with commentaries, (1966) http://legal.un.org/ilc/texts/instruments/english/commentaries/1_1_1966.pdf accessed 21 June 2015, 262.

³²⁰ *Nuclear Tests Case (Australia v France) (Merits)* (1974) para 46.

³²¹ *North Sea Continental Shelf Case (Germany v. Denmark; Germany v. Netherland)* (1969) 75 <http://www.icj-cij.org/docket/files/52/5563.pdf>

³²² *Fisheries Jurisdiction Case (United Kingdom v Iceland) (Merits)* (1974) 94 <http://www.icj-cij.org/docket/files/55/5979.pdf> accessed 21 June 2015.

³²³ *Gabcikovo-Nagymaros Project (Hungary vs Slovakia)* (1997) 63 <http://www.icj-cij.org/docket/files/92/7375.pdf> accessed 21 June 2015.

The obligations contained in Articles 15, 19 and 20 are, by definition, general and have to be transformed into specific obligations of performance through a process of consultation and negotiation. Their implementation thus requires a mutual willingness to discuss in good faith.”³²⁴

In this regard, conducting cyberespionage or economic espionage activities in order to gain vastly superior bargaining power could result in bad faith, while negotiating to conclude a treaty. Therefore, such a treaty may be declared as void or invalid under general principles of international law or customary law of treaties, even if it is signed. However, there is not any legal ground under the Vienna Convention as a failure to negotiate in good faith during negotiations for invoking a treaty as void or invalid. Thus, another legal ground should be adopted for invoking invalidity such as fraudulent conduct.

(b) Invalidity of Treaty by Fraud

The Vienna Convention devotes nine articles on invalidity, articles 46-53 and 64 cover provisions related with invalidity.³²⁵ It is generally accepted that invalidity is rarely applicable.³²⁶ According to Article 49 of the Vienna Convention,

“If a State has been induced to conclude a treaty by the fraudulent conduct of another negotiating State, the State may invoke the fraud as invalidating its consent to be bound by the treaty.”

Fraudulent conduct is not defined under the Vienna Convention. Article 49 purposely does not define fraud; “its precise scope to be worked out in practice and in the decisions of international tribunals.”³²⁷ However, the ILC commentary set out two

³²⁴ Ibid. 68.

³²⁵ Vienna Convention on the Law of Treaties (adopted on 22 May 1969, entered into force on 27 January 1980) 1155 UNTS 331.

³²⁶ Anthony Aust, **Modern Treaty Law and Practice** (Cambridge, 2013) 6 “even though the subject is no importance for the day-to-day work of a foreign ministry. The international Law Commission was well aware that invalidity was a rarity.”; Mark E. Villiger, **Commentary on the 1969 Vienna Convention on the Law of Treaties**, Martinus Nijhoff, (2009) 617 “Fortunately, cases of fraud are rare in international law.”; See Sinclair of the UK delegation, OR 1968 CoW 261, para. 24, “Article 49 might encourage States to invoke grounds of fraud more frequently”.

³²⁷ Humphrey Waldock, Fifth Report on the Law of the Treaties, **Yearbook of the International Law Commission**, 1965, II 11, para. 2; Final Draft, Commentary to Art 46, 244 para 2.

descriptive elements for fraudulent conduct. These elements are fraudulent conduct and the intention to deceive.³²⁸ According to the International Law Commission, the expression of “fraudulent conduct” is designed to include any false statements, misrepresentations or other deceitful proceedings by which a state is induced to give consent to a treaty which it would not otherwise have given.³²⁹ The elements then appears as (1) any false statements, (2) misrepresentations or other deceitful proceedings. Article 49 assumes fraudulent conduct of another negotiating state. Fraud can only relate to conduct in the making of a treaty during its negotiation and up to its conclusion, not in its subsequent performance.³³⁰

Fraud is the antithesis of good faith.³³¹ The prohibition of fraud, derived from good faith, which is a well known principle in domestic law and entered international law via general principles of international law.³³² The definition of fraud in international law is much broader than what is found in domestic law.³³³ It includes deliberately deceitful behavior in the formation of an international agreement.³³⁴ The Harvard Law School’s Draft Convention on the Law of Treaties from 1935, contained a provision on fraud as well; “State which claims that it has been induced to enter into a treaty with another State by the fraud of the latter State, may seek from a competent international tribunal or authority a declaration that the treaty is void.”³³⁵ It is also stated that this is a willful intent to deceive another.³³⁶

Article 44 of the Convention regulates the separability of treaty provisions:

“In cases falling under articles 49 and 50 the State entitled to invoke the fraud or corruption may do so with respect either to the whole treaty or, subject to paragraph 3, to the particular clauses alone.”

³²⁸ André Oraison, *Le dol dans la conclusion des traités*, *Revue Générale de Droit International*, (1971), 630.

³²⁹ ILC, *Draft Articles on the Law of Treaties with commentaries*, (1966) 245 http://legal.un.org/ilc/texts/instruments/english/commentaries/1_1_1966.pdf accessed 21 June 2015;

³³⁰ Mark E. Villiger, *Commentary ...*, 618 ; Statement in Vienna by the Italian delegation, OR 1968 CoW 262, para. 37.

³³¹ Cheng Bin, *General Principles of Law as Applied by International Courts and Tribunals*, Cambridge University Press, (1953) 158.

³³² Mark E. Villiger, *Commentary ...*, 619.

³³³ Donald K. Anton, ‘*Arbitrating the Treaty on Certain Maritime Arrangements in the Timor Sea*’, ANU College of Law Research Paper No. 13-20, (2013), 4.

³³⁴ Paul Reuter, *Introduction to the Law of Treaties*, Routledge (1989), 137-38.

³³⁵ Supplement 1144. Article 31, para. (a) of the Harvard Draft.

³³⁶ *Ibid.*

It emphasizes that in cases falling under articles 49 and 50 the state is entitled to invoke the fraud or corruption may do so with respect either to the whole treaty or to the particular clauses alone. In particular, in a case of alleged invalidity according to these provisions, the ground of invalidity may be invoked only by the state which was the victim of the fraud or corruption;³³⁷ and that state has the “permissive right”³³⁸ either to invalidate the entire treaty or solely the particular clauses to which the fraud or corruption relate.³³⁹ The paragraph gives states, which was the victim of fraud or corruption, the possibility to choose between two different options: the option to invoke the invalidity of its consent either with respect to the whole treaty or with respect to particular clauses alone. This provision is based on the idea of favoring the injured state’s party and sanctioning the state’s party, which is held responsible for the fraud.³⁴⁰

However, there is a legal question whether espionage activities amount to ‘fraudulent conduct.’ According to Mitchell and Akande, “access to information in a treaty negotiation that was obtained through espionage may limit the parties’ ability to negotiate freely and fairly”, so such activities apparently become contrary to the principle of good faith and include deception³⁴¹ Similarly, Anton includes espionage activities which aim to obtain classified, confidential and privileged “information in order to gain advantage in treaty negotiations is deceitful behavior.”³⁴²

Cyberespionage or intelligence gathering activities, due to their nature, are based on deception and done for acquiring political, economic and technological advantage. In the case of negotiations, the outcome of espionage activities put one of the parties in a well-informed position and creates information asymmetry, which certainly

³³⁷ ILC Report 1966, **Yearbook of the International Law Commission** 1966 II 238, para. 6.

³³⁸ Statement by Waldock in the ILC, *Yearbook of the International Law Commission*, 1963 I 226, para. 10.

³³⁹ Supra n.228; Waldock Report V, *ibid.* 9, para. 5; the statement by Waldock in the ILC, *Yearbook of the International Law Commission* 1966 I/2 318, para. 57 (“*paragraph 4 simply provided two alternative courses for the State*”).

³⁴⁰ Oliver Dörr, Kirsten Schmalenbach, **Vienna Convention on the Law of Treaties A Commentary**, Springer, (2012) 762-3.

³⁴¹ Kate Mitchell and Dapo Akande, ‘Espionage & Good Faith in Treaty Negotiations: East Timor v. Australia’ (2014) **European Journal of International Law** <<http://www.ejiltalk.org/espionage-fraud-good-faith-in-treaty-negotiations-east-timor-v-australia-in-the-permanent-court-of-arbitration/>> accessed 27 July 2015.

³⁴² Donald K. Anton, ‘The Timor Sea Treaty Arbitration: Timor-Leste Challenges Australian Espionage and Seizure of Documents’ (2014) 18(6) **American Society of International Law** <http://www.asil.org/insights/volume/18/issue/6/timor-sea-treaty-arbitration-timor-leste-challenges-australian-espionage> accessed 27 July 2015.

disrupts other parties' ability to negotiate. In this sense, conducting espionage during negotiations can be categorized under fraudulent conducts and can constitute a legal base for invoking invalidity by fraud according to the Vienna Convention.

(4) WTO Dispute Settlement Mechanism

"After decades of being ignored, trade secret rights have become a hot topic among international trade professionals and businesses alike. A primary driver of the increased attention is concern about foreign and cyber-espionage."³⁴³ Rowe and Sanden asserted that companies need more tools to combat such attacks and the institution of more effective trade secret laws is one possible solution.³⁴⁴ The TRIPS Agreement is a final outcome of the Uruguay Round, the 8th round of multilateral trade negotiations conducted within the framework of the General Agreement on Tariffs and Trade (GATT), which continued from 1986 to 1994, in which 123 countries attended as contracting parties.³⁴⁵

After the publication of several reports underlining Chinese sophisticated cyberespionage campaigns, some scholars have argued that "the victims of Chinese economic espionage should seek to establish clear guidelines and penalties within the World Trade Organization (WTO) system."³⁴⁶ Indeed, in 2014, some U.S. senators demanded U.S. Trade Representatives to initiate a case at the WTO against China for state-backed cyber espionage.³⁴⁷ However, the U.S. has not initiated a WTO complaint against China over this matter. The WTO is a global institution regulating trade negotiations in which WTO agreements cover goods, services and intellectual property, resolving disputes under the Dispute Settlement Understanding if the rights

³⁴³ Elizabeth A. Rowe and Sharon K. Sandeen, **Trade Secrecy ...**, 15

³⁴⁴ Ibid.

³⁴⁵ WTO, **Overview: The TRIPS Agreement**, accessed

www.wto.org/english/tratop_e/trips/intel2_2.htm; for the detailed history of drafting TRIPS, see: Rochelle C. Dreyfuss and Katherine J. Strandburg (eds), **The Law and Theory of Trade Secrecy: A Handbook of Contemporary Research**, Edgar Elgar Publishing, (2011).

³⁴⁶ Richard Clarke, 'A Global Cyber-Crisis Waiting to Happen' (Washington Post, 07 February 2013) https://www.washingtonpost.com/opinions/a-global-cyber-crisis-in-waiting/2013/02/07/812e024c-6fd6-11e2-ac36-3d8d9dcaa2e2_story.html accessed 27 July 2015.

³⁴⁷ Brian T. Yeh, **Protection of Trade Secrets: Overview of Current Law and Legislation**, Congressional Research Service (2016) 13.

and obligations under the agreements are being infringed.³⁴⁸ The WTO's Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) has several articles about protection of intellectual property rights during the course of international trade. Article 39 of the TRIPS is the first time that protection of trade secrets has appeared in a multilateral treaty.³⁴⁹ Article 39 set out principles to protect undisclosed information and trade secrets. According to the TRIPS:

1. *In the course of ensuring effective protection against unfair competition as provided in Article 10bis of the Paris Convention (1967), Members shall protect undisclosed information in accordance with paragraph 2 and data submitted to governments or governmental agencies in accordance with paragraph 3.*
2. *Natural and legal persons shall have the possibility of preventing information lawfully within their control from being disclosed to, acquired by, or used by others without their consent in a **manner contrary to honest commercial practices** so long as such information:*
 - (a) is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question;*
 - (b) has commercial value because it is secret; and*
 - (c) has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret.*³⁵⁰

Article 39/2 defines three requirements for information to be classified as undisclosed information or trade secrets. Article 39/2 states that information is protectable if it: (a) is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information

³⁴⁸ WTO, What We Do, https://www.wto.org/english/thewto_e/whatis_e/what_we_do_e.htm accessed 27 July 2015.

³⁴⁹ Francois Dessemontet, 'Arbitration and Confidentiality', 7 American Review of International Arbitration (1996) 307.

³⁵⁰ WTO, **Agreement on Trade-Related Aspects of Intellectual Property Rights** (adopted 15 April 1994, came in to effect 1 January 1995) art. 39 https://www.wto.org/english/docs_e/legal_e/27-trips.pdf accessed 27 July 2015.

in question; (b) has commercial value because it is secret; and (c) has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret.

In this sense, Article 39/2 did not give any definition about manners contrary to honest commercial practices, generally known, readily accessible, commercial value etc., so it is left for the legislatures and courts of each country to identify the terms and acts which are deemed dishonest.³⁵¹ However, footnote 10 to Article 39/2 states that a manner contrary to honest commercial practices shall mean at least practices such as: (1) breach of contract, (2) breach of confidence, (3) inducement to breach and (4) the acquisition of undisclosed information by third parties who knew, or who were grossly negligent in failing to know, that such practices were involved in the acquisition.³⁵² As in the commentary, “a manner contrary to honest commercial practices” has been explained as, “breach of contract, breach of confidence and inducement to breach, and includes the acquisition of undisclosed information by third parties who knew, or were grossly negligent in failing to know, that such practices were involved in the acquisition.”³⁵³

The WTO Agreement includes dispute settlement provisions that allow member states of the WTO to bring actions against other countries which violate or are not in compliance with the terms of the WTO Agreement.³⁵⁴ According to Article 64 of the TRIPS, “the provisions of Articles XXII and XXIII of GATT 1994 as elaborated and applied by the Dispute Settlement Understanding shall apply to consultations and the settlement of disputes under this Agreement except as otherwise specifically provided herein.”³⁵⁵ Therefore, any member states of the WTO which do not comply with the provisions of Article 39 of the TRIPS Agreement may bring forward the WTO Agreement’s dispute settlement process.³⁵⁶ The WTO dispute settlement system is

³⁵¹ Elizabeth A. Rowe and Sharon K. Sandeen, **Trade Secrecy....**, 30

³⁵² 1) a contract that promises confidentiality 2) an obligation not based upon a contract 3) inducement of a breach of a duty to maintain secrecy 4) referring to the previous three wrongful acts.

³⁵³ Supra 320.

³⁵⁴ Marrakesh Agreement Establishing the World Trade Organization, 15 April 1994. Dispute Settlement Understanding, Annex 2.

³⁵⁵ Supra 320.

³⁵⁶ Rufus Yerxa, ‘The Power of the WTO Dispute Settlement System’ in Rufus Yerxa and Bruce Wilson (eds.), **Key Issues in WTO Dispute Settlement**, Cambridge University Press, (2005), 4 “The dispute settlement system works on the basis of contractual remedies. What this means is that the violation of WTO rules by one Member gives adversely affected Members the right to withdraw some equivalent value of commitments in order to rebalance their respective rights and obligations. Please note that I said it gives them the right! However, the decision to ‘retaliate’ is entirely up to the aggrieved Member itself, just as the decision to correct a violation rests on the sovereign decision of the violator. Thus, the

codified in the Understanding on Rules and Procedures Governing the Settlement of Disputes.³⁵⁷

The WTO dispute settlement is a government to government procedure in which only WTO members themselves may invoke WTO rights and enforce WTO obligations against other members.³⁵⁸ The WTO dispute settlement is a four-stage procedure consisting of a mandatory consultation stage, a panel stage, an appellate stage, and an implementation/compliance stage. In the mandatory 60 day consultation stage, Complainant State should notify the other Member and the entire WTO membership of the nature of its complaint and any alleged violation of the WTO rule. If consultations fail the complaining member may then request and is entitled to have its complaint heard by a panel normally composed of three, and exceptionally five, experts selected on an ad hoc basis.³⁵⁹ If the panel finds that there are WTO violations, it recommends to the responding party to bring its disputed measures into conformity with its WTO obligations.

Panel proceedings are supposed to take no more than nine months.³⁶⁰ Either party can appeal the panel report to the Appellate Body, which has 90 days to issue its own report. Pursuant to Article 17, an appeal shall be limited to issues of law covered in the panel report and legal interpretations developed by the panel. The appellate body may uphold, modify or reverse the legal findings and conclusions of the panel.³⁶¹ Upon the completion of the appellate stage the appellate body, a report is adopted by the Dispute Settlement Body (DSB) and unconditionally accepted by the parties to the

dispute settlement process is merely a means of adjudicating whether a Member has acted contrary to its obligations, and if so, the extent to which other Members might be entitled to 'withdraw equivalent concessions' if the offending Member does not correct the violation. There are elaborate procedures designed to ensure that this 'right' they obtain from a WTO ruling is proportionate and fair. These are some of the basic realities one has to keep in mind when examining the WTO dispute settlement process. The WTO system works only to the extent Members want it to work, and only if they decide that compliance is in their overall economic interest. It therefore rests on the credibility of the rules, and also on the credibility of the dispute settlement decisions."

³⁵⁷ WTO, *A Handbook on the WTO Dispute Settlement System*, Cambridge University Press (2004), 17

³⁵⁸ Bruce Wilson, "The WTO dispute settlement system and its operation: a brief overview of the first ten years", in Rufus Yerxa and Bruce Wilson (eds.), *Key Issues in WTO Dispute Settlement*, Cambridge University Press, (2005) 16 : "If a private actor from a WTO Member (e.g. a company, labour union, trade association, etc.) wishes to activate the WTO dispute settlement system against another WTO Member government, it must first persuade its own government to prosecute a complaint on its behalf against such other WTO Member"

³⁵⁹ WTO, *A Handbook...*, 21

³⁶⁰ Bruce Wilson, "The WTO dispute settlement...", 17

³⁶¹ Annex 2 of the WTO Agreement, Understanding on rules and procedures governing the settlement of disputes (DSU), art 17

dispute unless the DSB decides by consensus not to adopt the appellate body report within 30 days following its circulation to the members. “Adoption by the DSB gives legal effect to the report or reports and a Member whose measures have been found in violation of its WTO obligations is expected to take such steps as necessary to bring the WTO-inconsistent measures into compliance with the relevant applicable WTO agreement.”³⁶² However, cases relating to “undisclosed information” are rare and a complaint involving Article 39 has occurred only once, and that case was eventually withdrawn after the parties (China and the European Communities) reached an agreement in the form of a Memorandum of Understanding.³⁶³

According to Fidler, obligations created by the WTO is only effective and binding not the outside, but within the territories of the parties.³⁶⁴ In other words, the targeted state should establish the link between responsibility of the targeting state and economic cyberespionage. Moreover, Fidler believes that the WTO is not an appropriate forum to solve economic cyberespionage problems legally, but is appropriate to “put political pressure on States through this high-profile diplomatic forum.”³⁶⁵

On the contrary, the preamble of the TRIPS Agreement stated the purpose of the agreement as to “reduce distortions and impediments to international trade... and promote effective and adequate protection of intellectual property rights.”³⁶⁶ From that point, Skinner underlined that cyber violations are within the limits of WTO Agreements, and the interpretation of the preamble of the TRIPS Agreement enable the inclusion of economic cyberespionage operations within the agreement.³⁶⁷

In this sense, WTO litigation against the perpetrators of economic cyberespionage is another legal argument in relation to violations of treaty obligations

³⁶² Bruce Wilson, “**The WTO dispute settlement...**”, 18

³⁶³ WTO, Dispute Settlement DS372, available at http://www.wto.org/english/tratop_e/dispu_e/cases_e/ds372_e.htm

³⁶⁴ David P. Fidler, ‘**Economic Cyber Espionage and International Law: Controversies Involving Government Acquisition of Trade Secrets through Cyber Technologies**’ 17 (10) ASIL (2013) <http://www.asil.org/insights/volume/17/issue/10/economic-cyber-espionage-and-international-law-controversies-involving> accessed 15 July 2015.

³⁶⁵ David P. Fidler, ‘**Why the WTO is not an Appropriate Venue for Addressing Economic Cyber Espionage**’ (Arms Control Law, 11 February 2013) <http://armscontrolaw.com/2013/02/11/why-the-wto-is-not-an-appropriate-venue-for-addressing-economic-cyber-espionage/> accessed 27 July 2015.

³⁶⁶ WTO, Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) (adopted 15 April 1994) Preamble.

³⁶⁷ Christina Parajon Skinner, **An International Law Response to Economic Cyber Espionage**, 46 Connecticut Law Review (2014) 1165 1197

and responsibility of states. Establishing the link between perpetrators of cyberespionage and violation of any rights and obligations under TRIPS is still lacking concrete legal argumentation. On the other hand, litigation in this field can be notoriously complicated and expensive, “particularly where highly technical trade secrets are involved and the defense alleges that the information the claimant seeks to protect is in fact widely known.”³⁶⁸ Moreover, Article 39 of TRIPS stipulates and obliged every contracting party to enact appropriate domestic legal mechanisms for trade secret protection and WTO regular follow-up whether those countries have sufficient protection mechanisms. Therefore even we applied literal interpretation for Article 39, it is challenging to assert that only this article is sufficient for tackle with State-State cyberespionage operations. In other words, States can still initiate WTO dispute settlement mechanism against States conducting cyberespionage, however, this process will be challenging for grounding illegality of such operations under existing WTO rules and especially TRIPS articles.

To this end, the WTO dispute resolution mechanism is politically “the most appropriate and effective forum,” but legally parties of the WTO and TRIPS should first agree on international norms and principles explicitly restricting economic cyberespionage operations under WTO Agreements.

E. Concluding Remarks

In light of the above explanations, summarizing some of the fundamental findings is considered to be explanatory. The world has experienced a revolution in information technologies which significantly influence various aspect of society. Firstly, it became easier to generate, transmit and store data. Secondly, the cost of collecting, storing and transmitting data sharply decreased. Therefore, interaction and relation between society and its environment became dependent to technological devices.

Furthermore, espionage has also undergone a transformation due to developments experienced in information technologies. The understanding of war has shifted from total war to hybrid war including cyber activities, insurgencies, and

³⁶⁸ Jon Lang, *The Protection of ...*, 471.

economic warfare. Additionally, purposes and targets, methods and means, actors, and incidents of espionage have been altered as illustrated in Table II-1.

Table 0-1: Comparison of Traditional Espionage and Cyberespionage

	Traditional Espionage	Cyberespionage
Target	• Political Intelligence • Military Intelligence • New weapons systems, military strategies or information about the stationing of troops	• High-Tech Products • Commercial Enterprises • IT, genetics, aviation, lasers, optics, electronics
Purpose	To Gain: • Political Supremacy • Military Supremacy • Tactical Supremacy	To Gain: • Commercial Advantage, • Upper Hand in Negotiations • Technological Advantage
Means/Tools	• Human based Intelligence • Field Operations	• Communication or Signal based Intelligence • Cyber weapons: APT
Actors	• States	• States • Corporations • Criminal Organizations • Hackers

Basically, espionage activities have shifted from human-based intelligence to technology-based intelligence; from times of peace to times of war. Mass collection of data, dragnet applications, cyberespionage and exfiltration became easily accessible tools for not only states, but also for criminal organizations, hackers, etc. Although such activities have legally grounded preventive measures, the national security of states, their targets, purposes, tools, and actors of espionage has altered. In addition to the change observed in features of espionage activities, more importantly they have begun to be deployed frequently in peacetime rather than wartime.

International legal approaches to espionage activities underline that peacetime espionage activities are not prohibited by international law. What is not prohibited is allowed as it was the situation in the *Lotus* case. However, wartime espionage activities are allowed under international law and there is vast literature about state practices.

Table 0-2: Regulation of Wartime Cyber/Espionage

Time	Type	Level	Regulation
Wartime	Espionage	Domestic	Prohibited / Regulated
		International	Allowed / Regulated
	Cyberespionage	Domestic	Prohibited/ Partly Regulated
		International	Allowed /Partly Regulated

Peacetime espionage and cyberespionage activities can be penalized under domestic laws. Targets can be trade secrets and assets protected under regulations relating to intellectual property and protection of trade secrets. Additionally, cyberespionage activities are criminalized under cybercrimes such as unauthorized access and illegal interception. With regard to cyberespionage activities as they aim to gain commercial advantage or upper hand in negotiations, they are also subject to certain sanctions, as a violation of principles such as good faith, fair trade, fair and free negotiations, and economic sovereignty.

Table 0-3: Regulation of Peacetime Cyber/Espionage

Time	Type	Level	Regulation
Peacetime	Espionage	Domestic	Prohibited / Regulated
		International	Allowed / Not Regulated
	Cyberespionage	Domestic	Prohibited / Regulated
		International	Allowed / Partly Regulated

Peacetime cyberespionage activities are not prohibited explicitly by any international legal document. Therefore, it is acknowledged that these activities are allowed under international law. As we have discussed, due to the special nature of economic and industrial cyberespionage, they can provide a basis for state's responsibility with regard to violation of several principles of customary international law. In this legal options such as countermeasure or retorsion can be adopted. With

regard to their targets as high-tech products and trade secrets, such activities are prohibited by the TRIPS Agreement and states are obliged to take necessary legal measures to provide protection for such values. There is also an international obligation that member states of the WTO should fulfill. Allowing any of its subjects to conduct cyberespionage provides that legal protections in the state of question are not sufficient to fulfill WTO obligations.



CONCLUSION

Although technological advancements ease our daily lives and bring new opportunities, they create certain political, economic, legal and technical problems but also new risks and threats. Tackling with those new risks and threats require either adopting new techniques and tools or revision of traditional structures. In order to tackle with new challenges and threats posed by cyberspace and information technologies, cybercrime and cyberespionage many regulations have enacted in domestic regional and international level.

Along with the existing legal structures, new definitions and crimes have been defined, older regulations have been interpreted comprehensively to cover this treat. Existing legal paradigm, in other words traditional legal norms, principles, techniques and tools are tough to be capable of giving answers and solutions to that problem effectively. In this regard, both newly enacted or accepted international law norms and principles and mechanisms can effectively confront with economic cyberespionage legally. However, dynamics of cyberspace is far more different than real life. Therefore, on the one hand changing features of cyberespionage and problems related with attribution and capturing criminals on the other, necessitate new interpretations and new approaches.

In this regard, we have discussed both traditional international law approach regarding espionage and further discussed new regulations relating cyberespionage. In case of economic and industrial cyberespionage, there is traditional legislations to protect commercial assets and newly enacted rules about cybercrime. They intertwine and create a legal barrier for economic and industrial cyberespionage. Lastly, within a decade States created sector specific and subject oriented legislations only for tackling with this issue.

It is estimated that in 2016, Internet economy will be 4.2 trillion U.S. dollar which means new opportunities, cybercrime and economic espionage cost \$445 billion

annually to the world economy which means new threats. The rising phenomenon, economic cyberespionage operations are targeting not only state owned infrastructures and network but also private networks, commercial and corporate databases. There are many reasons for such a motivation. First of all, due to oblivion of international norms of principles in terms of peacetime espionage and existing customary international law patterns on allowing espionage which is limiting our options to confront cyberespionage. Secondly it becomes easier and more efficient in case of cost-benefit analysis to conduct cyberespionage operations to gather strategic commercial information rather than deploying human resources. Thirdly nature and features of the espionage have altered with technological advancements and this ease to adopt cyberespionage operations.

On the international level, domestic legal actions is ineffective way to tackle with economic cyberespionage compering with invoking violation of treaty obligations or initiating WTO litigation. Attribution problem and lack of efficient investigations and extradition of criminals even if they are caught, create a legal ambiguities. Although traditional international law allows countermeasures and retortion under certain conditions, in case of cyberespionage which damages material and non-material assets, counter back option acknowledged as necessary and proportionate even if it is not legal yet. Therefore States resort to the countermeasures and other self-help options.

With regard to the, Timor-Leste vs. Australia case, violation of both treaty law obligations and established international law norms and principles (inviolability of diplomatic premises, good faith in negotiations, state sovereignty and non-intervention) provide concrete legal basis to assert illegality of cyberespionage. However, establishing the legal and factual link between espionage and fraudulent conduct is complex and problematic due to lack of any precedent as such.

To put into a nutshell, tackling with economic and industrial cyberespionage is legally and theoretically possible but in practice legal solutions fall behind the political and technical solutions. Perpetrators can easily develop new techniques and tools to initiate new attacks or adopt alternative routes, proxies which enable to act anonymously. In this context, first there is a need of commonly agreed international

cyber norms on economic and industrial cyberespionage which persuade States such operations are mutually destructible. Secondly most of the States inclined to take extra security measures to protect their digital assets. This is still a viable solution to deter such operations. However, keeping in the mind the mutual destruction and enforce it, States also have to adopt offensive cyber measures such as counter back, for deterrence even if it's legality. Last but not least economic countermeasures and solutions offered by treaty law can be considered as deterrent for cyberespionage operations conducted in peacetime.



BIBLIOGRAPHY

- Aaron Mamiit**, German Government Drops Verizon Contract in Fear of U.S. Espionage, Tech Times (2014).
- A. John Rasad**, ‘The Unresolved Equation of Espionage and International Law’, 28 MJIL (2007).
- Akif Emre Öktem**, Uluslararası Teamül Hukuku, Beta, (2013).
- Alexander Melnitzky**, ‘Defending America against Chinese Cyber Espionage Through The Use Of Active Defenses’ Cardozo Journal of International Comparative Law (2012).
- Ian Brownlie**, International Law and the Use of Force by States, Clarendon, (1963).
- Alonso Soto and Brian Winter**, ‘Saab wins Brazil jet deal after NSA spying sours Boeing bid’ Reuters, (2013).
- Amalie Weber**, ‘The Council of Europe Convention on Cybercrime’, Berkeley Technology Law Journal, 18, (2014).
- André Oraison**, Le Dol Dans La Conclusion Des Traités, Revue Générale de Droit International, (1971).
- Andrew Murray**, Information Technology Law, Oxford (2013).
- Anthony Aust**, Modern Treaty Law and Practice, Cambridge, (2013).
- Anthony D’Amato**, ‘Good Faith’, in Encyclopedia of Public International Law (1992).
- Antonio Cassese**, International Law, Oxford University Press (2001).
- Ariana Eunjung Cha and Ellen Nakashima**, ‘Google China cyberattack part of vast espionage campaign, experts say’ (14 January 2010).
- Ashley Deeks**, An International Legal Framework for Surveillance, Virginia Journal of International Law Vol 55:2 (2015).
- Aslı E. Gürbüz Usluel**, Anonim Şirketlerde Ticari Sırrın Korunması, Vedat, (2009).
- Barton Gellman and Laura Poitras**, ‘U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program’ Washington Post, (2013).
- Brian T. Yeh**, Protection of Trade Secrets: Overview of Current Law and Legislation, Congressional Research Service (2016).

- Catherine Morin-Desailly**, Rapport D'information fait au nom de la mission commune d'information nouveau rôle et nouvelle stratégie pour l'Union européenne dans la gouvernance mondiale de l'Internet, Rapports Parlementaires (2014).
- Catherine Lotrionte**, Countering State-Sponsored Cyber Economic Espionage under International Law, North Carolina Journal of International Law (2014).
- Cheng Bin**, General Principles of Law as Applied by International Courts and Tribunals, Cambridge University Press, (1953).
- Charles Doyle**, Stealing Trade Secrets and Economic Espionage: An Overview of 18 U.S.C. 1831 and 1832, Congressional Research Service Report, (2014).
- Chris Reed**, Internet Law: Text and Materials, Cambridge, (2004).
- Chris Buckley**, Beijing Levels New Attack at U.S. Cyber-Spying, (New York Times Snosphere Blog (2014).
- Christina Parajon Skinner**, An International Law Response to Economic Cyber Espionage, 46 Connecticut Law Review (2014)
- Christopher S. Yoo**, 'Cyber Espionage or Cyber War?' International Law, Domestic Law, and Self-Protective Measures' Faculty Scholarship Paper 1540 (2015)
- Claire Cain Miller**, Revelations of N.S.A. Spying Cost U.S. Tech Companies, New York Times, (2014).
- Colin Tapper**, Computers and the Law, Wiedenfeld and Nicolson, (1973).
- Craig Mundie**, Speaking on the Future of Technology Conference Columbia University School of International and Public Affairs (2013).
- Craig Forcese**, 'Spies without Borders: International Law and Intelligence Collection' 179 (5) Journal of National Security Law & Policy (2011).
- Daniel Hurst**, 'Australia has violated Timor-Leste's sovereignty, UN court told', Guardian, (2014).
- Daniel Bodansky**, Non-Liquet, Max Planck Encyclopedia of Public International Law (2006).
- Daniel Castro**, How Much Will PRISM Cost the U.S. Cloud Computing Industry?, Information Technology & Innovation Foundation, (August 2013).
- Daniel T. Kuehl**, 'From cyber space to cyberpower: Defining the problem' in Franklin D. Kramer, Stuart H. Starr, Larry K. Wentz, Cyberpower and National Security, National Defense University Press (2009).
- David P. Fidler**, 'Why the WTO is not an Appropriate Venue for Addressing Economic Cyber Espionage' (Arms Control Law, 11 February 2013).
- David Johnson and David Post**, "Law and Borders - The Rise of Law in Cyberspace," 48 Stanford Law Review (1996).

- David P. Fidler**, 'Economic Cyber Espionage and International Law: Controversies Involving Government Acquisition of Trade Secrets through Cyber Technologies' 17 (10) ASIL (2013).
- David Drummond**, 'A new approach to China' (Google Blog, 12 January 2010).
- David Alexander**, 'Theft of F-35 design data is helping U.S. adversaries –Pentagon' (Reuters, 19 Jun 2013).
- David Sutcliffe**, What are the Current Grand Challenges of Internet Research, Oxford Internet Institute Blog, (2016).
- David Fidler**, 'Tinker, Tailor, Soldier, Duqu: Why cyber espionage is more dangerous than you think' International Journal of Critical Infrastructures, (2012).
- Davis Brown**, 'A Proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict', Harvard International Law Journal 47 (2006).
- Dieter Fleck**, 'Individual and State Responsibility for Intelligence Gathering' 28 MJIL (2007).
- Dilma Rousseff**, President Of The Federative Republic Of Brazil, at the opening of the general debate of the 68th session of the United Nations General Assembly (New York, 24 September 2013).
- Donald K. Anton**, 'The Timor Sea Treaty Arbitration: Timor-Leste Challenges Australian Espionage and Seizure of Documents' 18(6) ASIL (2014).
- Donald K. Anton**, 'Arbitrating the Treaty on Certain Maritime Arrangements in the Timor Sea', ANU College of Law Research Paper No. 13-20, (2013).
- Dorothy E. Denning, Peter F. MacDoran**, 'Grounding Cyberspace in the Physical World', within Alan D. Campen, Douglas H. Dearth, R. Thomas Goodden (eds.), Cyberwar: Security, Strategy and Conflict in the Information Age, AFCEA International Press, (1996).
- EU Parliament**, Report on the Existence of A Global System for the Interception of Private and Commercial Communications (ECHELON interception system) (2001/2098(INI)).
- Elizabeth Dwoskin**, New Report: Snowden Revelations Hurt U.S. Companies, Wall Street Journal Digits Blog (2014).
- Elizabeth A. Rowe and Sharon K. Sandeen**, Trade Secrecy and International Transactions Law and Practice, Edward Elgar Publishing, (2015).
- Ellen Messmer**, 'Cyber-espionage attacks threaten corporate data in new unrelenting ways' Network World, (2011).
- Emilio Iasiello**, Are Cyber Weapons Effective Military Tools?, Military and Strategic Affairs, Vol.7/1, (2015).
- Eric Schmidt and Jared Cohen**, The New Digital Age: Reshaping the Future of People, Nations and Business, John Murray, (2013).

- Eric Cole**, *Advanced Persistent Threat: Understanding the Danger and How to Protect Your Organization*, Elsevier, (2013).
- Fred H. Cate**, *Privacy in Information Age*, Brookings Institute Press, (1997).
- Francois Dessemondet**, 'Arbitration and Confidentiality', 7 *American Review of International Arbitration* (1996).
- Geneva Convention** Relative to the Protection of Civilian Persons in Time of War (adopted on 12 August 1949, entered into force 21 October 1950) 75 U.N.T.S 287.
- Geoffrey B. Demarest**, 'Espionage in International Law' 24 *DJILP* (1996).
- Georger Kurtz**, *Global Energy Cyberattacks: "Night Dragon"*, McAfee, (2011).
- Gérard Cohen-Jonathan and Robert Kovar**, *L'espionnage en temps de paix*, *Annuaire français de droit international Année*, Vol. 6/1 (1960).
- Glenn Greenwald, Ewen MacAskill and Laura Poitras**, 'Edward Snowden: the whistleblower behind the NSA surveillance revelations' *Guardian*, (2013).
- Harold Hongju Koh**, Legal Advisor, US Department of State, "International Law in Cyberspace," *The USCYBERCOM Inter-Agency Legal Conference* (2012).
- H. Marshall Jarrett, Michael W. Bailie**, *Prosecuting Computer Crimes*, Office of Legal Education Executive Office for United States Attorneys, (2015).
- Heather Harrison Dinniss**, *Cyber Warfare and the Laws of War*, Cambridge, (2012).
- Henry Kissinger**, *World Order*, Penguin Books, (2014).
- H.M. Kindred**, *International Law, Chiefly as Interpreted and Applied in Canada* 5th Ed. (1993).
- Hugo Grotius**, *The Rights of War and Peace*, Book 3, Knud Haakonssen (ed.) *Liberty Fund* (2005).
- Hugo Grotius**, *On the Law of War and Peace*, A.C. Campbell, *Batoche Books*, (2001).
- Humphrey Waldock**, *Fifth Report on the Law of the Treaties*, *Yearbook of the International Law Commission*, (1965).
- Ivan Arreguín-Toft**, *How the Weak Win Wars, A Theory of Asymmetric Conflict*, *Cambridge Studies in International Relations*, (2005).
- Jack L. Goldsmith**, "Against Cyberanarchy," 65 *University of Chicago Law Review* (1998).
- Jack L. Goldsmith and Eric Posner**, *Limit of International Law*, *Oxford University Press*, (2005).
- James Sperling** (ed) *Handbook of Governance and Security*, *Edward Elgar Publishing*, (2014).
- James Williard Hurst**, *The Growth of American Law: The Law Makers*, *Boston, Little Brown and Company*, (1950).

Jennifer Valentino-Devries and Danny Yadron, Cataloging the World's Cyberforces, Wall Street Journal, (2015).

Jens Ringsmose and Karsten Friis, Conflict in Cyber Space, Routledge, (2016).

Jon R. Lindsay, Tai Ming Cheung, Derek S. Reveron (eds), China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain, Oxford University Press, (2015).

John Kish and David Turns (ed.), International Law and Espionage, Kluwer Law International, (1995).

John Yoo, 'Counterintuitive: Intelligence Operations and International Law' 28 MJIL (2006).

John Perry Barlow, "A Declaration of the Independence of Cyberspace" Electronic Frontier Foundation (1996).

Joshua Philipp, The Staggering Cost of Economic Espionage Against the US, Epoch Times, (2013).

Joshn Chin, 'Cyber Sleuth Track Hacker to China's Military', The Wall Street Journal, (2015).

Joe Lang, The Protection of Commercial Trade Secrets, European Intellectual Property Review, Vol 25/10 (2003).

Jan Klabbers, International Law, Cambridge, (2013).

James Glanz and Andrew W. Lehren, 'N.S.A. Spied on Allies, Aid Groups and Businesses', The New York Times, (2013).

Jens David Ohlin, Kevin Govern, and Claire Finkelstein, Cyber War: Law and Ethics for Virtual Conflicts, Oxford, (2015).

Joe Leahy, 'Brazil's Petrobras to invest heavily in data security', Financial Times, (2013).

Kate Mitchell and Dapo Akande, 'Espionage & Good Faith in Treaty Negotiations: East Timor v Australia' EJIL (2014).

Katharina Ziolkowski, 'Peacetime cyber espionage – new tendencies in public international law', in Katharina Ziolkowski (ed.), Peacetime Regime for State Activities in Cyberspace: International Law, International Relations and Diplomacy CCDCOE, (2013).

Katharine Murphy and Lenore Taylor, 'Timor-Leste spy case: 'witness held, and lawyer's office raided by ASIO', Guardian, (2013).

Katherine L. Herbig and Martin F. Wiskoff, Espionage Against the United States by American Citizens 1947-2001, Defense Personnel Security Research Center, (2002).

Kristen Boon and Douglas Lovelace, Terrorism: Commentary on Security Documents Volume 133. The Drone Wars of the 21st Century: Costs and Benefits, Oxford, (2014).

Kristin Bergtora Sandvik, Towards a Militarization of Cyberspace? Cyberwar as an Issue of International Law, PRIO Papers, (2012).

Lassa Oppenheim, International Law, a Treatise II, LONGMANS, (1912).

Laura Poitras, Marcel Rosenbach and Holger Stark, ‘Codename “Apalachee”: How America Spies on Europe and the UN’, Der Spiegel, (2013).

Lance Strate, ‘The Varieties of Cyberspace: Problems in definition and delimitation’, 63 Western Journal of Communication, (1999).

Luke Pelican, ‘Peacetime Cyberespionage: A Dangerous, but Necessary Game’ 20 CommLaw Conspectus (2012).

Matt Lichtfuss, Cyber-Espionage Making Headlines over Past Couple Weeks, SurfWatchLabs (2016).

Mark D. Young, ‘National Cyber Doctrine: The Missing Link in the Application of American Cyber Power’, Journal of National Security Law & Policy 173, (2010).

Mark E. Villiger, Commentary on the 1969 Vienna Convention on the Law of Treaties, Martinus Nijhoff, (2009).

Malcolm N. Shaw, International Law, Cambridge 6th edition, (2008).

Marco Alexandre Saias, Unlawful Acquisition of Trade Secrets by Cyber Theft: between the Proposed Directive on Trade Secrets and the Directive on Cyber Attacks, JIPLP, Vol.9/9, (2015).

Marco Roscini, Cyber Operations and the Use of Force in International Law, Oxford, (2014).

Marco Roscini, ‘World Wide Warfare - Jus ad bellum and the Use of Cyber Force’ 14 Max Planck Yearbook of United Nations Law (2010).

Marco Roscini, ‘Evidentiary Issues in International Disputes Related to State Responsibility for Cyber Operations’, Texas International Law Journal, Vol.50:2, (2015).

McAfee, ‘Global Energy Cyberattacks: Night Dragon’ (10 February 2011).

McAfee, ‘Net Losses: Estimating the Global Cost of Cybercrime’ (June 2014).

McAfee, Combating Advanced Persistent Threats, White Papers (2011).

Mandiant ‘APT1 Exposing One of China’s Cyber Espionage Units’ (18 February 2013).

Marco Gercke, ‘Understanding cybercrime: phenomena, challenges and legal response’, ITU, (2012).

Michael N. Schmidt (ed.), Tallinn Manual on the International Law Applicable to Cyber Warfare Cambridge, (2013).

Michael N. Schmidt, ‘Cyber Responses “By the Numbers” in International Law’, EJIL, (2015).

- Michael N Schmitt**, “Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework,” 37 Columbia Journal of Transnational Law, (1999).
- Michael Rogers**, ‘Panel Discussion “Rebooting Trust? Freedom vs. Security in Cyberspace’ (Munich Security Conference, 31 February 2014).
- Michael Hickins**, Spying Fears Abroad Hurt U.S. Tech Firms, Wall Street Journal, (2014).
- Micheal Vatis**, ‘The Council of sEurope’s Convention on Cybercrime’, Berkeley Technology Law Journal, 18, (2014).
- Mike Keyser**, ‘The Council of Europe Convention on Cybercrime’, Journal of Transnational Law and Policy, 12, (2003).
- Mark Colvin**, ‘Lawyer representing E. Timor alleges ASIO agents raided his practice’, ABC, (2013).
- Mehmet Emin Bilge**, Ticari Sırların Korunması, Asil, Ankara, (2005).
- Muhammed Sulu**, Ticari Sırların Korunması, On İki Levha Yayıncılık, (2016).
- Murat Volkan Dülger**, Bilişim Suçları ve İnternet İletişim Hukuku, Seçkin (2012).
- Moises Naim**, End of Power: From Boardrooms to Battlefields and Churches to States, Why Being in Charge isn’t what it Used to be, Basic Books, (2013).
- Montevideo Convention**, (signed on 26 December 1933, entered into force on 26 December 1934).
- Myriam Dunn Cavelty**, The Militarisation of Cyberspace: Why Less May Be Better, NATO CCD COE Publications, (2012).
- Myriam Dunn Cavelty**, The Militarisation of Cyber Security as a Source of Global Tension, Strategic Trends Analysis, Center for Security Studies, (2012).
- Nicholas Tsagourias and Russell Buchan** (eds.), Research Handbook on International Law and Cyberspace, Edward Elgar Publishing, (2015).
- Nils Melzer**, Cyberwarfare and International Law, UNIDIR, (2011).
- Norbert Wiener**, Cybernetics or the Control and Communication in the Animal and the Machine, MIT Press, (1948).
- NSA**, In the Matter of Foreign Governments, Foreign Factions, Foreign Entities and Foreign-Based Political Organizations (2010).
- Olufemi Elias**, ‘The Nature of the Subjective Element in Customary International Law’, 44 ICLQ, (1995).
- Oğuz Kaan Pehlivan**, İpin Ucunu Kaçırarak: NSA, Analist Journal, Vol. 34, (2013).
- Oğuz Kaan Pehlivan**, Siber Dünya: Gerçekler ve Reel Tehditler, Analist Journal, Vol. 31, (2013).

- Ottis, R. & Lorents, P.**, ‘Cyberspace: Definition and Implications’, In Proceedings of the 5th International Conference on Information Warfare and Security, Dayton, Academic Publishing Limited, (2010).
- Oscar Schachter**, International Law in Theory and Practice, Martinus Nijhoff Publishers, (1991).
- Oliver Dörr, Kirsten Schmalenbach**, Vienna Convention on the Law of Treaties A Commentary, Springer, (2012).
- Paul Reuter**, Introduction to the Law of Treaties, Routledge (1989).
- Paul Craig, Gráinne de Búrca**, EU Law: Text, Cases and Materials, 6th Edition, Oxford, (2015).
- Peter J. Torren**, Intellectual Property and Computer Crimes, Law Journal Press, (2016).
- Phillip Knightley**, The Second Oldest Profession: Spies and Spying in the Twentieth Century, New York, W.W. Norton & Co., (1986).
- Pierluigi Paganini**, ‘Snowden reveals that China stole plans for a new F-35 aircraft fighter’ (19 January 2015).
- Protocol Additional to the Geneva Conventions** of 12 August 1949, and relating to the Protection of Victims of International Armed Conflict (Protocol I) (Adopted June 8, 1977) 1125 U.N.T.S. 3.
- Quincy Wright**, ‘Espionage and the Doctrine of Non-Intervention in Internal Affairs’ Essays on Espionage and International Law, OHIO State University Press, (2008).
- Richard Clarke**, ‘A Global Cyber-Crisis Waiting to Happen’, Washington Post, (2013).
- Richard Falk**, “Forward” in Roland J. Stanger (ed.), Essays on Espionage and International Law Columbus OH: Ohio State University Press (1962).
- Ron Deibert and Rafal Rohozinski**, ‘Tracking GhostNet: Investigating a Cyber Espionage Network’, University of Toronto, Munk Centre for International Studies at Trinity College, (2009) .
- Rudolf Bernhardt**, Encyclopedia of International Law Vol. 4 North Holland Publishing (1982).
- Russell Buchan**, ‘Cyberattacks: Unlawful uses of force or prohibited interventions?’ 17 Journal of Conflict and Security Law (2012).
- Rufus Yerxa and Bruce Wilson** (eds.), Key Issues in WTO Dispute Settlement, Cambridge University Press, (2005).
- Shannon Hopkins**, ‘Cybercrime Convention: A Positive Beginning to a Long Road Ahead’, Journal of High Technology Law, 2, (2003).
- Sattarova Feruza Y., Prof. Tao-hoon Kim**, ‘IT Security Review: Privacy, Protection, Access Control, Assurance and System Security’ International Journal of Multimedia and Ubiquitous Engineering, 2, 2, (2007).
- Steven Reinhold**, ‘Good Faith in International Law’, Paper No 2/2013 (2013).

- Selçuk Öztekin**, 'Protection of Trade Secrets through IPR and Unfair Competition Law', AIPPIA, (2010).
- Scott J. Shackelford**, *Managing Cyber Attacks in International Law, Business, and Relations In Search of Cyber Peace*, Cambridge, (2014).
- Sam Ball**, *Plans to Stop US Spying with European Internet*, FRANCE 24, (2014).
- Sam Jones**, 'US spies engaged in industrial espionage will be jailed, says lawmaker', Financial (2014).
- Sean Rayment**, 'Britain under attack from 20 foreign spy agencies including France and Germany', The Telegraph, (2009).
- Peter Roudik**, *Foreign Intelligence Gathering Laws*, Law Library of Congress, (2014).
- PCIJ**, *Phosphates in Morocco*, Judgment, Series A/B No. 74 (1938).
- PCIJ**, *The Case of the S.S. Lotus*, Judgement, Series A. No. 10 (1927).
- P. W. Singer and Allan Friedman**, *Cybersecurity and Cyberwar: What Everyone Needs To Know*, Oxford University Press, (2014).
- Rosa Brooks**, *How Everything Became War and the Military Became Everything*, Simon and Schuster, (2016).
- Rochelle C. Dreyfuss and Katherine J. Strandburg** (eds), *The Law and Theory of Trade Secrecy: A Handbook of Contemporary Research*, Edgar Elgar Publishing, (2011).
- Thomas Rid and Peter McBurney**, *Cyber-Weapons*, RUSI Journal, Vol.157:1, (2012).
- Thomas Rid**, *Cyber War Will Not Take Place*, Oxford University Press, (2013).
- Tim Cooper and Ryan LaSalle**, *Guarding and Growing Personal Data Value*, Accentura, (2014).
- The Boston Consulting Group Inc.**, 'The Internet Economy in the G-20', BCG, (2012).
- The White House Cyberspace Policy Review*, (2009).
- Threat Connect and Defense Group Inc.**, 'Project Camerashy: Closing the Aperture on China's Unit 78020', (2015).
- T.V. Paul**, *Asymmetric Conflicts: War Initiation by Weaker Powers*, Cambridge University Press, (1994).
- Turkey's National Cyber Security and 2013-2014 Action Plan*, (2012).
- Uğur Aktekin**, Deniz Doğan Alkan, 'Trade Secret Protection Turkey Chapter' within Trevor Cook (ed), *Trade Secret Protection: A Global Guide*, Globe Law and Business, (2016).
- U.S. Department of Justice**, 'U.S. Charges Five Chinese Military Hackers with Cyber Espionage against U.S. Corporations and a Labor Organization for Commercial Advantage', (2014).

U.S. Department of Defence, Dictionary of Military and Associated Terms, (12 April 2001) (as amended through August 26, 2008).

U.S. Department of Defence Joint Publication 3-12, Cyberspace Operations, (2013).

U.S. Department of Justice, ‘U.S. Charges Five Chinese Military Hackers with Cyber Espionage against U.S. Corporations and a Labor Organization for Commercial Advantage’ (2014).

U.S. Department of Justice, U.S. Charges Five Chinese Military Hackers for Cyber Espionage against U.S. Corporations and a Labor Organization for Commercial Advantage, (2014).

US Department of State, Digest of United States Practice in International Law, Chapter 18, (2014).

U.S.-China Economic and Security Review Commission, Hearing on Commercial Cyber Espionage and Barriers to Digital Trade in China, testimony of Jen Weedon, (2015).

U.S. Chamber of Commerce, The Case for Enhanced Protection of Trade Secrets in the Trans-Pacific Partnership Agreement, (2013).

UK Government, ‘A Strong Britain in an Age of Uncertainty: The National Security Strategy’ (2010).

UK Houses of Parliament, Cyber Security in the UK, (2011).

UK Law Commission, ‘Legislating the Criminal Code: Misuse of Trade Secrets’, Law Commission Consultation Paper 15, (1997).

UNGA, Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism A/HRC/14/46.

Warrington Parker, President Obama Signs into Law the Theft of Trade Secrets Clarification Act, Orrick, (2013).

Wesley L. Gould & Michael Barkun, International Law and the Social Sciences, Princeton, (1970).

W. Hays Parks, ‘The International Law of Intelligence Collection’ National Security Law (1999).

William Gibson, Neuromancer, Ace Publishing, (1984).

William M Stahl, ‘The Uncharted Waters Of Cyberspace: Applying The Principles of International Maritime Law To The Problem Of Cybersecurity’, GJICLR (2011).

William A. Owens, Kenneth W. Dam and Herbert S. Lin (editors), Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities, National Academy of Sciences, (2009).

WTO, A Handbook on the WTO Dispute Settlement System, Cambridge University Press (2004)

Yearbook of International Law Commission, Vol. II (1) Third Report on State Responsibility, A/CN.4/440 (1991).

Yoram Dinstein, War, Aggression and Self Defense, Cambridge University Press 5th ed, (2011)

Yoram Dinstein, ‘The Principle of Distinction and Cyber War in International Armed Conflicts’, 17 (2) Conflict Security Law, (2012).

Yoram Dinstein, ‘Cyber War and International Law: Concluding Remarks at the 2012 Naval War College International Law Conference’, 89 International Law Studies, (2013).

Yoram Dinstein, Computer Network Attacks and Self-Defense, International Law Studies Vol 76, US Naval War College, (2002).

TREATIES & OTHER LEGAL DOCUMENTS

Agreement on Mutual Legal Assistance in Criminal Matters, U.S. - China (2000)

Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) (adopted 15 April 1994).

Australian Minister for Foreign Affairs & Special Minister of State, ‘**Arbitration under the Timor Sea Treaty**’ (3 May, 2013)

Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries, Yearbook of the International Law Commission, Vol. 2 part 2 (2001)

Draft Convention on the Law of Treaties, Harvard Law School (1935)

Canadian Security Intelligence Service Act (Re) (F.C.), 2008 FC 301

CCDCOE, Tallinn Manual on The International Law Applicable to Cyber Warfare (2013)

Council of Europe, Convention on Cybercrime, European Treaty Series - No. 185, (signed 23 November 2001, in effect 1 July 2004)

Economic Espionage Act, 18 USC § 1831 (1996)

European Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems

European Parliament and The Council, Directive 2013/40, “**On Attacks Against Information Systems and Replacing Council Framework Decision 2005/222/JHA**”, Official Journal of European Union L218/8 (2013)

Foreign Intelligence Surveillance Act 50 U.S.C. sec. 1881a

Geneva Convention Relative to the Protection of Civilian Persons in Time of War (adopted on 12 August 1949, entered into force 21 October 1950) 75 U.N.T.S

Hague Convention on respecting the Laws and Customs of War on Land (adopted on 18 October 1907, entered into force 26 January 1910)

HPCR, Manual on International Law Applicable to Air and Missile Warfare, Harvard University, (2009)

International Law Commission, Draft Articles on the Law of Treaties with commentaries, (1966)

ICRC, The Montreux Document on Private Military and Security Companies, (2009)

Marrakesh Agreement, Establishing the World Trade Organization, 15 April 1994.

Montevideo Convention, (signed 26 December 1933, entered into force on 26 December 1934)

Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflict (Protocol I) (Adopted June 8, 1977) 1125 U.N.T.S.

Timor Sea Treaty between the Government of East Timor and the Government of Australia, ATS 13 (adopted 20 May 2002 entered into force Apr. 2, 2003).

Treaty on Open Skies, (entered into force on 1 January 2002).

Treaty between Australia and The Democratic Republic of Timor-Leste on Certain Maritime Arrangements in The Timor Sea (adopted 12 January 2006, entry into force, 23 February 2007) ATS 12.

Turkish Criminal Code, Law with Nr. 5237 (passed on 26.09.2004, Official Gazette No. 25611 dated 12.10.2004).

Turkish Commercial Code, Law with Nr.6102, (accepted on 13.01.2011, Official Gazette No. 27846 dated on 14.02.2011).

Turkish Law on Personal Data Protection, Law with Nr.6698 (accepted on 24.03.2016 Official Gazette No. 29677 dated on 07.04.2016)

Turkish Draft Law on Trade Secrets, Banking Secrets and Client Secrets

United Nations Charter, San Francisco, (signed 26 June 1945, came into force 24 October 1945)

Uniform Law Commission, Uniform Trade Secret Act (1979, amended in 1985)

UKUSA Agreement, (adopted on 10 May 1955).

UKUSA COMINT Agreement and Appendices Thereto, (adopted 26 June 1951).

Vienna Convention on Diplomatic Relations, (adopted 18 April 1961, entered into force 24 April 1964) 500 UNTS 95.

Vienna Convention on the Law of Treaties (adopted on 22 May 1969, entered into force on 27 January 1980) 1155 UNTS 331.

Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies, accepted on 11-12 July 1996.

CURRICULUM VITAE

Oğuz Kaan PEHLIVAN was born in Zara in 1988. He has graduated from Pendik Anatolian High School, before attending İhsan Doğramacı Bilkent University, Department of Law. He pursued his studies as an exchange student in Katholieke Leuven University, Belgium in 2010-2011. After being graduated in 2012 from İhsan Doğramacı Bilkent University, he has worked as a lawyer and legal advisor focusing on international law and security in think-tank environment. In 2014, he has been granted UK Government Chevening Scholarship to pursue his studies in Queen Mary University of London. He is focusing on information technology law, cyber security and applicable international law to cyberspace.

TEZ ONAY SAYFASI

Üniversite : T.C. Galatasaray Üniversitesi
Enstitü : Sosyal Bilimler Enstitüsü
Adı Soyadı : Oğuz Kaan PEHLİVAN
Tez Başlığı : Confronting Economic and Industrial Cyberespionage under International Law
Savunma Tarihi : 22/12/2016
Danışmanı : Prof. Dr. Akif Emre ÖKTEM

JÜRİ ÜYELERİ

Ünvanı, Adı, Soyadı

İmza

Prof. Dr. Akif Emre ÖKTEM

Yrd. Doç. Dr. Mehmet KARLI

Yrd. Doç. Dr. Zeynep PİRİM



Enstitü Müdürü

Prof. Dr. M. Yaman ÖZTEK

