UNIVERSIDAD PONTIFICIA COMILLAS
Faculty of Humanities and Social Sciences

Bachelor´s Degree in International Relations

Final Dissertation

3D-PRINTING, AN ADDITIVE MENACE TO INTERNATIONAL SECURITY?

STUDENT: MARÍA CARMEN MARTÍN PALACIOS

DIRECTOR: ILEANA DANIELA SERBAN

Madrid, April 2018

INDEX

LIST OF ABBREVIATIONS

- **3D:** Three-dimensional space.
- **4D:** Four-dimensional space.
- **AM:** Additive Manufacturing Technologies.
- **CAD:** Computer Aided Design Technologies.
- **DAESH:** Islamic State of Iraq and the Levant, Salafi Jihadist organization.
- **DD:** Defense Distributed.
- **DIY:** Do-it-Yourself.
- **EU:** European Union.
- **FDM:** Fused Deposition Modelling.
- **IoT:** Internet of Things**.**
- **ISS:** International Security Studies.
- **ITAR:** International Traffic in Arms Regulation.
- **GPS:** Global Positioning System**.**
- **LED:** Light Emiting Diodes.
- **LENS:** Laser Engineering Net Shaping**.**
- **OSCE:** Organisation for Security and Cooperation in Europe.
- **REF:** Rapid Equipping Force.
- **SMALS:** Small Arms and Light Weapons.
- **UAV:** Unmanned Aerial Vehicles.
- **UFA:** Undetectable Firearms Act.
- **UK:** United Kingdom.
- **UN:** United Nations**.**
- **UNODA:** United Nations Office of Disarmament Affairs.
- **US:** United States of America.
- **WoT**: War on Terror.
- **WMD:** Weapons of Mass Destruction.
- **WWW:** World Wide Web.
- **XXI:** Twenty-First Century.

María Carmen Martín Palacios

201303867 5º E6

ABSTRACT

The objective of this dissertation is to analyse the role of new technologies, and more specifically 3D printing, as disruptive elements to International Security, linked to the phenomenon of modern terrorism and the non-proliferation of weapons. In addition, this paper has explored the possible applications of this technology to support existing security systems, encouraging policy-makers and specialised scholars to reflect on whether current defence mechanisms are prepared to combat modern menaces such as 3D printed weapons. Therefore, this thesis has been structured in three major parts: an overview of the functioning and accessibility of 3D printers to contextualise its weaponry use, a study on the challenges that additive manufacturing poses for International Security; and a final analysis on how International Administrations are both combating 3D criminality and using this procedure for defence reinforcement.

KEY WORDS:

Additive manufacturing technologies, 3D printing, International Security, Terrorism, Criminality, FDM, LENS.

RESUMEN:

Este Trabajo de Fin de Grado tiene por objetivo estudiar el rol de las nuevas tecnologías en el ámbito de la Seguridad Internacional, centrándose en el análisis de la impresión 3D como herramienta de apoyo a organizaciones criminales y terroristas. Por otro lado, este trabajo también examinará sus posibles usos para reforzar las medidas de protección y defensa existentes, así como su aplicación en otros campos relacionados con la seguridad y el bienestar ciudadano. Para ello, este proyecto queda dividido en tres partes fundamentales: una aproximación al funcionamiento de la tecnología 3D contextualizado en las técnicas de impresión de armas, un estudio de los desafíos criminalísticos y terroristas derivados del uso de esta tecnología y un análisis de la impresión 3D como elemento de refuerzo de las medidas de seguridad internacionales.

PALABRAS CLAVE:

Tecnologías de fabricación aditiva, impresión 3D, Seguridad Internacional, Terrorismo, Criminalidad, FDM, LENS

1. INTRODUCTION

The first decades of the XXI Century have witnessed the hatching of the Fourth Industrial Revolution, a technological phenomenon that is fostering the development of ground-breaking advancements. These inventions are called to alter traditional manufacturing processes, transform citizen´s routines and promote the inclusion of new technological themes into the international political agenda. Among these innovations, additive manufacturing technologies, also known as 3D printing, stand as one of the crafting procedures with greater potential of disruption, as it intends to revolution not only the industrial sector but also household activities, aiming to make citizen´s lives easier.

3D printing enables the manufacturing of digitally designed goods, whose pieces are joint in a computer-supervised assembling process. This monitorization permits ad-hoc customization of the resulting three-dimensional object, endowing this technology with a flexibility factor that other production means lack. This distinction, along with the increasing materials that are becoming eligible to be used in the printing procedure, has fostered the rapid inclusion of this manufacturing process into the industrial chain of different sectors, including heavy engineering or the health-care industry (Yvon, 2016). The intersectoral application of 3D printing, and the prospective introduction of this production process into cutting-edge domains such as astronautics[1] or photovoltaics[2] have positioned additive manufacturing procedures among the most impactful technologies of this century[3].

Nonetheless, this 3D printing revolution has also given rise to new security challenges, which are resulting from the crime-oriented use of these technologies. Additive Manufacturing is boosting illegal industries such as the counterfeiting sector, which is profiting from the high quality of the printed goods to produce more sophisticated copies at a cheaper cost; as this technology permits the elimination of substantial expenses including those that derive from transportation and stock logistics.

Even though the illegal application of additive manufacturing procedures in the counterfeiting sector would be worth an independent analysis, this dissertation has focused in examining one of the most severe challenges that derive from the misutilization of 3D technologies: the fabrication of small and light weapons (SALW). This manufacturing technique has helped illegal gunsmiths to substitute more rudimentary fabrication means and boost production by replicating any given computer-aided designed weapon on a rolling-basis.

[1] NASA aeronautics is working in the construction of a 3D printer that enables astronauts to print their food in the International Space Station. (Pallottino, 2016)
[2] The Australian Government has financed the construction of solar panels which have been entirely built with additive manufacturing technologies. (Valk, 2015)
[3] 3D technologies have been ranked as some of the most impactful inventions of the XXI Century by prestigious reports such as the KPMG´s Disruptive Technologies Barometer or McKinney's Disruptive Technologies Report. (Manyika, J., 2013); (Yvon, 2016)

Although international authorities have struggled against home-made arms during decades, 3D guns present several challenges to non-proliferation policies, as their plastic nature hampers their detection by traditional security mechanisms. Furthermore, the online distribution of their blueprints accounts for an additional defiance, as deterring their online circulation and ensuring that they are not re-uploaded into illegal sites requires a notable coordination effort along with the drawing of stricter law codes.

These insecurity vacuums have driven the attention of Terrorist organisations, which have witnessed in 3D printing a valuable ally to supply pledged supporters with the required material to commit massacres. Moreover, the rising performance of lone wolf attackers and the prospective development of AM[4] techniques that could enable the printing of critical arms such as biological weapons; have set 3D terrorism into the spotlight of counter-terrorist policies.

Therefore, this dissertation aims to raise awareness on the consequences that the misutilization of AM may have on International Security, focusing in the criminal and terrorist application of 3D printing; whilst examining the preventive tools required to address these challenges, including the utilization of this technology to reinforce existing protection measures. Hence, this combined approach will provide a complete overview on the challenges and opportunities that Additive Manufacturing technologies present to International Security.

2. RESEARCH FOCUS AND SCOPE

2.1. RESEARCH AIM

As one of the core branches of International Relations, the main objective of Security Studies is to provide factual and updated information aimed at not only specialised scholars, but also policy-makers and strategists whom wish to partake in the volatile dynamics of the International Arena. Therefore, this work seeks to contribute to conceptual development within International Security by analysing both the potential threats that may arise from the misuse of 3D printing and the opportunities that this technology offers to the sector of Defence.

Given the rising interconnectivity of the global society, this dissertation is not centred at a national level, but it considers the present and prospective implications of additive manufacturing technologies from an international perspective. This transnational approach seeks to encompass the multiple security

[4] AM is the general abbreviation of Additive Manufacturing technologies.

implications of additive manufacturing as well as to explore the existing and potential synergies between the Industry of Defence and the 3D printing sector.

Therefore, this thesis will present a multipolar vision on additive manufacturing, identifying the positive and negative outcomes that can derive from the spread of this technological advancement. This double-edged perspective is due to the consequences that any innovation usually brings to the international arena: a combination of progress and disruption (Malerba, 2007).

Consequently, the core of the analysis thesis will be divided in a double perspective: a review of the threats that 3D printing presents to International Security (embedded in the debate of modern terrorist techniques) and a study of the positive use of this technology to reinforce International Security Systems.

2.2. TERMINOLOGICAL CLARIFICATIONS

Prior to describing the objectives of this thesis, it is necessary to clarify the use and definitions of certain terms that will be recurrently mentioned in the successive chapters of this dissertation.

A. DISTINCTION BETWEEN CRIMINAL AND TERRORIST

In this thesis, there has been made a distinction between criminals and terrorists, following the reasoning of some specialised scholars such as Dr. David Goldstein from Boston University. (Goldstein, 1979)

According to Dr. Goldstein, the main difference between a criminal and a terrorist lies in the purpose behind the commitment of the attack or illicit action. While an ordinary criminal seeks to obtain a profit for himself, the ultimate goal of the terrorist is the success of the organisation to which he has pledged support.

Moreover, given that terrorists are backed up by organised groups, they are often better trained and equipped than ordinary criminals. Therefore, the level of impact of terrorist actions is usually greater than those of a common criminal. (Goldstein, 2007)

Another significant difference between both terms lies in the publicity of the perpetrated action. Whilst ordinary criminals do not want to be acknowledged as the authors of a crime, terrorists do not only seek to vindicate their authority, but they also use the attack scenario as a marketing platform to spread the message of their supporting organization.

Considering these disparities, it has been deemed appropriate not to include terrorism as a type of criminal action, but as an independent phenomenon.

B. ETYMOLOGY AND SCOPE OF TERRORISM

In this dissertation, the notion of terrorism has a fundamental role in the analysis of the potential harmful use of 3D printing technologies. Therefore, it is necessary to delimit this concept and clarify the way in which it will be deployed in the current research. This descriptive procedure has been significantly complex given the ongoing academic discussion on the characteristics of this term, which will be explained in the following lines.

Understanding the concept of terrorism and the multiple dimensions that it comprises, has challenged scholars in the field since the creation of the term. Even though it was officially coined by the Jacobins to describe the attitude of revolutionaries during the French Revolution, some specialists argue that the etymologic origins of the word trace back to the Roman Empire (Conte, 2010).

The idiom "terror cimbricus" was used by roman centurions to describe the feeling of thrill and dread that spread among their troops before attacking a Barbarian tribe (Matusitz, 2013). This expression resulted from the combination of the Latin word "terror", which meant "to tremble", and the Cimbri people, which were fierce warriors of the second century before Christ. Therefore, even in the primitive root of the term, there was implicit that sense of fear that is the main feature of modern terrorist attacks.

According to the estimations of the senior expert on terrorism, Jeffrey Simon, there have been registered over 200 different definitions of the term across the world, including academic and governmental descriptions (Simon, 2007). This etymological proliferation has been due to two major reasons. If we consider the academic sector, this diversification has resulted from the momentum of studies centred on terrorism, which have gained importance since the beginning of the "War on Terror"[5]

Given that these definitions are oriented to the main field of study of their authors, their content is heterogenic, and some elements of terrorism may remain "outside the picture" (Schmid, 2010). Moreover, some critics believe that the strict academic nature of these definitions sometimes hampers the understanding of the term, "defying its common usage" (Badey, 1998).

The other reason that justifies the proliferation of definitions on terrorism is the governmental trend to customise them according to each country´s law codes. However, these definitions sometimes fail to be totally objective, as they may be influenced by the repercussion of terrorist attacks on that state´s society and the ideology of the sitting government (Simon, 2001). Nonetheless, the common feature of these

[5] The "War on Terror", which was declared during the American Presidency of George W. Bush, consists in an international belligerent campaign against the Islamic terrorist organisations that carry attacks on behalf of the creation of a new "Global Caliphate" (Clarke, 2008).

institutional definitions is the ambiguous delimitation of terrorist actions and the pejorative connotation of the terrorist term (Badey, 1998).

Therefore, most of the existing definitions of terrorism fall into these political or academic categories. However, according to a statistic study of the University of Leiden, these two domains have resemblances in the components that they include as core elements of terrorism. This study concluded that the three main elements present in these definitions are the use of violence, the existence of political, ideological or religious objectives and the aim of propagating fear in a targeted population (Schmid, 1988).

Despite the several initiatives of the United Nations to develop a universal and legally binding definition, the international community has failed to agree on its formulation due to political and emotional impediments.

Moreover, some States have argued that no agreement will be reached until there is consensus on delimiting the use of violence in the context of national conflicts and self-determination actions (Martyn, 2002). In addition to these obstacles, the broad nature of terrorist activities and the ideological differences between UN members is further impeding the consecution of a conjoint agreement (Obado Ochieng, 2017).

Given this lack of official framework, this thesis has followed what, to date, represents the closest universal approximation to a common definition of terrorism. Even though the United Nations has failed to formally agree on a definition, in 1994 the General Assembly passed a resolution on “Measures to eliminate International Terrorism” which included an annexed provision describing the term. In the mentioned document, terrorism is defined as:

"Criminal acts intended or calculated to provoke a state of terror in the general public, a group of persons or particular persons for political purposes are in any circumstance unjustifiable, whatever the considerations of a political, philosophical, ideological, racial, ethnic, religious or any other nature that may be invoked to justify them.”

United Nations Declaration on Measures to Eliminate International Terrorism, 1994

(Annex to UN General Assembly Resolution 49/60)

Since the Resolution 49/60 has been recurrently used by subsequent UN Resolutions[6] and recalled in the UN Counter Terrorism Committee working papers, this research has based its approach on terrorism on the provisions of this Resolution.

[6] This description is present in the Resolution 1566 of the Security Council, which tackled the Threats to international peace and security caused by terrorist acts. In addition, this pseudo-definition is also included in the Resolution 1373 of this same body, which was produced following the 11-S attacks and which gave birth to the UN Counter Terrorism Committee.

C. MODERN TERRORISM AND LEVEL OF ANALYSIS

The first decades of the XXI century have witnessed the rise of a new type of terrorism, embedded in the global jihadist movement. This modern phenomenon results from the ongoing "Fourth Wave of Global Terrorism", which started in 1979 and whose philosophical aim is to rearrange the International Order according to extreme religious principles (Rapoport, 2002). Even though most of the organisations that have been created during these Religious Waves have manifested their support to the Islamic creed, other religions and sects have also produced their own terrorist groups. Therefore, religious fundamentalism is one of the core elements of this new terrorism.

In addition to this religious component, another characteristic of modern terrorism is the prominent use of new technologies to perpetrate attacks. The rise of Internet and the spread of connected devices has enabled the dispersion of terrorists, which are needless to gather in concentrated cells to be informed of the targets of their supporting organisation. Moreover, this digitalised network of terrorists has given more autonomy to the attackers, which sometimes decide to act without the supervision of any terrorist organisation (White, 2013).

Despite their autonomous operating methods, these "lone wolves" are usually influenced by the ideology of a terrorist group and tend to show their support to that command when they commit the attack. This has been the modus operandi of some of the last European terrorist massacres, including the recent bloodsheds of Las Vegas, Manchester or London. (Byman, 2017)

While some scholars argue that there are still important terrorist cells in regions like Europe, such as the now dismantled cell that carried the Barcelona attack in 2017, it is evident that the lone wolf phenomenon is a menace that poses enormous difficulties to the preventive effort of intelligence services. Therefore, this research work has decided to focus its scope on the lone wolf menace and the rise of digital-based terrorism to analyse the potential use of 3D printers to provide terrorists with lethal home-produced armament.

Lastly, regarding the level of analysis from which this study has addressed terrorism, the approach that was deemed more appropriate was the micro level, which is the dimension that studies the tactical elements of terrorist attacks, aiming to identify the means and procedures of their aggressions to prevent future attacks and contribute to the development of counter-terrorist methods. (Jackson, 2009) Consequently, the study of 3D Printing applications to terrorism has been framed in this micro-level of analysis.

2.3. JUSTIFICATION OF THE STUDY AND OBJECTIVES

In the last 30 years, the rapid evolution of new technologies has shaped the societal structure, defying the limits that decades ago were only trespassed by science fiction entertainment. New generations have been born into a digital world, in which the existence of Internet and the interconnection of objects are taken for granted. This technological blossoming makes necessary the study of these new advances, in order to understand both its positive applications and the threats that its misuse poses to the International society.

Therefore, this thesis seeks to provide a double perspective regarding the potential utilization of additive manufacturing technologies, being its two major objectives:

1) **Analyse 3D printing as a potential threat to International Security, considering its potential use as a criminal and terrorist mean**:

This dissertation will study the threats that 3D printing presents to International Security, framed in the current momentum of weapon proliferation and the rising phenomenon of modern terrorism. Even though there are multiple criminal areas which could profit from additive manufacturing, this work will only deepen on the challenge of illegal 3D weapons production, focusing on the potential use of these armaments to conduct attacks against civilians.

To ensure the proper understanding of the scope of this menace, this dissertation will firstly introduce the functioning of 3D printers. Secondly, the analysis of the case study of "Defense Distributed" will argue the existence of individuals and firms that are challenging international security by using these devices, evidencing the difficulties that governments are having in combating illegal 3D-weapon entrepreneurs.

Apart from this criminal analysis, this thesis will also examine how terrorists are profiting from this technology to carry their attacks, paying especial attention to the new lone wolves ´phenomenon. Lastly, this part of the analysis will conclude with the study of the security challenges that are arising with regards to the illegal manufacturing of 3D weapons, focused in the detection of these firearms and the online distribution of the printing blueprints.

Therefore, and considering these previous elements, the threat of additive manufacturing will be addressed from three complementary perspectives, which will include:

1.1. An analysis on the difficulties that exist to detect and monitor 3D printed weapons.

1.2. A study on the preventive actions that can be conducted to avoid the terrorist and criminal use of 3D armament.

1.3. A proposal on how to stop the online distribution of the weapons´ printing guidelines.

These three dimensions will present a combined approach to the technological threat that additive manufacturing poses while providing governments with suggestions on how to address this new security challenge.

2) Consider the possible applications of 3D technologies to reinforce International Security:

Global citizens receive private and public protection from both the Industry of Defence and the governmental security network of their countries. Therefore, this section will provide an overview of the organisations and states that have already incorporated 3D printing technologies to improve the level of security of their facilities. In addition, this thesis will analyse the positive impact that additive manufacturing is having on the modernisation of these defence systems and will explore potential applications to further reinforce human security.

3. STATE OF THE ART

Even though additive manufacturing technologies originated in the 1990´s it was not until the mid- 2000´s when 3D printing became a buzzword, being the first non-industrial printer sold in the year 2006. (Flynt, 2018) Until then, 3D printing seemed to be secluded to scientific industries, and the idea of home-printing objects had been too futuristic. Therefore, most of the academic studies that tackled this emergent technology between 1990 and 2006 were centred around the impact of 3D technologies on sectors such as the heavy metals ´industry. (Ross, 2015)

However, the media effort to sell 3D printing as the latest technological innovation and the global debate over the opportunities that additive manufacturing presented to multidisciplinary domains gave momentum to the investigation of 3D printing from broader academic perspectives. Nonetheless, regarding the approach of international security, the production of studies on this topic has not been as prolific, possibly due to the relatively new emergence of 3D printed weapons and the progressive introduction of additive manufacturing technologies in the industry of Defence (Campbell, 2017). Therefore, this thesis seeks to contribute to this area of investigation, aiming not only to support prospective research papers, but also to undertake a rigorous analysis of the Security role of 3D technologies.

Among the reviewed literature, there have been two research papers that have nourished the production of the present thesis. On one hand, the Peace Research Institute of Frankfurt dissertation on “The Risks and Challenges of 3D Printing” by the scholar Marco Fey has supported the investigation over the threats that additive manufacturing currently presents to the International Community.

On the other hand, and considering the positive applications of this technology to the Industry of Defence, the study "The 3D printing Revolution", published by the Harvard Business Review researcher Richard D´Aveni has highly contributed to identify these applications.

3.1. METHODOLOGY AND STRUCTURE

Regarding the methodology utilized for the configuration of this thesis, it has followed a deductive research process. This procedure has consisted in three main phases: an extensive examination of the existing sources of information, the curation of the most complete research paper and the synthesis of their content aimed at supporting the production of the final document.

Moreover, this study has been backed up with mainly qualitative information obtained from multidisciplinary data bases such as EBSCOHOST and International Relations Academic Entities. Among these consulted research institutions, the work of think tanks such as the American Centre for Strategic and the International Studies or the Stockholm International Peace Research Institute have been largely used in the production of this thesis.

This dissertation has been divided into nine chapters, including these former introductory and methodological clarifications. Regarding the analytical content, the third and fourth chapters explain the evolution of this manufacturing technique as well as its most utilised procedures, to ensure the better comprehension of the subsequent parts of the analytical body. Then, the fifth, sixth and seventh chapters present the link between additive manufacturing technologies and international security, focusing in the criminal and terrorist use of this technique, and more specifically in its utilisation to fabricate 3D printed weapons. This analysis on the threats that derive from the misutilisation of this technology contrast to the content of the eight chapter, which introduces the positive use of AM to reinforce international security, whilst fostering reflection on the future prevention policies to be applied in order to better address this problem. These insights are coined in the conclusion chapter, that serves as a final reflection on the outcomes of this dissertation.

4. RECENT HISTORY OF 3D TECHNOLOGIES

When the French economist Auguste Blanqui coined in 1837 the term "Industrial Revolution" to define the "transition from industries carried in homes, to industries in factories with power-driven machinery" (Aggarwal, 2016), he could have never imagined that only two centuries afterwards home manufacturing would again be in vogue; being 3D printing the crowning jewel of the "Do it yourself" industrial revolution.

Since the 1980´s, two-dimensional production has been overthrown by the rapid development of 3D printing techniques, whose sophistication is contributing to drive change in manufacturing companies by streamlining their industrial processes and cutting costs of their lines of production. 3D printing has progressively been introduced in production chains, and today it is becoming a usual procedure in the automotive, healthcare or aerospace industry (Stratasys, 2017). Moreover, it is expected that this technology will not only alter the traditional functioning of industries, but it will also involve the adaptation of the whole society to a technique that is called to become part of our personal and professional routines.

In the last 10 years, 3D manufacturing has shifted from being an exclusive element of the engineering industry to a promising technique for daily-life aspects. This new approach has resulted from the large public and private investment in research and development, which have boosted progress of additive manufacturing by broadening its prospective applications.

Furthermore, the intensive investigating effort has not only resulted in the development of alternative 3D printing methods but has also given birth to an additional dimension of additive manufacturing technology: 4D printing. This technique provides a smart feature to the printed elements, as the materials used in the 4D process are self-assembling, which implies that once the object is printed, they can alter its shape by reacting to determined environmental parameters such as heat or humidity (Tibbits, S. 2014).

Given that 4D printing is only recently developing as a method, this dissertation will be centred on 3D printing, to better address its present and prospective implications from the new security perspective. Thus, in the next pages 3D printing techniques will be encompassed under the general labelling of Additive Manufacturing (AM).

4.1. GENERAL ADDITIVE MANUFACTURING TECHNIQUES

Prior to analysing the potential of Additive Manufacturing as a disruptive element to international security, it is essential to examine the basic mechanisms and functioning of this technology, which is rapidly penetrating multiple domains of our societies.

There are different 3D printing techniques, which differ from each other in two main aspects: the process applied to layer the components of the final object and the raw materials used during the printing phase. However, the functional part of the process is the same for the alternative existing methods, which eases the methodology of additive manufacturing.

The printing process is divided into four major stages. Every process starts with the development of a 3D model, which is created in a computer equipped with Computer Aided Design technology (CAD) that

enables the configuration of the prospective printed object. This design can be drawn by using two alternative mechanisms: a 3D scanner or 3D modelling software. The first method profits from the advancements of reverse engineering technology, which has resulted in the plummeting of the prices of "Do It Yourself" scanners, whose simplest models are sold online for less than 40 dollars (Ravis, 2015). On the other hand, 3D modelling software offers a wider compilation of design guidelines, depending on the industry in which the object is aimed at. However, aside professional grade software, there is also a free open source software available for the design of other non-industrial prototypes. Among the existing programs, the "Tinkercad" platform and the "Blender 2.79" open-source creation suite have become some of the most used resources (Redwood, 2017).

Once the model is crafted, the next phase consists in dividing the model into different horizontal layers, which ease the printing procedure. This division is either done by the same previously used 3D software or through a special "Slicing machine". The sliced file is then inserted inside the 3D printer by using either a physical USB drive or via Wi-Fi. Once this "Feeding Process" is completed, the printer is ready to build the designed model.

There are seven main additive manufacturing technologies, depending on the selected printed material (plastic, resin, wax, composite or metal) and the technique used to join the different layers (material extrusion, direct energy deposition, etc.). However, when considering 3D weaponry printing, the two processes to take into consideration are Fused Deposition Modelling (FDM) and Laser Engineering Net Shaping (LENS).

Fused Deposition Modelling is the most widely used additive manufacturing technology, given the low cost of the materials used to create the final models and the high impact of the printed objects. This technique, which belongs to the material extrusion family, consists in depositing melted material layer by layer to build the resulting items. FDM processes are very permissive with the type of materials used in the printing phase, ranging from commodity thermoplastics to engineering materials or composites. Therefore, it is not surprising that FDM is the preferred method for "Do-It-Yourself" 3D printing processes (Hall, 2017).

On the other hand, Laser Engineering Net Shaping (LENS) accounts for a more complex technique, derived from direct energy deposition technologies. This process consists in fusing metal powder through a potent laser beam, which will merge the different layers into a solid final component. The main advantage of this method is the wide range of alloys allowed in the printing stage, which permit rapid prototyping and manufacturing of metal objects. Therefore, LENS technology is much appreciated in heavy industries, as it accelerates the production of complex structures (Waterman, 2017).

Until 2016, it seemed that metal 3D printing was exclusive to wealthy companies of the secondary sector, given the high cost of LENS-compatible 3D printers and the specialised know-how required to manage the productive process. However, in 2016 the company "The Virtual Foundry" announced the launch of a new metal filament that could turn any FDM 3D printer into a 3D metal printer under the highly competitive price of 100$ (Hall, 2016). Consequently, this printing technology is becoming accessible to a larger public, which can now afford to have one of these multifunctional printers at home. However, as the demand grows the fewer the prerequisites for the tenancy of this devices and the more evident becomes the question:

Are we overseeing the target of the buyer of these devices or are we opening the door to the misuse of 3D printers?

5. INTERNATIONAL SECURITY AND 3D PRINTING

Throughout history, technological improvements have not only served to enhance progress. Unfortunately, there have always been actors that have profited from these advancements to cause damage and global disruption. Consequently, in the last decades the world has witnessed the birth of new security dilemmas, caused by several factors which range from chemical conflicts to drone wars.

In the last 20 years, the rapid development of 3D manufacturing has turned this phenomenon into one of the most revolutionary technologies of the century. The multiple applications and associated features of 3D printing has sky rocketed the private investment in R&D, and experts foresee an exponential penetration of this technology in different industries in the upcoming years. However, specialised scholars and defence institutions have manifested their high concern regarding the security risks that this promising technology entails. (Geissbauer, Lehr, & Wunderlin, 2017)

Since the inclusion of coal and metal as printing-eligible materials, the range of products that can be printed has almost become limitless. Among this broad scope of production, there has been reported a significant growth in weaponry printing, as this technology enables a speeder and cheaper production. Moreover, and as 3D printers work based on blueprints, any type of weapon could theoretically be produced by using these devices: from small arms and light weapons (SMALS) like handguns, grenades or missiles to other non-conventional weapons such as drones. Even though today there are not any records of 3D-printed chemical nor nuclear printed weapons, the evolution of this technology makes experts fear that in the future weapons of mass destruction could be produced via 3D printing (Fey, 2017).

What is certain is that even though additive manufacturing offers many opportunities for many productive sectors, it also poses a serious menace for International Security. However, as mentioned in the methodological chapter, this study seeks to look beyond the uncertainties that this technology presents to this area and explore potential opportunities as well.

5.1. THE ORIGINS OF ADDITIVE MANUFACTURING CRIMINALITY: COUNTERFEITING

The first Additive Manufacturing criminal traces were found in the counterfeiting sector in the 1990´s. Back then, 3D printing techniques were not only more rudimentary than current procedures, but its management also required a technical knowledge which was scarcer than today. Consequently, AM was initially only used for the production luxury counterfeits, being Stereolithography (light laser printing) the preferred printing procedure (Desai, 2013).

However, the rapid evolution of additive manufacturing has turned 3D printing into a recurrent counterfeiting practice. The improved quality of the copies produced with AM has ousted primitive methods of plagiarism that produced less competitive copies. The development of Internet and the ease of access to 3D printers has given counterfeiters the key to produce more sophisticated goods, based in the blueprints available in pirate sites (Shams, 2017).

In addition, the attractiveness of Additive Manufacturing can also be understood from a cost efficiency perspective. The mobility and relatively easy setup of 3D printers enables counterfeiters to locate the manufacturing centres closer to the final consumer, avoiding shipping and border-crossing costs of traditional practices. Therefore, AM is opening the door to the creation of economies of scale, which will ultimately hinder the fight against this illegal practice.

The lack of legislative precision with regards to 3D printing techniques presents an additional problem to multiple manufacturing sectors, which fear that the existing legal vacuum could result in irreversible loses for their industries; derived from the violation of the rights of the holders of patents and trademarks (Depoorter, 2014). This concern has been endorsed by specialised consultancy firms such as The Gartner Group, which esteemed that by 2018, the global losses in intellectual property derived from 3D printing will amount to $100 billion (Hornick, 2014).

Despite the effort in including specific regulation for 3D printing in law codes, jurists are experiencing difficulties in specifying which goods can and cannot be reproduced using additive manufacturing technology, as there is no current impediment to copy functional objects. However, defenders of AM believe that restricting the use of these techniques would not stop counterfeiters from conducting their

illegal activities but will only restrain the modernisation of the industry by hampering the creation of economies of scale and synergies in the manufacturing chain.

5.2. 3D PRINTING AND ARM MANUFACTURING

The unstoppable evolution of additive manufacturing technology has made possible the printing of a wide variety of items, including weapons, explosives and ammunition. This applicability is regarded as a significant threat to international security, given that it enhances the unsupervised production and circulation of arms.

Therefore, International Organisations and public institutions are increasing their effort to raise awareness on the consequences of the misuse of these devices. For this regard, numerous global forums like the European Expo on Counterterrorism are including 3D printing as a central issue of debate. This symposium hosted a public conference that linked terrorism and insecurity with additive manufacturing, in which the Metropolitan Police warned about the menace of AM technologies. More specifically, the senior officer Mark Rowley manifested that intelligence bodies are already wrestling 3D terrorism, as the use of this machinery to create weapons is “no longer a hypothesis” (Whitehead, T. 2015).

Likewise, the Organization for Security and Cooperation in Europe (OSCE) included in the final report of 2014 Conference on “Illicit Trafficking in Small Arms and Light Weapons and Fight against Terrorism in the Mediterranean Region”, a specific section that warned about the applicability of 3D printers to the production of light and small arms (SALW). In this document, additive manufacturing was not only listed as an aggravating factor for the illicit trade and production of SALW, but it was also identified as an element that can heighten terrorist attacks by improving their access to the needed weaponry to perpetrate them (OSCE, 2014).

However, additive manufacturing has not only been object of discussion in International forums but has also been exposed by referent public figures in speeches targeted at the general society. For instance, the former Secretary General of the United Nations Ban Ki Moon listed 3D printing as one of the most dangerous global threats in his last speech in the Security Council, voicing his concern of its potential for mass destruction (Mendoza, R. 2016).

5.3. 3D PRINTING AND WEAPONS OF MASS DESTRUCTION

This linkage between additive manufacturing and weapons of mass destruction is one of the major concerns of security analysts. Considering the rapid advancement of AM technologies, many experts fear of the possible use of 3D printers to build nuclear or biological weapons; as these devices are progressively been adapted to further types of printable materials. Among the produced research papers studying this

menace, the Swedish think tank SIPRI has conducted a profound analysis[7] on the feasibility of this security threat. This publication sustains that to enhance the printability of weapons of mass destruction, very concrete materials would be required, and to date their viability presents significant limitations. Their flammability and pressure-sensitiveness prevent materials such as plutonium to be malleable and apt to be included in the printing process (Kelley, 2017).

Nonetheless, the SIPRI research paper also states that the impossibility of printing a full WMD at once does not impede additive manufacture devices to print individual aluminium or beryllium alloyed components that could jointly be used in a bomb core or to repair a damaged weapon (Kelley, 2017). Therefore, regardless of the current obstacles, it is certain that additive manufacturing poses an additional challenge to the non-proliferation of nuclear weapons, especially considering potential advancements.

Likewise, the United Nations Office of Disarmament Affairs (UNODA) has strongly advised global governments to keep up with current, new and emerging trends related to additive manufacturing, so that they become prepared to efficiently address future challenges to non-proliferation. For this regard, one of the major topics discussed in the 2017 Preparatory Committee for the 2020 Nuclear Non-Proliferation Treaty Review Conference has been the possible implications of additive manufacturing technology for the long-term goals of the Committee (UNODA, 2017).

Even though the connection between weapons of mass destruction and 3D printers is one of the most concerning risks of AM to International Security, the significant material obstacles for the printing process has relegated this menace to a second place in the short term. To date, the most dangerous applicability of this technology is regarding the proliferation of firearms and ammunition, aimed at self-consumption, terrorism or arm trafficking (Hidalgo García, 2017).

5.4. ADDITIVE MANUFACTURING AND GUNSMITHS: STUDY CASE OF DEFENSE DISTRIBUTED

The illicit trade of weapons is one of the most complex security issues that international governments and partner organisations have been struggling against in the last decades. However, since the digitalisation of this illegal market, combating arm traffickers has become more difficult, as additional challenges have emerged from the development of new technologies, including additive manufacturing techniques.

The Dark web has become the usual scenario for both the trading of finished printed weapons as well as the blueprints needed to replicate them. These blueprints are detailed tutorials which explain the printing

[7] The research paper "Is three-dimensional (3d) printing a nuclear proliferation tool?" was published by SIPRI on February 2017 in coordination with the EU Non-Proliferation Consortium, being the leading researcher Robert Kelley, former Director of the International Atomic Energy Agency.

process aimed at either converting a gun replica into real weapon or at manufacturing a new arm or explosive from the beginning (Persi Paoli, Aldridge, Ryan, & Warnes, 2017).

The first entirely printed firearm was produced in the United States in 2013, as a result of a crowdfunding initiative called Wiki-Weapon project. The aim of this project, run by the online organisation Defense Distributed, was not only to prove that printing arms was possible, but to ensure that anyone could have access to weapons. The name of the project was inspired by the Wiki-Leak's organisation, given that Defense Distributed´s founder finds a level of resemblance between the missions of both entities, which is to bring to the public a certain need (information or the access to weapons) (Prestigiacomo, 2017).

Therefore, guaranteeing the right to keep and bear weapons is understood by Defense Distributed as its principal objective, and it is described in its official website in the following terms:

"We seek to defend the civil rights to bear arms as guaranteed by the United States Constitution by collaboratively producing, publishing and distributing public information and knowledge related to digital arm manufacturing" (Defense Distributed, 2017).

The Wiki Weapon project resulted in the creation of the Liberator pistol, thanks to the initial support of the 3D printing company Stratasys, which initially provided the company with the pieces needed to produce the gun. The crucial accomplishment of the 3D printing procedure was to print the lower receiver of the firearm, which is the component that includes the trigger and the magazine port (the operative parts of the arm), and thus considered as the real "firearm" within the American laws (Mattise, 2017).

However, Stratasys retrieved its sponsorship as soon as Cody Wilson-the director of Defense Distributed-manifested his aim to design and release the blueprints for a plastic weapon created with an open source that costed less than 1,000 dollars, as Stratasys believed that Wilson was illegally operating (Hotz, 2012).

This was due to two major arguments. Firstly, as Wilson lacked the official arm manufacturing licence, he would be breaking the American regulations for the official manufacturing of weapons. In addition, as the only sunk cost for home-made future guns producers would be the purchase of the blueprints and the 3D device, this could allow them to lower the selling price of the printed firearm, ultimately encouraging dumping practices. Consequently, as soon as the company knew about the long-term plans of Defense Distributed, it threatened legal action and pulled the lease of the rented printer (Beckhunsen, 2012).

However, the end of the partnership with Stratasys did not put an end to Wilson´s 3D printing ambitions. He acquired the federal licence to manufacture and deal firearms to ensure that the company would not face fines on that regard and could legally continue working on further printable prototypes. His effort

resulted in the creation of the Liberator pistol, whose printable files were downloaded over 100,000 times during first two days in which the blueprints were available on the official website of Defense Distributed.

Then, the State Department Office of Defence Trade Controls Compliance demanded the company to remove the files from its website, as it believed that Defense Distributed was violating the laws regarding the international export of unapproved arms (Greenberg, 2013). The International Traffic in Arms Regulations laws, largely known as ITAR, supervise the fair and competitive export procedure of all weapons manufactured within the US territory, aiming to safeguard US national security. This law, combined with the Arms Export Control Act (AECA) entitles the President of the US as the authority to supervise the export of defence related articles.

Since the beginning of the War on Terror and the rising public criticism towards the tenancy and manufacturing of weapons, the ITAR law has experienced several reforms related to the development of new technologies and regarding satellite manufacturing, while restricting the export of weaponry to specific countries like North Korea, Iraq or Iran (Controls, 2018).

Therefore, the uploading of the Defense Distributed blueprints for the development of a plastic pistol defied the restrictions of the ITAR laws, as anyone, anywhere, could manufacture the Liberator with an affordable open-source 3D printer, which could be acquired online for less than 1,000$ (Greenberg, 2013). Therefore, the State Department Office of Defence Trade Controls Compliance demanded Cody Wilson´s group to retrieve the blueprints from their official website.

Nonetheless, this command did not stop the online circulation of the Liberator manufacturing files, as by the time that Defense Distributed applied the Official demand, the blueprints of the firearm had already been uploaded in alternative pirate sites like Pirate Bay or Mega. This latter dark web domain is administered by the experienced hacker Kim Dotcom and it uses advanced cryptographic methods to guarantee the safety of its users. Dotcom is a Finish Internet entrepreneur that heads the Unites States list of internet piracy enemies, and has faced several trials regarding racketeering, money laundry, copyright infringement or wire fraud (Farivar, 2015).

The anarchist philosophy of Kim Dotcom matched the ideals of Cody Wilson, which led the founder of Defense Distributed to seek an alliance that went beyond the initial cooperation in the spread of the Liberator files. The cooperation between Mega and Defense Distributed is believed to be one of the most dangerous partnerships on the Dark Web, and a consequent threat for International Security, given the broad dimensions of hidden internet domains and the applicability of 3D weapons. In fact, in a conjoint interview in 2013, Cody Wilson stated that their mutual goal was to create unblockable files and store them in an archive that enclosed multidimensional blueprints, ranging from weapons to human organs

(Rayner, 2013). This manifest illustrates how dangerous the partnership between 3D printing and criminal mindsets can become.

Therefore, the case study of Defense Distributed proves that the illegal use of additive manufacturing technologies is already a menace to International Security as it is significantly contributing to the proliferation of unregistered weapons. This threat is due to three major reasons, which have been introduced during the analysis of this case study:

1) **3D printers are becoming more affordable**: The rising popularity of this new technology and its increasing applications aside from the industrial sector is boosting the demand of these devices. This consumer trend is increasing the competition between additive manufacturing firms, which are lowering the price of their products to attract new consumers. Therefore, even though the price of most of these private consumer-oriented printers is already affordable, compared to the average price of a mobile phone, it is expected that in the upcoming years their price-quality relationship will improve (Geissbauer, Lehr, & Wunderlin, 2017).
2) **Internet is contributing to the distribution of 3D weapon´s blueprints**: As the ratio of people that are connected to the global net increases[8], more people can have access not only to the legal facilities of Internet, but also to the dark content of the web, including this type of files.
3) **The lack of regulation of this technology**: As seen in the counterfeiting sector, the slow inclusion of 3D printing to the codes of law is creating legal vacuums from which 3D criminals are profiting. We will study this matter using the Defense Distributed case study in the next epigraph.

5.4.1. THE WIKI-WEAPON PROJECT: LEGAL OBSTACLES AND RESOLVING MECHANISMS

Despite the effort of shutting down Defense Distributed and its partner operating network, Cody Wilson has managed to overcome all sort of judiciary impediments. He has profited from the existing legal vacuums with regards to the ITAR regulations. Given that Defense Distributed is registered as a non-profit domain, Wilson has argued that the files created by the company are aimed at fostering research activities or to provide a service for the "public interest" and therefore would be excluded from the ITAR regulations. (Wilson, 2013)

As a former law graduate, Wilson knew that to be eligible for this exemption, the files produced by Defense Distributed needed to be stored in a depository open to public with free Internet access. Thus,

[8] According to Nielsen Online, the number of Internet Users in 2017 amounted to 4 billion people, which resulted from a 54.4% penetration rate in the last 18 years. (Nielsen, 2017)

Defense Distributed has registered a selling-partnership with a bookstore in Austin, whose name has remained veiled by request of its owners (Greenberg, 2013).

These strategic protection movements have safeguarded the business of Cody Wilson, who has continued defending his firms´ slogan “an arm in every home” (DD, 2017). Moreover, the company has filed a lawsuit against the US Government, seconded by the Second Amendment Foundation, an organisation whose aim is to “promote the private possession of firearms by carrying legal action programs to defend fair causes”. (Second Amendment Foundation, 2018)

Defense Distributed and its partner plaintiffs accused the Federal Administration of violating the civilian rights coined in the First and Second Amendments of the American Constitution. On one hand, as the First Amendment ensures the non-violation of freedom of speech, if online files are understood as “code of speech”, the government may have no power to monitor and impede the transfer of those files.

Nonetheless, the appellation to the First Amendment is not an invention of Cody Wilson´s defence, as this strategy was also recurrently used in the 1990´s during the rise of the Cryptographic Wars. The “Crypto Wars” is the unofficial name of the United States struggle to diminish the creation of cryptographic methods advanced enough to impede decryption processes of national intelligence bodies (EEF, 2016). In that decade, one of the legal tools used to prosecute cryptographers that posted free online strong encryption tools were the ITAR regulations. The solidity of the law seemed to be uncontested until Dan Bernstein, one of the most renowned hackers of that time, decided to take the State Department to trial, basing his accusations on infringements of the First Amendment. The trial did not only result in the victory of Bernstein, but he stood as a reference for future internet entrepreneurs like Cody Wilson. Indeed, he has publicly referred to himself as “the spiritual heir of Bernstein” (Greenberg, 2015).

The additional argument used by the founder of Defense Distributed is based on the Second Amendment right of “keeping and bearing arms”, the original request of the State Department Office of Defence Trade Controls Compliance of retrieving the blueprints of the Liberator pistol would be unsubstantiated. Therefore, the central claim of Defense Distributed is that posting anything on Internet cannot be understood as a potential export, as this statement would justify the imposition of a veiled censorship prior to the publishing of any online content; a suppression that would be unconstitutional (Greenberg, 2015).

The complexity of this case is not only due to the well-supported arguments of Defense Distributed´s defence, but also to the future implications that the final resolution may have not only for 3D gunsmiths but also for further illegally printed goods. Therefore, the transcendental conclusions of this trial are lengthening its judiciary resolution.

Apart from this ongoing lawsuit process, Defense Distributed may have to face future charges regarding the Undetectable Firearms Act. This law was passed in 1988, aiming to safeguard the National Security by "banning the manufacture, possession or transfer of firearms with less than 105 grams of metal content, and obliging the manufacturing of legal firearms in the traditional shape of a handgun" (Undetectable Firearms Act, 1988).

The Undetectable Firearms Act, which expired in 2013, was renewed for a ten-year period to protect Americans from potential harmful consequences of 3D printing. This relatively short expansion in time was due to the strong opposition of the National Rifle Association, who had been lobbying against any modification of the expiring law. Moreover, the pressure derived from the Weapon Lobby has been one of the major impediments for the approval of one bill extension suggested by the Democrats, which aimed to include a more detailed specification regarding the components of the weapon that should be made of metal, depending on the nature of the concrete firearm (rifle, pistol, etc.) (Roberts, 2013).

The additional modifications applied to the 1988 Act sought to impede the circulation of "Ghost Guns", arms which are untraceable as they do not contain metal pieces nor have been assigned a legal serial number (Greenfield, 2017). Even though the resulting 2013 Modernisation Act does not impede the manufacturing of 3D weapons per se, it makes mandatory for the firearms to contain a non-removable piece of metal which makes the circulation of firearms less difficult to monitor. Therefore, this legal imposition ensures that any weapon could be detectable by traditional security devices such as X-ray machines or airport metal detectors; regardless of their printed or non-printed nature.

However, critics to this reform argue that this latest modification would not stop 3D gunsmiths from producing firearms with a disguised removable metal component. Even though this law does not prohibit the manufacturing of 3D weapons, this metal requirement could serve as a deterrent policy for those who opt to carry a Ghost gun, and a precedent for similar modifications in international codes of law. At the end of the day, Additive Manufacturing is an example of the future legal battlefields that are expected to take place in international courts, related to the security provisions of new technologies.

Even though the 2013 Modification Act implied a significant advancement in the regulation of additive manufacturing technology from the security standpoint, the difficulty to reach consensus and the inherent length of the debating procedure has diversified the legislative combating methods against illegal 3D weapon manufacturing. For example, during the Obama Administration, the Operation Choke Point was an alternative policy to combat the illicit production of firearms, including 3D printed weapons.

This policy, supervised by the United States Department of Justice, was aimed at investigating the banks and individual lenders that provided funding to firearm dealers, aiming to identify potential money

laundry operations and safeguarding national security. However, the underlying reason of this policy was to discourage financial institutions to support gunsmiths, and ultimately leaving them with no access to alternative funding resources to produce new weaponry. However, this policy was repealed in 2017 under the Presidency of Donald Trump, which is fonder of weapon-related activities than the Obama´s Administration (Guida, 2017).

Despite the regulatory advancements in the American Law and the ongoing judiciary procedures, the Administration´s effort to shut down Defense Distributed has been in vain. Cody Wilson has not only continued operating his project, but he has also widened the list of products offered to ease the production of home-made firearms. He understood the manufacturing of 3D plastic printed lowers only as a starting point, and his steady investigating endeavour has resulted in the accomplishment of a more ambitious achievement.

In 2015 Defense Distributed released the Ghost Gunner, a mill that enables the production of 80% aluminium lowers by using Computer Numerical Control; a technology that transfers pre-programmed sequences to the machine cutters, which shape the final object (Lynch, 2015). The Ghost Gunner mill ensures the production of lowers that are apt not only for single shot handguns like the Liberator pistol, but also for more complex weapons such as the AR 15 semi-automatic rifle and the AR 10 battle riffle, firearms that can last more than 650 rounds (Beckstrand, 2018).

Nonetheless, the initial price of the Ghost Gunner was not as competitive as the second edition of the Ghost Gunner mill, released in 2017, whose price was set below the 1,200$ barrier. This mill is more sophisticated than its predecessor as it offers its customers the opportunity to fully print the receivers of M1911 and Glock pistols, two of the most common handguns in the market (Mattise, 2017). This machine is the crowning jewel of the revenues of Defense Distributed, which amounted to $2,7 million in 2017 thanks to the sale of 4,000 Ghost Gunner mills (Del Castillo, 2018).

The launching of the Ghost Gunner II took place following the new legal status of the owner of Defense Distributed. Since Cody Wilson had not acquired the federal gun manufacturer license by the time that Ghost Gunner I was released, this previous machine needed to be fed with semi-finished lowers, which had to be purchased in advanced by the mill user. However, since the owner of Defense Distributed became registered as a firearms dealer in 2016, customers are no longer required to purchase the lower prior to acquiring the Ghost Gunner II, as Wilson is today legally allowed to provide them with this essential piece (Mattise, 2017).

Therefore, Wilson has been counteracting the legal movements of the American Administration to safeguard the running of Defense Distributed. The still embryonic additive manufacturing regulating laws

has helped Wilson to profit from the existing legal vacuums to defend his business with legally supported arguments. In his last public interview in 2017, he argued that as Defense Distributed mills can print out other goods apart from firearms (depending on the CAD file inserted in the machine), these devices cannot be exclusively understood as a gun manufacturing machines, and neither conceived as a threat to arm proliferation.

Moreover, the owner of Defense Distributed defends that printing guns with his mills does not break the rules regarding the official regulation of firearms, as the only piece that is regulated by the Government is the receiver, not the lower (Prestigiacomo, 2017). This reasoning follows the manifested anarchist philosophy of the organisation, as they believe that the development of new weaponry products only menaces the Government´s monopoly of firearm production. In addition, Cody Wilson has argued that 3D printing is rather than a threat to security a tool to ensure the protection of American citizens, with regards to the bloodsheds that have taken place in the last years in the United States (Greenfield, 2017).

Nonetheless, the Government´s standpoint differs from this belief, and Cody Wilson has been ranked since 2015 as one of the most dangerous people in the world (Shortlist, 2018). The American Administration fears that the ease of weapon manufacturing could result in the commission of new attacks, given the increasing sophistication of printed firearms. The most recent achievement on this regard has been the launching of the first fully printed metal 1911 gun by the company “Solid Concepts”, one of the leading providers of 3D printers (Stratasys, 2017).

6. CIRCULATION OF 3D PRINTED WEAPONS AND INTERNATIONAL TERRORISM

Even though Defense Distributed and Solid Concepts are only two examples of the rising importance and sophistication of AM firearm production, they illustrate how the circulation and manufacturing of 3D printed weapons has become one of the most difficult technological threats that International Governments face when combating the Dark Web operations.

According to the United Kingdom´s National Strategy for Additive Manufacturing Report of 2018-2025, there are three differentiated consumers of printed weapons and their related documents. The main demander of this technology is an individual consumer which can´t either access to a legal gun license or who wishes to acquire an additional weapon for a more affordable price than that of the average market (Additive Manufacturing Steering Group, 2018). In the first case, the consequences of the acquisition or production of the printed gun can be highly dangerous, as the denegation of a gun license is generally due to age or mental limitations or previous crime records.

The second consumer profile are arm traffickers or illicit manufacturers, who wish to profit from the obtuseness of the black Internet to trade their products, by producing the weapons under specific demand while lessening the risk of being detected by security forces. As these monetary transactions are usually done in crypto coins, a monetary unit that is not supervised by official financial institutions, the money flows from these illegal operations are highly difficult to monitor. (Additive Manufacturing Steering Group, 2018). This financial modus operandi has been promoted by figures like Cody Wilson, given that around 45% of Defense Distributed´s annual revenues come from cryptocurrency (Redman, 2017). In addition, he has also supported the creation of the "Dark Market", a hidden digital exchange platform in which the trade operations can only be made in bitcoins (Del Castillo, 2018).

Nevertheless, among the three groups signalled in the report, the most dangerous users of printed weapons and files are terrorists, who have found in 3D technology an access to fully operative arms at a cheaper cost (Additive Manufacturing Steering Group, 2018). Moreover, the attractiveness of Additive Manufacturing is especially justified in regions were arm trade is more supervised and weaponry counterfeiting is combatted with stricter legal regulations and punishments. Thus, 3D printing presents terrorists with the opportunity of limitless weaponry supply to commit their attacks, freeing them from their dependency on traditional arm providers.

In addition, additive manufacturing has helped terrorist groups to broaden their funding resources by increasing their participation in counterfeiting operations. Even though this illegal trade was already one of their preferred financial methods; according to Interpol statistics, it is expected that the sophistication of AM methods would increase the participation of terrorist groups in counterfeit operations in the upcoming years (Nastase, 2008).

The increasingly efficacy of printed firearms has become an additional reason for terrorists to conceive 3d printing as a priceless ally. The rapid advancements in additive manufacturing technology have enabled the creation of firearms made of powdered metal instead of plastic, which provides the bullet with a larger and more precise trajectory. To date, the most proficient metal 3D printed pistol can impact an object located at 30 meters from the shooter, but it is expected that in the upcoming years this trajectory could be expanded thanks to technological advancements (Plafke, 2017).

Therefore, the Fourth Industrial Revolution is not only enhancing progress in key areas such as engineering or the biomedical sector, but it is also helping terrorists and criminals to profit from these technologies to be more efficient while conducting their illegal activities or attacks.

6.1. NEW TERRORIST METHODS

Since the beginning of the Fourth Wave of International Terrorism[9], scholars in the field have discussed the role that innovation plays in the development of new terrorist tactics, focusing the debate on the degree of incorporation of new technologies into their operative apparatus. In this regard, we can distinguish two opposite academic currents: the defenders of the role of innovation for terrorist groups and those that subscribe that innovation is a secondary feature for international terrorists.

Regarding this former group of scholars, they defend that terrorist groups only adopt innovative technologies when their implementation cost is not significant. According to them, the decision of introducing a new attacking method is driven by two key aspects: the ratio of damage caused and the cost of implementation of the new tactic, measured in terms of investment and training required. Nonetheless, if the new method proves to be impactful enough, funding becomes a secondary issue, especially for financially-sound organisations such as Al-Qaeda. Thereby, the ultimate decision drivers are the lethal capacity of the new tactic and its potential to spread/transmit the organisation's message while spreading fear. However, if the new weapon proves to be as impactful as other more rudimentary methods to which the organisation is already accustomed to, such as bombing devices, it will be dismissed (Ranstorp & Normark, 2015).

This argument is partially influenced by the historical performance of organisations such as Al-Qaeda. During the 90´s Osama Bin Laden manifested his "Islamic duty" to include weapons of mass destruction in his Jihad, attempting to perform more impactful attacks by using this technology. Despite the procurement efforts of that decade, aimed at carrying a nuclear-based attack following the 9/11, Al-Qaeda failed in his WMD adventure. According to Rolf Mowatt-Larssen, former director of the CIA, the reason for this failure was the "overpowering interest of Al-Qaeda to carry as many as possible big-impression attacks", which was incompatible with the slow development of these weapons (Larssen-Mowatt, 2010).

The enormous coordination and expertise that the WMD development plans required left Al-Qaeda in a practical dichotomy: It was either investing in R&D and hope to carry few impressive attacks, separated in time, or to rely in conventional tactics to carry more frequent and still impactful attacks. Osama Bin Laden chose the second option (Rapoport, 2002).

[9] As specified in the terminological chapter, the history of modern terrorism is divided into 4 Waves depending on the nature and goals of the attacks committed. The 4th Wave, that started in 1979 is also known as the religious wave, given that the main aim of most of the terrorist groups is to rearrange the International Order according to extreme religious principles (Rapoport, 2002).

In addition to Al-Qaeda´s case study argument, these scholars defend their position by stating that in the last forty years international terrorists have preferred to emulate successful attacking methods rather than seeking to innovate (Ranstorp & Normark, 2015). This has been demonstrated in the replication of the airplane hijackings during the 1980´s, 1990´s and early 2000´s and more recently with the successive vehicle-ramming attacks in Europe. However, given that these reproduced methods were once innovative attacks, these scholars acknowledge that innovation is not completely absent in terrorist organizations. Nonetheless, they argue that it only takes place occasionally and it is more often due to the disruptive effort of a single cell or an individual combatant than the result of a coordinated long-term strategy of the whole organisation (Ranstorp & Normark, 2015).

Opposing these theorists, the alternative academic current defends that innovation is a core element of international terrorism. These scholars believe that terrorists profit from innovation and new technologies to better target their objectives, as well as to sort the surveillance of counter-terrorist agencies. Rafaello Pantucci, Director of International Security Studies at the Royal United Services Institute (RUSI) and one of the subscribers of this vision, argues that Innovation and learning are the "essence of modern Jihad", providing the example of Al-Qaeda to defend his perspective (Pantucci, 2015).

In the last years, this terrorist organisation has created an online network through which its members can distribute key documents and new attacking guidelines, which are later published in Al Qaeda´s Inspire magazine. This publication, whose first issue was distributed in 2010, has fostered the emergence of autonomous international combatants, whom have followed the advices of this magazine to carry their attacks. These are lone-wolf[10] attackers, whose activity is the consequence of the globalisation of terrorism and the rise of new technologies; they mutually support each other by transferring soft skills and technological know-how thanks to new instruments such as the magazine and the world wide web (Spaaij, 2010).

This exchange of technological knowledge has contributed to the development of new terrorist tactics, which include the introduction of Additive Manufacturing as a supportive attacking technology. Even though the Inspire magazine has not published blueprints for 3D printed weapons, it has already included instructions for building similar undetectable home-made weapons, such as the pressure-cooker bombs, used to carry the Boston Marathon attacks (Hopkins, 2016). Therefore, we can conclude that it is only a matter of time that this publication includes instructions on how to use additive manufacturing as a terrorist tactic.

[10] Lone wolves are terrorists who usually commit attacks on their own, and even though they may be willing to contribute to the mission of a concrete organization, they have no formal ties to it. (Strohm, 2017)

Prior to describing the role that 3D printing plays in modern terrorism, this chapter will briefly cover other new terrorist tactics that proving that innovation is not only present in terrorist organisations, but that it is also fostering the development of new dangerous attacking techniques; including drone-jacking, med-jacking and terrorism of things as the most representative examples (Wittman, 2017).

6.1.1. DRONE-JACKING

In the last years, intelligence agencies have warned about the rising utilisation of drones as terrorist weapons, parallel to the incorporation of Unmanned Aerial Vehicles (UAV) to the defence fleets of international governments. These machines, crafted to reach inaccessible locations and to transport light packages, are being used by terrorists to deliver weapons or to drop bombing devices, especially in warzones. In fact, drone attacks have become a serious problem for the United States´ Army when combating DAESH fighters in Iraq or Syria, as terrorists have modified unmanned vehicles to drop grenades against US Forces (Von Drehle, 2017). Terrorist´s access to these devices has been granted due to two main reasons: the price plummeting of commercial drones and the mastering of the "drone-jacking" technique.

Regarding the affordability of drones, this statement refers to the most basic commercial Unmanned Aerial Vehicles, whose starting price can be found around a hundred dollars (B.I, 2017). Therefore, purchasing a basic vehicle would not require a large investment effort for terrorists, who could subsequently modify it and provide the UAV with the ad-hoc features required to commit an attack (Meola, 2017).

However, when analysing military drones, they are not as affordable as commercial UAVs, as their price rises in accordance to the features of the vehicle. According to the United States Airforce Report of 2015, the most expensive drone purchased in that year was the MQ-9 Reaper, commonly known as "Predator B[11]", whose price amounted to $64.2 million (US. Airforce, 2015). This significant cost would justify the new terrorist phenomenon known as "drone-jacking", which consists of kidnapping these devices to either knock out the vehicle or re-program the device to obey new commands (Rodday, 2016).

The first registered drone-jacking attack took place during the Iraqi war in 2009 when a Predator drone was kidnapped by using a $25,95 Windows software designed in Russia (Staniford, 2017). This program enabled hackers to silently take over the drone and use it to commit an attack against US Forces. Moreover, according to a study conducted by the University of Twente, this kidnapping procedure is

[11] Predator B is the flagship unmanned vehicle of the firm General Atomics, and it is able to launch Hellfire missiles and laser bombs while being controlled at a distance of 7,500 miles (Villarejo, 2017).

relatively easy for hackers, given that most military UAVs are equipped with a vulnerable GPS unit that enables their penetration (Di Nucci, 2016).

Therefore, experts fear that drone-jacking could become a recurrent modus operandi for terrorists to carry bloodier attacks. In addition, the study of the University of Twente warns about how drones can even be used as "potential missiles against civilians" a feature that will increase the lethality of these weapons (Di Nucci, 2016). Even though drone strikes have already caused civilian casualties[12] in war zones, this study warns about how terrorists may use these devices as blackmailing instruments, as they can program them to deliberately crash against determined human populations. Moreover, according to this previous study, it is also a matter of time that terrorists use drones to commit attacks in western ground such as in sporting or music events (Di Nucci, 2016).

This reflection shall be taken into consideration by counter-terrorist experts, given that it is expected that in the upcoming years the fleet of international UAVs will amount up to 30,000 operating vehicles (Humphrey, 2017).

6.1.2. MED-JACKING

Apart from "Drone-jacking", experts in terrorism have warned about a second technological hijacking practice in vogue, known as "Med-jacking". This technique consists in hacking an implanted medical device of a patient, who can only recover the full-control of the device if he satisfies the terrorist demands (Mackey, 2016).

Med-jacking has leveraged extorsion practices to a "life or death" dimension, as random manipulation of medical devices can have fatal consequences in sensitive patients. Nonetheless, hacking implantable devices is still a limited practice, given that med-hackers still hesitate when to attack these inserted devices due to the risk of assassinating the patient before the fulfilment of the blackmailing demands (Newman, 2017).

Even though med-jacking generally refers to the attack of implantable elements such as pacemakers or hybrid organs[13], the hacking of other hospital instrumental such as X-ray machines can also be considered as med-jacking attacks. Hackers use these machines, which lack of advanced mechanisms of cyber protection, as launchpads for larger attacks, such as those aimed at stealing classified hospital data (Newman, 2017).

[12] During Barak Obama´s Administration, there was controversy about the civilian casualties that derived from the imprecision of American drone strikes when eliminating "targeted enemies". (Ackerman, 2014)
[13] Hybrid organs are partially crafted by biomedical machines and consist in artificial organs which result from the combination of synthetic materials and living cells (Colton, 1995).

According to the New World Economic Forum report on Cyber Risk, terrorists and cybercriminals have increased their interest in stealing personal information from patients. This is due to the attractiveness of the data kept in hospital´s archives, which usually includes sensitive content ranging from personal data to financial information, which could be used by med-jackers to commit illegal operations, including tax fraud or identity theft (Newman, 2017).

One of the most recent med-jack attacks to hospital archives took place during the 2017 WannaCry international cyberattack, when some of the hospitals of the American and British network were attacked by malicious ransomware (Fox-Brewster, 2017). The international scope of this operation along with the value of the data stolen from the hijacked clinics did not only illustrate the consequences that medical cyberattacks can have; but it also evinced that current measures of cyber-protection are insufficient to combat these digital attacks (Gayle, 2017).

Therefore, it is essential that modern counter-terrorist policies consider med-jacking as a key element to tackle, as the rapid evolution of technology and the increasing obtuseness of cyber-insecurity dimensions may lead international terrorists to use med-jacking as a recurrent extorsion technique.

6.1.3. TERRORISM OF THINGS

The threat of med-jacking is linked to the new "Terrorism of things" phenomenon. This term derives from the concept "Internet of Things" (IoT), which is the international network of devices that are interconnected thanks to the electronic sensors and software that comprise their systems (Brown, 2016). Technology enthusiasts have embraced IoT as the ultimate invention of the Fourth Industrial Revolution[14], given the limitless opportunities that multipolar connectivity offers. However, in the advent of the recent cyberattacks, the Internet of Things could be used by terrorists to commit more precise and damaging attacks, as any device connected to this Mega network is subjected to be hacked and remotely commanded by the cyber-attacker (Columbus, 2016).

Internet of things has been ranked by International Security Agencies such as Interpol as one of the most troublesome security dilemmas of the upcoming years. This threat is due to two major concerns, that derive from the exponential growth of Internet-connected devices. In 2020, it is expected that the number of intelligent devices will amount to 50 billion objects, whose nature will range from home appliances to governmental devices that monitor urban infrastructures (Columbus, 2016). If these objects were

[14] The "Fourth Industrial Revolution" is the technological process that is "fusing the physical, digital and biological dimensions" thanks to the development of new elements such as machine learning, internet of things or artificial intelligence which are shaping multidisciplinary domains (Schwab, 2017).

hijacked, terrorists will not only have access to public information or official buildings, but they will also obtain the key to every "intelligent" home, being able to carry attacks from the "inside" (Columbus, 2016).

In 2014 the CIA directorate of science and technology, reported several cyberattacks to home appliances as a criminal extorsion technique (CIA,2014). One of the most recurrent IoT attacks consists in the random manipulation of the LED lights of the house, aimed at causing physical damages to its dwellers, including lack of sleep or psychological crisis, so that they are obliged to fulfil the blackmailing demands (Lang, 2014).

The increasing introduction of intelligent devices in households has pushed manufacturers to cut production costs to turn their technologies into more price-competitive, rather than in focusing on the improvement of their firewalls. Even though some institutions[15] have warned about the consequences of this manufacturing choice, there is still lack of consensus with regards to safety standards of IoT devices; and hackers are profiting from this security gaps to hijack these devices and turn them against their owners (Howard, 2015).

In addition to these household attacks, Terrorism of Things has already been reported in larger operations against governmental infrastructures. In 2016, a group of hackers affiliated to Hezbollah penetrated the network of security cameras of the Ministry of Defence building in Tel Aviv. This action enabled hackers to penetrate the security system of the Ministry and steal sensitive material from its archives (Staff, 2016). Therefore, considering these attacking possibilities, it is likely that Internet of Things will become a key supportive attacking tool for international terrorists in the upcoming years, being an essential area to take into consideration by counter-terrorist institutions.

7. 3D TERRORISM: THE DARK APPLICATIONS OF ADDITIVE MANUFACTURING

Drone-jacking, Med-jacking and Terrorism of Things are three examples that illustrate how terrorists are eager to profit from technological advancements to ensure that their performance is as impactful as possible. Therefore, the incorporation of Additive Manufacturing techniques into their modus operandi follows this same reasoning, as this technology enables terrorists to print either weapons or any other supportive attacking material. Given the rapid evolution of 3D technologies, today´s printing barriers (such as the materials eligible for the manufacturing process) will likely be torn down in the upcoming years, providing terrorists with even more lethal instrumental to support their attacks (Pearson, 2018).

[15] The European Commission has addressed this concern with the new Proposal of Regulation on Privacy and Electronic Communications, which was presented in 2017, and which aims to regulate the minimum-security standards of IoT devices (European Commission, 2017).

This menace has been progressively understood by Intelligence bodies as a present threat to international security, rather than a future menace. This warning hype begun in 2013, when the American Department of Homeland Security Intelligence distributed a bulletin that warned about the impossibility to stop or monitor the production of 3D-printed guns, raising awareness on how terrorists could profit from this situation (Winter, 2013).

This bulletin was one of the first official documents that warned about the linkage between terrorism and 3D printing. Despite its national focus, centred in how this technology threatened domestic counter-terrorist policies, this study contributed to the development of further investigations conducted from an international perspective (Swanner, 2017).

In the last years, experts in counter-terrorism have increasingly warned about the consequences that the terrorist utilisation of 3D technologies may have over international security. During 2015 Counter-Terror Expo in London, Mark Rowley (Head of Special Operations of the Metropolitan Police) signalled in a public speech that it is not unrealistic to assume that terrorists may seek access to these technologies to build airborne drones or bombing devices (Goerke, 2015). According to Rowley, the combat against this new technology has just started and will be one of the main intelligence wrestling arenas of this century (Goehrke, 2015). Therefore, he showed his concern regarding the current preparation of international security forces to address this threat, as he believes that most counter-terrorist units are excessively focused on combating traditional tactics (Goehrke, 2015). To conclude his intervention, Rowley provided the example of his own team of police investigators, who were able to detain a British 3D gunsmith which was suspected of manufacturing weapons for local terrorists (Goehrke, 2015).

Nonetheless, despite the laudable effort of his team, the Metropolitan Police of London was unable to prevent the assassination of the British congresswomen Jo Cox, who was shot dead by a neo-Nazi terrorist in 2016 with a home-made pistol (Evans, 2013). Even though the official reports did not specify how the gun was constructed, experts such as Poole from the University of Coventry fear that the crime weapon was indeed 3D-printed (Mezzofiore, 2016). This is due to the testimonies of the witnesses to the assassination, who reported to the police that the murdered had used a somewhat rudimentary weapon that had to be reloaded to shoot another bullet (Mezzofiore, 2016). This description would adjust with that of a basic 3D printed gun, as these weapons need to be reloaded after each shot (Kantchev, 2013).

Moreover, later investigations demonstrated that the murderer, Thomas Mair, had bought several manuals issued by the Neo-Nazi terrorist organisation National Alliance which taught its supporters on how to build home-made guns (Hatewatch, 2016). If Thomas Mair had had access to a 3D printer, he could have even improved the blueprints of these old-fashioned manuals to develop the lethal weapon that

assassinated Jo Cox. Nonetheless, it needs to be mentioned that these are just theorist´s suspicions and that the crime weapon was never publicly categorised as a 3D printed gun.

Even though the Police forces were not able to avoid Jo Cox´s assassination, in the last years there have been successful stories concerning the prevention of the terrorist use of 3D printed weapons. In 2015 an investigation carried by the Hong Kong Public Security Bureau stopped a cell of terrorists that attempted to attack government infrastructures by using airsoft guns modified with 3D printers (Lubrano, 2018). Moreover, during the police raid of the terrorist´s warehouse, there were found materials that could indicate that this cell was attempting to build a 3D printed bombing device, as there were detected residues of Hexamethylene triperoxide diamine (Lubrano, 2018).

This material is a highly explosive organic compound used by terrorists to build home-made bombs, such as those detonated in the London attacks of 2005 (Savage, 2005). Therefore, if this cell had not been dismantled, it may have continued experimenting potential ways of including this material in the printing procedure, possibly resulting in the innovation of a new dangerous 3D printing ad hoc technique (Lubrano, 2018).

The dismantlement of this cell took place following the detention of Yoshitomo Imura in 2014 (Ensor, 2014). This Japanese employee of the Shonan Institute of Technology was imprisoned for having developed a home-made 3D printed gun, whose manufacturing blueprints were posted and distributed online. Although the Japanese police was unable to link Yoshitomo with any terrorist organisation, they feared that he may have inspired Asian terrorist cells such as that of the failed Hong-Kong attack (Lubrano, 2018).

Even though Japanese security forces have dealt with other 3D printing insecurity problems since the detention of Yoshitomo in 2014, in the last years this technology has become an issue of major concern in the context of the ongoing dispute between the Yakuza´s[16] splinter groups. During a raid of the Hyogo Police Department, it was discovered that some of these minority groups possessed 3D printed weapons stored in their warehouses, as well as the machines that had been used to produce these arms (Keiligh, 2015). These findings did not only demonstrate that additive manufacturing was arming these groups, but it was also enabling the continuation of the inter-Yakuza´s conflict, as these splinter groups would otherwise have a more limited access to weapon supplies (Adelstein, 2015). Consequently, the role of 3D printing was key to prolong this conflict and therefore alter the country´s security.

[16] The Yakuza is the largest transnational organised crime syndicate of the country, as it has over 100,000 active members which are aligned to four sub-branches of the organisation: the Yamiguchi-gumi, the Sumiyoshi-kai, the Inawaka-kai and the Aizukotetsu-kai (Kaplan, 2012).

These previous examples show that if 3D printing technologies fall into the hands of terrorist or similar supporting organisations, the consequences for international security could be severe. This warning was one of the issues tackled by Ban Ki Moon during his last speech in the United Nations Security Council as Secretary General in 2016. During his intervention, the former Secretary General manifested his concern on the role that emerging technologies will play in the upcoming years in the international arena, arguing that security forces need to be prepared to struggle against non-traditional threats, explicitly mentioning 3D printing as a technology with "potential for mass destruction" (UN Archives, 2016). This concern has been subscribed by several non-proliferation scholars, such as Grant Christopher, who has recommended governments to enact export restrictions on certain 3D desktop printers to minimise this risk (Tirone, 2016).

Therefore, considering the previous examples and warnings of renown security authorities and scholars, we can identify three main elements inherent to the use of 3D printing as a weapon facilitator that are challenging International Security. These challenges comprise the detection and tracking of plastic weapons, the dismantlement of illegal gunsmith´s facilities and the difficulties that derive from the elimination of online blueprints.

7.1. DETECTION OF 3D PRINTED WEAPONS

The detection of 3D printed weapons accounts for one of the most difficult challenges that additive manufacturing presents to traditional security systems, which include X-ray scanners and metal detectors as the most representative security provisions. Considering this former device, these machines are only programmed to track items that contain metal pieces, and therefore are incapable of identifying printed plastic weapons, offering no protection against these arms (Randolph, 2015). Given that the most frequent security mechanisms that safeguard public and private facilities are metal detectors, 3D printed weapons will diminish their functionality, and thus minimise these buildings 'protection.

However, given that most of the circulating 3D manufactured weapons still require a firing pin to be operative or are crafted to function with metal bullets, these elements would be noticed by metal detectors (Koslow, 2017). For example, in 2016 the security system of the Reno-Tahoe airport of Nevada identified a 3D printed gun inside a luggage because it was loaded with live rounds. Thereby it was the ammunition that revealed the transportation of that pistol, which would otherwise have trespassed the metal detectors without being noticed (Lubrano, 2018).

Nonetheless, it must be borne in mind that some of these metallic elements, including the bullets, can be removed from the gun to fool these security mechanisms, being re-loaded into the weapon once it reaches its final destination. Therefore, these systems can only minimise the chances of terrorists to use

these guns inside these facilities, but they cannot help to combat the circulation of the plastic carcass of 3D weapons (Koslow, 2017).

Thereby, security forces should remain vigilant and willing to upgrade their security mechanisms, as plastic criminals are eager to continue improving the features of these weapons to turn them into more lethal and less traceable arms. Moreover, it is a matter of time that 3D printed weapons are recrafted to admit ammunitions that are not entirely made of metal, enabling them to be camouflaged from metal detectors.

In fact, there already exist some prototypes of these bullets, such as those crafted in 2013 by the German industrial engineer Jeff Heeszel, who was able to manufacture the first entirely printed bullets made of plastic and a minimum proportion of a metal alloy (Kleinman, 2013). Even though he did not distribute the blueprints to guide others to replicate his invention, as he manifested that his investigations were only for a scientific purpose, if terrorists managed to copy this prototype, current security detectors would become insufficient to track 3D printed guns (Greenberg, 2013).

In addition to metal detectors, X-ray scanners account for the most frequent security system that complements their protection function. Even though these machines could seem to amend the detecting weaknesses of metal arches, as they are able to trace objects regardless of their composition; since the introduction of disguisable and foldable weapons in the black market, the efficiency of X-ray machines has also become limited.

Although security corps have fought against these types of weapons since the 90´s, the decade in which the first foldable machine guns were created, the introduction of foldable 3D printed pistols presents an additional challenge to the detection of disguisable weapons. In 2016, the American company Ideal Conceal presented the prototype of a gun that simulated a smartphone when folded and which was intended to be created with additive manufacturing technologies (Chuck, 2016).

According to the company´s website description, this gun, which can be loaded with two bullets, can be folded upwards to be disguised as “an unassuming mobile phone” and therefore become “virtually undetectable to plain sight” (Ideal Conceal, 2017). Ideal Conceal has defended its product by claiming that it is aimed at serving “the same function as a derringer for people who carry concealed legally” and that its only objective is to give their customers access to an improved weapon for self-defence (Maccar, 2016).

However, the company´s vision differs from that of the security forces, who fear that if the weapon (which is pending patenting approval) becomes eligible to be distributed, it would present a challenge to security

agents, as they won´t be able to detect at first sight whether a citizen is carrying a normal cell phone or a two-bullet weapon (Hughes, 2017).

Despite the stand-by situation of the manufacturing of the "iPhone-gun", Ideal Conceal would already have received over 12,000 pre-orders for the gun, whose market price amounts to 375 euros (Hughes, 2017). Moreover, according to investigations of the British newspaper "The Times", European police departments such as the Belgian Police have already been notified about the potential introduction of these disguisable weapons in the continent and would be debating on how to prevent those importations to be distributed among European terrorist cells (Waterfield, 2017).

Therefore, high-tech printed weapons such as the "iPhone-gun" are not only challenging traditional security systems such as metal detectors or X-ray machines, but they are also defying the human capabilities of protection forces. These deficiencies need to be tackled both by fostering the know-how of security specialists and by amending the partial obsolescence of the most common safety systems. However, the upgrading of these mechanisms must not be an ad-hoc measure, as it requires an in-depth analysis that permits a thoughtfully adaptation of these devices to the detection demands of this new security menace (Koslow, 2017).

7.2. HOW TO COMBAT ILLEGAL GUNSMITH ACTIVITIES.

The second element that difficulties the combat against 3D terrorism is the detection of facilities in which the illegal gunsmiths manufacture printed weapons that can be potentially used to commit terrorist attacks. The process of identification and dismantlement of those facilities is complex, given the investigative effort required to target those suspects of being producing illegal additive manufacturing weapons (Kipp, 2016).

This process of identification is complicated due to the multiple profiles of the terrorists that either create their own 3D weapons or that order them to an additive manufacturing gunsmith. On one hand, the easiest group to target is the "public" supporters, people who are suspected of having become radicalised and whose behaviour has been affected since they decided to support a certain organisation (Rempo, 2018). These lone-wolves tend to be active users of Internet and social networks, in which they indirectly manifest their believes or ideological stigmas. These digital traces help investigators to monitor the actions of these combatants, so that it becomes more difficult for them to perpetrate their attacks (Bates, 2016). Therefore, once they are supervised, it would be highly difficult for these terrorists to either craft their 3D weapons or to order them to a 3D gunsmith without being uncovered (Rempo, 2018).

On the other hand, there is an alternative group of silent terrorists whose identification is significantly more difficult for intelligence bodies. Their profile is that of an apparently ordinary citizen, with none or insignificant previous police records and whose recent behaviour has not raised suspects (Bates, 2016). Unlike the other group of lone-wolves, these combatants do not share their radical views, and they do not reveal them until they commit their attacks. Therefore, it becomes highly difficult for the police not only to stop them before they carry a bloodshed, but to identify the places where they store their weapons (Goldstein, 2017).

Therefore, considering 3D printed weapons, the only feasible alternative that could help to combat 3D terrorism would be to register and monitor the activity of international 3D printers. However, this mission would not only overpass the current capabilities of intelligence bodies, but it will not prevent terrorists from accessing the black-market printers and thereby continue experimenting with 3D weapons.

7.3. HOW TO STOP THE DISTRIBUTION OF ONLINE BLUEPRINTS

Lastly, the third required area of intervention to fight against 3D terrorism would be the Dark Web, the digital network in which the online blueprints of the 3D weapons are distributed. However, this task faces two main obstacles, which are related to the obscureness of this online platform: the impossibility to remove all the distributed files and the lack of capabilities to prevent them to be uploaded again (Chen, 2008).

First of all, given that the Dark Web is a semi-hermetic network (it requires specific software and authorisations to navigate through it), there is no international organisation that supervises the content uploaded in the peer-to-peer darknets[17] that comprise this web. Therefore, intelligence bodies cannot be backed up by this system and would be helpless in their task to remove and stop the distribution of these files. Therefore, even if they succeeded in their removal mission, nothing would prevent anonymous individuals to re-upload them again (Chen, 2011).

Despite these three obstacles, 3D printing cannot be considered as an unbeatable menace nor the crowning jewel off modern terrorist methods. However, it is true that struggling against this threat requires not only the modernisation of existing security devices, but also extending current counter-terrorist policies. Nevertheless, and as mentioned in previous chapters, 3D printing has also positive implications for the reinforcement of International Security, a dimension that will be addressed in the next chapter.

17 Darknets are overlayed networks whose access is restricted to certain users, who can access them with specific software or by the explicit authorization of inner users (Wood, 2010).

8. POSITIVE USE OF 3D PRINTING TECHNOLOGIES TO REINFORCE INTERNATIONAL SECURITY

Even though the last chapters have illustrated the criminal and terrorist potential of 3D printing, additive manufacturing technologies have also become a key ally for international governments to modernise the existing security mechanisms, whilst creating new protection apparatus that can altogether contribute to the reinforcement of International Security.

The most direct application of 3D technologies has taken place in the Defence industry, which has introduced additive manufacturing procedures to update the maintenance systems of the military fleets and to craft new printed instrumental and vehicles. The main advantage that 3D technologies present to the manufacturing of military devices is that it allows Just-in-Time[18] production on a speed-to-market[19] basis, enabling multiple adjustments to traditional models while permitting their customization (Wen Wei & Thong Seah Ser, 2017). Its flexibility and rapidness are key to develop innovative solutions to traditional manufacturing limitations, such as the long production cycles of military material (Grant, 2010).

In the last decade, some of the most acknowledged military powers have included 3D technologies into their production chains, creating of economies of scale that have boosted their manufacturing logistics. Among these nations, the British Royal Air Force or the Polish Air Force have proudly reported that their fleet already includes aerial vehicles[20] with "protective covers and support struts" that have been manufactured with 3D- printing technologies.

Moreover, AM is helping international governments to combat military obsolescence, one of the most recurrent problems of defence logistics and whose solving accounts for a significant percentage[21] of International Defence budgets. Additive manufacturing can help to customise the components needed to keep the military equipment updated and thus contribute to the modernisation of Defence arsenals on a rolling basis; minimizing the sum traditionally needed to address this deficiency (OUSD, 2008).

Considering battlefield applications of 3D-printing, this process could prevent deployed troops from running out of material, providing them with any required supplies. The attractiveness of this possibility can be regarded from a double perspective. First of all, if military units carried portable 3D-printers, this would alleviate the weight of the objects transported during the mission, easing the mobility of the troops (Crouse, 2015). Secondly, given the rapid advancement of this technology and the diversification of the printable materials, these machines could supply military personnel with different goods, ranging from

18 Just-in-Time production is a production methodology which seeks to reduce flow times and response times from suppliers to costumers (Ohno, 1988).
19 Time-to-market refers to the length of time between a good is conceived until it is used by the final consumer (Kahn, 2004).
20 The first successful 3D-printed military components in the British Army have been crafted for the Tornado Fighter Jets, a variable-sweep multirole combat aircraft (Kelly, 2015).
21 Considering the Spanish Defence Budget, in 2017 the Modernization cost accounted for a 25% of the total budgetary sum (7.635 million euros) (BOE, 2017). In that same year, the French Administration spent 33% of its total Defence budget (45 billion euros) to modernise its military equipment; and the American Department of Defence allocated 44% of the total 650 billion dollars for the same regard (Louis & Joyce, 2016).

weapons to other functional objects (canteens, containers, etc.). The United States 'Army has already introduced these machines into its Rapid Equipping Force (REF), which carries a potent 3D printer and supportive workshop equipment during its missions (Wen Wei & Thong Seah Ser, 2017).

Apart from these military applications, additive manufacturing can also be used as a supportive tool to address humanitarian catastrophes. This technology will serve to back up humanitarian agents whenever there are difficulties to deliver assistance goods to the areas of disaster relief, due to broken procurement chains or weak communications´ infrastructures. Therefore, 3D printers could help to counteract these scarcities by procuring goods of basic needs while adjusting them to any given requirements (James, 2016). Moreover, the progressive introduction of machines that are eligible to print food can help to combat hunger, as these devices are able to produce edible food from basic elements such as "algae, mud, leaves or insects" (Editorial, 2018).

In addition of the utilisation of 3D printing in the military and humanitarian fields, this technology is also helping international governments to strike back at 3D-criminals by using their same attacking weapon. Additive manufacturing along with the advancements of Artificial Intelligence has enabled the prototyping of the first scanner that is able to trace 3D-printed pistols, as long as they are located at a maximum distance of thirty meters (Saunders, 2016). Their detection is possible as this machine does not focus on the shape or material of the objects, but on its density, which is analysed through the emission of radar waves similar to those of traffic-control devices. This new detector is conceived to be placed in strategic checkpoints in key buildings, so that they can rapidly scan individuals and alert Security bodies if they carry a suspicious plastic weapons (Physics, 2018). Despite the enthusiastic proposal of Radio Physics, the private enterprise in charge of developing this mechanism, the project has not been completed yet, and a team of R&D exerts are still working to sophisticate the tracing mechanism (Physics, 2018).

Another tool that is helping to combat plastic weapons is the development of an artificial dog-nose device that has been specifically designed to identify and track 3D-printed guns. The idea behind this "sniffing device" is to reproduce dog´s olfactive sensitiveness, with the replication of the smell receptors that enable these animals to detect plastic weapons. Even though it is not recognisable for human senses, the plastic material used to print 3D guns has a barely noticeable smell that does not escape the sniffing capabilities of dogs (Saunders, 2016). Hence, this nose replica, conjointly created with additive manufacturing technologies by the Massachussetts´ Institute of Technology and the United States Food and Drug Administration, will account for an essential security mechanism to combat the illegal distribution of these plastic firearms (Saunders, 2016).

Furthermore, international governments are not only working to stop the circulation of 3D weapons, but they are also focusing in deterring the online distribution of the blueprints of DIY arms. To struggle against the digital transmission of these files, they are using two complementary policies, inspired by the lessons learned from the fight against online copyright infringement (Trimble, 2017).

The first initiative consists in the creation of blocking codes, similar to those that combat online piracy, that detect the uploading of sensitive material as well as the online platform in which the file is posted. Once the content is detected, an automated algorithm blocks it and addresses the domain to demand its elimination (Suzor, 2014). However, this policy presents certain obstacles. Given that most of the websites in which 3D gun files are uploaded are illegal or anarchist, it is very unlikely that their administrators will be eager to fulfil the government´s request and eliminate their content. Moreover, as a high percentage of their controllers are experienced hackers, these individuals could counter the government´s blockade of the files and subsequently re-upload the content. Hence, this reaction capability will force international governments to constantly scrutinise these domains to erase the dangerous content.

Nevertheless, this former initiative will not only require a strong effort of surveillance, but also the development of solid codes of law that tackle these illegal operations (De Beer, 2009). However, passing new laws that discuss how to combat plastic weapons on the Internet is presenting some difficulties, especially in countries such as the United States, where the weapon lobby has a notable influential power and the Second Amendment questions the excessive banning of the right to bear arms (Tirone, 2016). Moreover, even if the legislative institutions reached consensus and introduced new laws that addressed this problem, given that criminals and terrorists do not respect legal regulations, these codes will not serve to entirely defeat illegal 3D gunsmiths (Butler, 2015).

Consequently, these previous combating policies along with the above-mentioned utilisation of 3D printing technologies in the industry of Defence or the Humanitarian Assistance sector, demonstrate that additive manufacturing has also positive applications that can contribute to struggle against those whom negatively attempt to profit from this technology and ultimately serve to Reinforce International Security.

9. CONCLUSIONS

This research work has sought to provide a vision of the positive and negative consequences that derive from the unstoppable inclusion of additive manufacturing technologies into present societies. Similar to other inventions, depending on its utilisation, 3D printing can either pervade International Security or serve as a valuable tool to reinforce it. This dissertation has proved that even though there are not black

and white scenarios, fostering the analysis of this innovative manufacturing process can help to pool its beneficial utilisation in multidisciplinary domains, ranging from industrial procedures to household activities. In this regard, this study has sought to call for reflection and raise awareness on both the new threats and opportunities that additive manufacturing offers.

Considering the first objective of the dissertation, the misapplications of 3D technology, two major threats have been analysed: the criminal use of additive manufacturing technologies and its utilisation by modern terrorists to supply themselves with plastic attacking firearms such as SALW. This second part of the study has showed that terrorists are eager to profit from new technologies as long as they leverage the impact of their actions. However, given the rapid advancement of this manufacturing process and the multiple applications that new printable materials would offer to these organisations and lone wolf combatants, 3D terrorism should become a core area of intervention for counter-terrorist agencies.

Furthermore, it is essential that local and supranational entities cooperate to impede the illicit use of additive manufacturing technologies, as the combat against 3D insecurity takes place in a global scenario. Thereby, these institutions should collaborate in different intelligence areas including R&D to better understand the utilisation possibilities that these machines offer, aiming to improve existing security mechanisms and to develop better counter-attack policies.

Moreover, it is necessary to enhance the legal codes that regulate 3D technologies, as plastic criminals and terrorists are profiting from the existence of legal vacuums to supply themselves whilst distributing printed weapons worldwide. Hence, this area of intervention is key not only to stop the proliferation of non-regulated weapons, but to impede the online circulation of the blueprints required to craft those firearms. Given the innovative nature of additive manufacturing, collaboration between International Law Institutions and national legislative bodies is imperative to establish codes that impede the illegal production of plastic weapons without hampering the growth potential of this technology in other sectors such as the Defence industry.

Therefore, to ensure the drawing of effective laws, all stakeholders affected by their content should be invited to a legislative debate prior to their definitive approval, including government representatives, industry manufacturers, civil society members and academic experts. These meetings will serve to leverage multidisciplinary proposals on how to supervise the use of this technology while considering possible countermeasures to deal with additive manufacturing delinquency.

Nonetheless, to make these legislative and intelligence efforts effective, it is also required that international institutions conduct awareness campaigns that present the opportunities that this technology offers, whilst warning about the red line that should not be crossed when crafting these plastic

goods. However, these informative policies should be carefully conducted to avoid confrontation with liberties such as freedom of speech, a potential clash that is already generating controversy in countries such as the United States, as studied in the lawsuit case of Defense Distributed.

Apart from examining the illegal applications of additive manufacturing technologies and the measures required to combat its misutilisation, this dissertation has had a second objective; showing how 3D printing is contributing to reinforce global security networks. This technology is enabling key sectors such as Health Care or the industry of Defence to profit from its rapid prototyping and customisation possibilities to better safeguard international welfare standards. In addition, 3D printing is creating partnerships between strategic disciplines such as cybersecurity and additive engineering, which can work towards the development of new applications aimed at improving the features of public and private services.

Therefore, considering all the dimensions tackled in this study and the expected advancements of 3D printing technologies in the upcoming years, it is evident that this manufacturing process demands to be further analysed and monitored to guarantee that it serves to reinforce International Security rather than to harm it. These prospective studies along with the development of robust regulating laws should support international governments to defeat 3D criminality and plastic terrorism, whilst utilising additive manufacturing technologies to build more solid security networks.

10. BIBLIOGRAPHY[22]

1. Ackerman, S. (2014). 41 men targeted but 1,147 people killed: US drone strikes – the facts on the ground. *The Guardian*. Retrieved from: https://www.theguardian.com/us-news/2014/nov/24/-sp-us-drone-strikes-kill-1147
2. Adelstein, J. (22 de september de 2015). A Yakuza War Is Brewing in Japan — And the Police Are Taking Sides. *Vice News*. Retrieved from: https://news.vice.com/article/a-yakuza-war-is-brewing-in-japan-and-the-police-are-taking-sides
3. Affairs, U. N. (2017). Official Documents of the 2017 Preparatory Conference for the Review of the Treaty of Nuclear Non-Proliferation. Vienna. Retrieved from: https://www.un.org/disarmament/wmd/nuclear/npt2020/prepcom2017/
4. American, C. (1791). *Second Amendment of the American Constitution.* Retrieved from: https://www.loc.gov/law/help/second-amendment.php
5. Archives, U. (2016). *At Security Council, Ban calls for eradicating weapons of mass destruction 'once and for all'.* New York: UN. Retrieved from: https://news.un.org/en/story/2016/08/537212-security-council-ban-calls-eradicating-weapons-mass-destruction-once-and-all
6. Badey J., T. (1998). Defining international terrorism: A pragmatic approach. *Journal on Terrorism and Political Violence*, 90-10
7. Bai, X., Liu, Y., Wang, G., & Wen, C. (2017). The pattern of technological accumulation: the comparative advantage and relative impact of 3D printing technology. *Journal of Manufacturing Technology Management*, *28*(1), 39-55.
8. Bartlett, S. (2013). Printing organs on demand. *The Lancet Respiratory Medicine*, *1*(9), 684.
9. Bates, R. (2016). Tracking Lone Wolf terrorists. *The Journal of Public and Professional Sociology*.
10. Beckstrand, T. (5 de January de 2018). *Guns and Ammunition Glosary*. Retrieved from: http://www.gunsandammo.com/rifles/ar-15/
11. Breene, K. (2016). *What is medjacking?* World Economic Forum.Retrieved from: https://www.weforum.org/agenda/2016/10/medjacking-health-cyber-risk-explainer/
12. Brown, E. (13 de september de 2016). *Who needs the Internet of Things. Linux News*. Retrieved from: https://www.linux.com/news/who-needs-internet-things
13. Butler, J. (2015). NSW Tightens 3D Printed Gun Legislation As Expert Warns They're Getting Cheaper, More Effective. *The Huffington Post*. Retrieved from: https://www.huffingtonpost.com.au/2015/11/20/3d-printed-gun-laws-nsw_n_8595818.html
14. Byman L., D. (15 de march de 2017). Can lone wolves be stopped? *Brookings Institution*. Retrieved from: https://www.brookings.edu/blog/markaz/2017/03/15/can-lone-wolves-be-stopped/
15. Campbell, T. (2015). Could 3D printing change the world? *Center for Security Studies*.Retrieved from: http://www.atlanticcouncil.org/publications/reports/could-3d-printing-change-the-world

[22] All URL´s in the references were most recently retrieved on the 11Th of April 2018.

16. Chuck, E. (2016). Company Invents Gun That Folds Up to Look Like a Cellphone. *NBC News*. Retrieved from: https://www.nbcnews.com/news/us-news/company-invents-gun-folds-look-cellphone-n547221

17. Coll, S. (2014). The drone war in Pakistan. *The New Yorker*. Retrieved from: https://www.newyorker.com/magazine/2014/11/24/unblinking-stare

18. Columbus, L. (2016). Roundup Of Internet Of Things Forecasts And Market Estimates, 2016. *Forbes*. Retrieved from: https://www.forbes.com/sites/louiscolumbus/2016/11/27/roundup-of-internet-of-things-forecasts-and-market-estimates-2016/#571b2a58292d

19. Conte, A. (2010). *Human Rights in the Prevention and Punishment of Terrorism .* New York: Springer Heidelberg .

20. Controls, U. D. (2018). *United States Regulations and Laws*. Retrieved from:https://www.pmddtc.state.gov/regulations_laws/itar.html

21. Crouse, M. (13 de August de 2015). 3D Printing Helps Modernize, Standardize NATO Jets. *PDD*. Retrieved from: https://www.pddnet.com/news/2015/08/3d-printing-helps-modernize-standardize-nato-jets

22. D. Simon, J. (1994). *The Terrorist Trap.* Bloomington: Indiana University Press

23. D´Aveni, R. (2015). The 3-D Printing Revolution. Harvard Business Review. Retrieved from: https://hbr.org/2015/05/the-3-d-printing-revolution

24. Daly, A. (2017). Don't Believe the Hype? Recent 3D Printing Developments for Law and Society.

25. De Beer, J., & Clemmer, C. D. (2009). Global trends in online copyright enforcement: a non-neutral role for network intermediaries?*Jurimetrics*, 375-409.

26. Del Castillo, M. (2018). *Cryptocoins keep Cody Wilson´s dream alive*. Retrieved from: https://www.coindesk.com/guns-crypto-bitcoin-helping-keep-cody-wilsons-anarchist-dream-alive/

27. Defensa, M. d. (2017). *Presupuestos Generales del Estado.* Madrid: BOE. Retrieved from: http://www.defensa.gob.es/Galerias/presupuestos/presupuesto-defensa-2017.pdf

28. Defense, O. (2008). *Military Equipment Useful Life Study.* Washington DC: Department of Defence. Retrieved from: https://www.acq.osd.mil/pepolicy/pdfs/OPTEMPO/OPTEMPO%20Phase%20II%20Final%20Report.pdf

29. Editorial. (2018).Printing Food: *3D printing*.Retrieved from: https://3dprinting.com/food/

30. Ensor, J. (2014). Japanese man becomes first person to be jailed for making gun with 3D printer. *The telegraph*. Retrieved from: https://www.telegraph.co.uk/technology/news/11187481/Japanese-man-becomes-first-person-to-be-jailed-for-making-gun-with-3D-printer.html

31. Evans, M. (2013). 3D printed gun discovered by police. *The Telegraph*. Retrieved from: https://www.telegraph.co.uk/news/uknews/crime/10403432/3D-printed-gun-discovered-by-police.html

32. Fey, M. (2017) 3D Printing and International Security: Risks and Challenges of an Emerging Technology. *Peace Research Institute.*

33. Flynt, J. (2018). A detailed history of 3d printing. *3D Insider*. Retrieve from: http://3dinsider.com/3d-printing-history/

34. Fordyce, R. (2015). Manufacturing imaginaries: Neo-Nazis, men's rights activists and 3D printing. *Journal of Peer Production*, *6*(1).

35. Fox-Brewster, T. (2017). Medical Devices Hit by Ransomware for the first time in US hospitals. *Forbes*. Retrieved from: https://www.forbes.com/sites/thomasbrewster/2017/05/17/wannacry-ransomware-hit-real-medical-devices/#674d6a81425c

36. Français, G. (2017). *Budget D´Etat Français.* Paris: Ministère d´Economie et de Finance

37. Gayle, D. (2017). NHS seeks to recover from global cyber-attack as security concerns resurface. *The Guardian*. Retrieved from: https://www.theguardian.com/society/2017/may/12/hospitals-across-england-hit-by-large-scale-cyber-attack

38. García, M. D. M. H. (2016). Las impresoras 3D: un desafío en la lucha de la proliferación de armas de destrucción masiva. *bie3: Boletín ieee*, (1), 277-283.

39. Geissbauer , R., Lehr, J., & Wunderlin, J. (2017). *A look at the challenges and opportunities of 3D printing.*

40. Goehrke, S. A. (2015). Uk Police note potential for 3D printing uses in Terrorist Activity. *3Dprint*.Retrieved from: https://3dprint.com/59830/uk-anti-terror-3d-printing/

41. Grant, G. (2010). The Limitations of China´s Defense Industry. *The Military*. Retrieved from: https://www.military.com/defensetech/2010/06/09/the-limitations-of-chinas-aerospace-industry

42. Greenberg, A. (2015). 3-D Printed Gun Lawsuit Starts the War Between Arms Control and Free Speech. *Wired*. Retrieved from: https://www.wired.com/2015/05/3-d-printed-gun-lawsuit-starts-war-arms-control-free-speech/

43. Greenberg, A. (2013). Gunsmiths 3D-Print High Capacity Ammo Clips To Thwart Proposed Gun Laws. *Forbes*. Retrieved from: https://www.forbes.com/sites/andygreenberg/2013/01/14/gunsmiths-3d-print-high-capacity-ammo-clips-to-thwart-proposed-gun-laws/&re

44. Halopeau, B. (2014). Terrorist use of the Internet. In *Cyber Crime and Cyber Terrorism Investigator's Handbook* (pp. 123-132).

45. Hatewatch, S. (2016). *Alleged killer of British MP was a longtime supporter of the neo-Nazi National Alliance.* South Poverty Law Center.Retrieved from: https://www.splcenter.org/hatewatch/2016/06/16/alleged-killer-british-mp-was-longtime-supporter-neo-nazi-national-alliance

46. Hern, A. (6 de may de 2013). A gun made on a 3D printer has been fired – let's look at this in perspective. *The Guardian*. Retrieved from: https://www.theguardian.com/commentisfree/2013/may/06/3d-printer-gun-has-been-fired

47. Hidalgo García, M. (2017). *3D printing: A challenge to battle against WMD proliferation.* Madrid: IEE.

48. Hopkins, S. (2014). Al-Qaeda publishes recipe for easy-to-make bomb that would evade airport check that 'any determined Muslim can prepare. *The daily mail UK*. Retrieved from: http://www.dailymail.co.uk/news/article-2905276/Al-Qaeda-publishes-recipe-easy-make-bomb-evade-airport-check-determined-Muslim-prepare.html

49. Hughes, O. (2017). You can now buy a handgun that looks like a smartphone and police are worried. *Business Insider*.Retrieved from: http://www.businessinsider.com/you-can-now-buy-a-gun-that-looks-like-a-smartphone-police-concerned-2017-1

50. Humphrey, T. (2017). Hacking drones, overview of the main threats.Retrieved from: http://resources.infosecinstitute.com/hacking-drones-overview-of-the-main-threats/#gref

51. International, N. (2017). *World Internet usage and population statistics* . Nielsen. Retrieved from: https://www.internetworldstats.com/stats.htm

52. Jacobs, J. B., & Haberman, A. (2017). 3D-printed firearms, do-it-yourself guns, & the Second Amendment. *Law & Contemp. Probs.*, *80*, 129.

53. Jackson, R. S. (2009).C*ritical terrorism studies: A new research agenda.* Routledge.

54. James, E., & James, L. (2016). *3D printing humanitarian supplies in the field.* Humanitarian Practice Network. Retrieved from: https://odihpn.org/magazine/3d-printing-humanitarian-supplies-in-the-field/

55. Kaplan, D. (2012). *Yakuza: Japan's criminal underworld.* California: University of California

56. Kahn, K. (2004). *The PDMA Handbook for new Product and Development.* John Willey and Sons.

57. Keiligh, B. (29 de august de 2015). Japan braces for a wave of gang violence after a split in its largest 'yakuza' crime syndicate . *The Daily Mail*.Retrieved from: http://www.dailymail.co.uk/news/article-3215031/Split-emerges-Japans-biggest-yakuza-gang.html

58. Kelly, J. (2015). Why is the UK still so reliant on the Tornado? *BBC News*. Retrieved from: http://www.bbc.com/news/magazine-33772093

59. Kleinman, A. (23 de may de 2013). 3D-Printed Bullets Exist, And They're Terrifyingly Easy To Make. *The Huffington Post*.Retrieved from: https://www.huffingtonpost.com/2013/05/23/3d-printed-bullets_n_3322370.html

60. Lai, E., Petch, M., & Armstrong, K. Manufacturing Imaginaries: Neo-Nazis, Men's Rights Activists and 3D Printing.

61. Lang, D. (30 de july de 2014). Cyber wrap. *The strategist*. Retrieved from: https://www.aspistrategist.org.au/cyber-wrap-173/

62. Larssen-Mowatt, R. (2010). Al-Qaeda´s pursuit of Weapons of Mass Destruction. *Foreign Policy*.Retrieved from: http://foreignpolicy.com/2010/01/25/al-qaedas-pursuit-of-weapons-of-mass-destruction/

63. Lewis, A. (2014). The legality of 3D printing: how technology is moving faster than the law. *Tul. J. Tech. & Intell. Prop.*, *17*, 303.

64. Louis, M., Seymour, T., & Joyce, J. (2016). *3D opportunity in the Department of Defense: Additive Manufacturing lines up.* New York: Deloitte University Press. Retrieved from: https://www2.deloitte.com/content/dam/insights/us/articles/additive-manufacturing-defense-3d-printing/DUP_1064-3D-Opportunity-DoD_MASTER1.pdf

65. Lubrano, M. (2018). *Emerging technologies: when terrorists print their own weapons.* Global Risk Insights.Retrieved from: https://globalriskinsights.com/2018/01/terrorism-additive-manufacturing-weapons/

66. Maccar, D. (2016). No, this folding gun is not made by terrorists to fool police . *Range365*.

67. Macik, T. (2015). Global data meets 3-D printing: the quest for a balanced and globally collaborative solution to prevent patent infringement in the foreseeable 3-D printing revolution. *Indiana Journal of Global Legal Studies*, *22*(1), 149-173.

68. Mackey, T. K., & Liang, B. A. (2011). The global counterfeit drug trade: patient safety and public health risks. *Journal of pharmaceutical sciences*, *100*(11), 4571-4579.

69. Manyika, J., Chui, M., Bughin, J., Dobbs, R., Bisson, P., & Marrs, A. (2013). *Disruptive technologies: Advances that will transform life, business, and the global economy* (Vol. 180). San Francisco, CA: McKinsey Global Institute.

70. Martyn, A. (2002). *The Right of Self-Defence under International Law-the Response to the Terrorist Attacks of 11 September.* Sydney: Parlament of Australia.

71. Matusitz, J. (2013). *Terrorism & Communication: A critical introduction.* Florida: Sage Publications.

72. McVeigh, K. (2013). Drone strikes, tears in Congress. *The Guardian*. Retrieved from: https://www.theguardian.com/world/2013/oct/29/pakistan-family-drone-victim-testimony-congress

73. Mezzofiore, G. (2016). How the killer of British politician Jo Cox could have obtained his gun. *Mashable.* Retrieved from: https://mashable.com/2016/06/18/thomas-mair-guns-uk-jo-cox-murder-antique/

74. Newman, L. H. (3 de february de 2017). Medical Devices are the next security nightmare. *The Wire*. Retrieved from: https://www.wired.com/2017/03/medical-devices-next-security-nightmare/

75. Nieuwenhuizen-TNO, M. (2014). Chemical weapons detection, protection & destruction.

76. Ning, H., Liu, H., & Yang, L. T. (2013). Cyberentity security in the internet of things. *Computer*, *46*(4), 46-53.

77. Obado Ochieng, M. (2017). The elusive legal definition of terrorism at the United Nations: An inhibition to the criminal justice paradigm at the state level. *Heinonline*, 1-3.

78. Ohno, T. (1988). *Toyota Production syste: Beyond Large-Scale Production.* Tokyo: CRC Press.

79. Okumura, T. (1996). Report on 640 victims on the Tokyo subway sarin attack. *Annals of emergency medicine*, 129-135.

80. O'Malley, J. (2017). Pirates of the skies [drone-jacking]. *Engineering & Technology*, *12*(3), 32-35.

81. O'Neill, K. (2012). Is Technology Outmoding Traditional Firearms Regulation? 3-D Printing, State Security, and the Need for Regulatory Foresight in Gun Policy.

82. OSCE. (2014). *2014 OSCE Mediterranean Conference Illicit Trafficking in Small Arms and Light Weapons and Fight against Terrorism in the Mediterranean Region.* Neum.

83. Pantucci, R. (2015). *We love death as you love life: British Suburban Terrorists.* London: Hurst Publishers.

84. Pallottino, F., Hakola, L., Costa, C., Antonucci, F., Figorilli, S., Seisto, A., & Menesatti, P. (2016). Printing on food or food printing: a review. *Food and Bioprocess Technology*, *9*(5), 725-733.

85. Parsons, M., McGuire, T., Hirsch, M., Leake, S., Straub, J., & Kerlin, S. (2016). National Defense 3D Space Printing.

86. Pearson, A. (2018). *Disadvantages of 3D Printing Technology. 3DInsider*. Retrieved from: http://3dinsider.com/3d-printing-disadvantages/

87. Plafke, J. (2017). *The World´s first 3D printed metal gun is a beautiful pistol.Extreme Tech*. Retrieved from: https://www.extremetech.com/extreme/170574-the-worlds-first-3d-printed-metal-gun-is-a-beautiful-45-caliber-m1911-pistol

88. Physics, R. (2018). *About Radio Physics*. Retrieved from http://www.radiophysicssolutions.com/company

89. Prestigiacomo, A. (2017). How This 'Crypto-Anarchist' Could Completely Destroy Gun Control. *The Dailywire*. Retrieved from: https://www.dailywire.com/news/22283/diy-untraceable-handguns-crypto-anarchist-cody-amanda-prestigiacomo

90. R. White, J. (2013). The Nature of Modern Terrorism. *The Huffington Post*. Retrieved from: https://www.huffingtonpost.com/jonathan-r-white/confusion-about-boston_b_3128995.html

91. Ranstorp, M., & Normark, M. (2015). *Understanding terrorism Innovation and Learning: Al Qaeda and beyonf.* Routledge.

92. Rapoport, D. (2002). The Four Waves of Rebel Terror and September 11. *Antropoetics: The Journal of Generative Anthropology*, 1-3.

93. Roberts, D. (2013). 3D-printed guns prompt US House to renew prohibition on plastic firearms. *The Guardian*.Retrieved from: https://www.theguardian.com/world/2013/dec/04/3d-guns-house-renew-prohibition-plastic-firearms

94. Rodday, N. (2016). *Hacking Drones, overview of the main threats.* Twente, The Netherlands: University of Twente.

95. Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of security and privacy in distributed internet of things. *Computer Networks*, *57*(10)

96. Ross, F. J. (2015). 3D printing with moondust. *Rapid Prototyping Journal*. Retrieved from: https://www.emeraldinsight.com/doi/abs/10.1108/RPJ-02-2015-0022

97. Satniford, A. (2017). Cyber drone-jacking: Emerging threats to Unmanned Aerial Vehicles. *Trends*. Retrieved from: http://trendsinstitution.org/cyber-drone-jacking-emerging-threats-to-unmanned-aerial-vehicles/

98. Saunders, S. (2016). 3D Printed Dog Nose is Helping to Enhance Electronic Scent-Detection Devices. *3D printing magazine*. Retrieved from: https://3dprint.com/157560/3d-printed-dog-nose/

99. Savage, S. (2005). London bombers used everyday materials. *Reuters*.Retrieved from: http://www.redorbit.com/news/general/197067/london_bombers_used_everyday_materialsus_police/

100. Schilling, W. R., Hammond, P. Y., & Snyder, G. H. (1962). *Strategy, politics, and defense budgets*. Columbia University Press.

101. Schneider, T., Apel, E., Brost, P. (2014). 3D Printing: Perceptions, Risks, and Opportunities.

102. Schubert, C., Van Langeveld, M. C., & Donoso, L. A. (2014). Innovations in 3D printing: a 3D overview from optics to organs. *British Journal of Ophthalmology*, *98*(2), 159-161.

103. Shields, B. (2017). Air Traffic Control: How Mexican Cartels are Utilizing Drones to Traffic Narcotics into the United States. *Penn St. JL & Int'l Aff.*, *5*, 207.

104. Schinkel, W. (2011). Prepression: The actuarial archive and new technologies of security. *Theoretical Criminology*, *15*(4), 365-380.

105. Schwab, P. (2017). *The Fourth Industrial Revolution.* New York: Crown Publishing Group.

106. Staff, T. (2016). Hezbollah: we hacked into iraeli security cameras. *Times of Israel* . Retrieved from: https://www.timesofisrael.com/hezbollah-we-hacked-into-israeli-security-cameras/

107. Strohm, C. (2017). Lone-Wolf terrorism. *Bloomberg*. Retrieved from: https://www.bloomberg.com/quicktake/lone-wolf-terrorism

108. Suzor, N. (2014). Forced negotiations and industry codes won't stop illegal downloads. *The Conversation*. Retrieved from: https://phys.org/news/2014-12-industry-codes-wont-illegal-downloads.html

109. Swanner, J. (2017). *3D Printing as an Emerging Homeland Security Risk.* HDIAC.

110. Swanson, S. (2013). 3D Printing: A Lesson in History: How to Mold the World of Copyright. *Sw. L. Rev.*, *43*, 483.

111. Tirone, D. (2016). 3-D Printing: New Threat to Gun Control and Security Policy? *US News*. Retrieved from Tirone, D. (2016). 3-D Printing: New Threat to Gun Control and Security Policy? *US News*.

112. Tironr, A. (19 de july de 2016). 3D printing, a new threat to gun control and security policy? *The Conversation*.Retrieved from: https://theconversation.com/3d-printing-a-new-threat-to-gun-control-and-security-policy-61416

113. Trimble, M. (2017). *U.S. State Copyright Laws: Challenge and Potential.* California: Stanford Technology Law.

114. Vak, D., Hwang, K., Faulks, A., Jung, Y. S., Clark, N., Kim, D. Y., ... & Watkins, S. E. (2015). 3D Printer Based Slot-Die Coater as a Lab-to-Fab Translation Tool for Solution-Processed Solar Cells. *Advanced Energy Materials*.

115. Villarejo, E. (2017). España paga a General Atomics los primeros 53,6 millones para recibir el drone Reaper. *ABC*. Retrieved from: http://abcblogs.abc.es/tierra-mar-aire/public/post/reaper-general-atomics-20707.asp/

116. Waterfield, B. (11 de january de 2017). Police on alert for handgun that looks like an iPhone. *The Times*.Retrieved from: https://www.thetimes.co.uk/article/police-on-alert-for-handgun-that-looks-like-an-iphone-bhw2v2rm3

117. Weber, R. H. (2010). Internet of Things–New security and privacy challenges. *Computer law & security review*, *26*(1), 23-30.

118. Wen Wei, C., & Thong Seah Ser, C. (2017). *3D Printing – Revolutionising Military Operations.* Singapore: Journal of the Singapore Armed Forces. Retrieved from: https://www.mindef.gov.sg/oms/safti/pointer/documents/pdf/Vol42No2_4%203D%20Printing.pdf

119. Winter, J. (23 de may de 2013). Homeland Security bulletin warns 3D-printed guns may be 'impossible' to stop. *Fox News*. Retrieved from: http://www.foxnews.com/us/2013/05/23/govt-memo-warns-3d-printed-guns-may-be-impossible-to-stop.html

120. Wittman, G. H. (2017). DO-it-yourself terrorism. *The Washington Times*. Retrieved from: https://www.washingtontimes.com/news/2017/nov/24/do-it-yourself-terrorism/

121. Wolinsky, H. (2014). Printing organs cell-by-cell: 3-D printing is growing in popularity, but how should we regulate the application of this new technology to health care? *EMBO reports*.

122. Yvon, A. (2016). *Disruptive Technologies Barometer - Tech Report.* KPMG. Retrieved from: https://home.kpmg.com/ca/en/home/insights/2016/12/disruptive-technologies-barometer-tech-report.html

123. Zhao, K., & Ge, L. (2013). A survey on the internet of things security. In *Computational Intelligence and Security (CIS), 2013 9th International Conference on* (pp. 663-667). IEEE.

124. Zhou, L., & Chao, H. C. (2011). Multimedia traffic security architecture for the internet of things. *IEEE Network*.