ieee.es
Instituto Español de Estudios Estratégicos

Analysis
Document

17/2016 March 15, 2017

María del Mar Hidalgo García

3D printing: A challenge to the battle against WMD proliferation

This document has been translated by a Translation and Interpreting Degree student doing work experience, LAURA REVUELTA GUERRERO, under the auspices of the Collaboration Agreement between the Universidad Pontificia Comillas, Madrid, and the Spanish Institute of Strategic Studies.

3D printing: A challenge to the battle against WMD proliferation

Abstract:

The malicious use of technological developments by non-state actors is one of the major challenges for the international community. The rapid development of information technologies and the possibility of "making real" that information through the use of 3D printers has created a new risk scenario both for the proliferation of weapons of mass destruction and the illicit trafficking in conventional arms.

Keywords:

3D printing, proliferation, technological developments, WMD.

Technological advances and globalisation: challenges and opportunities

Today's asymmetrical conflicts and hybrid warfare have shown evidence that a State's technological superiority does not guarantee a successful operation. Similarly, technological and innovative monopolies have failed to achieve the non-proliferation of weapons of mass destruction in a globalised, interconnected world where everything is available, in more or less difficult conditions.

Globalisation and global interconnectedness through the internet are usually linked to progress, easy access to information, and even a greater ability to build social relations. Citizens can easily acquire certain products which are not available commercially or that are subject to greater regulation in their countries.

Such an easy access to information and products is convincing society of the fact that everything is possible and available. Anonymity in the Deep Web makes it easy to imagine that there are actual handbooks available on how to create chemical and biological weapons or dirty bombs for non-experts. The confusion between information and knowledge is boosting the Do It Yourself phenomenon (DIY). Easy access to information without prestigious scientific journals —usually subject to membership— being necessary reinforces the idea that extensive scientific knowledge and installations with the minimum security measures required are no longer necessary to manufacture chemical or biological weapons.

Traditionally, these weapons have been encompassed within the category of weapons of mass destruction (WMD), together with nuclear and radiological weapons. But this term might become outdated in the 21st century for two reasons. Firstly, the kind of weapons mentioned before can be used by non-State actors to cause destabilisation and chaos instead of "massive destruction" or a high number of casualties. In the second place, there is another kind of weapons that could we developed; these are more sophisticated weapons capable of provoking destruction similar to that caused by nuclear bombs. For instance, the high-power microwave weapon (HPM) and other directed-energy weapons (DEW), hypersonic kinetic energy weapons, high-explosive incendiary materials, or even geophysical manipulation[1] fall under this category.

Some experts even speak of Weapons of Mass Effects to indicate that the greatest challenges will originate from the enemy's capability to cause a massive damage or disruption instead of a high number of casualties.[2] A cyber-attack is a clear example

[1] Caves, J. and Seth, W. "*The future of weapons of Mass Destruction: Their Nature and Role in 2030. Occasional Paper 10. National Defense University Press. Washington, D. C. June 2014.*
[2] Bowman H. Miller Ph.D. "*From WMD to WME: An Ever-Expanding Threat Spectrum".* Journal of Strategic Security, Vol. 8. Nº3, Fall 2015.

of this new concept of "massive damage". The 2013 Spanish National Security Strategy has included this risk: "*Cyberspace is today's clearest example of an area easily accessible, largely unregulated, and difficult to control. And so, along these lines, cyber security is one of the main fields of action in this Strategy*.[3]"

Amid the uncertainty surrounding the outlook, technological advancements pose a challenge to the States and global governance. Any technology currently under development can be used in a different way to the use for which it was conceived, and so this malicious use poses a major risk. Among the new dual-use technologies that could pose a major risk, biotechnology, information technology, the development of new energy sources, and nanotechnology are the most significant ones.[4]

Concerning biotechnology, and this includes genome editing, its progress represents one of the greatest and most promising steps forwards for mankind, as it opens the door to creating organs, curing illnesses, and reinforcing the immune system. However, it raises ethical issues due to its impact on the evolution of human existence and, more importantly, it also entails the risk of creating new illnesses in humans, animals, and plants.

Biotechnological development can be employed in an almost infinite number of ways, both positive and negative, and consequently it has been included in the main security strategies. For the first time, the World Threat Assessment of the US Intelligence Community, which was published in February 2016[5], defined genome editing as a threat, since there exists the possibility that non-Western countries with different regulatory and ethical standards might develop harmful biological agents.[6]

The role of 3D printing in WMD proliferation

The rapid development of information technologies and the possibility of making real this information through the use of 3D printers have created a new risk scenario, both for the proliferation of weapons of mass destruction and the illicit trafficking in conventional arms. This has challenged the validity of international agreements on trade control and dual-use material and weapons exports.

[3] http://www.lamoncloa.gob.es/documents/seguridad_1406connavegacionfinalaccesiblebpdf.pdf
[4] Waller F. *Emerging Weapon of Mass Destruction Technologies: Impact on US Security.* FUTURE TAKES. Vol. 3, nº4, Winter 2004-2005.
[5] http://www.dni.gov/files/documents/SASC_Unclassified_2016_ATA_SFR_FINAL.pdf
[6] http://www.dni.gov/files/documents/SASC_Unclassified_2016_ATA_SFR_FINAL.pdf

Dual-use exports control agreements create lists of material subject to strict regulation with an impact on both the exporter and the importer. Part of this regulation obliges the parties to detail every piece of information regarding the final use of the product, thus diminishing the risk of a deviation for illicit purposes. Some examples are the Australia Group[7], the Missile Technology Control Regime (MTCR)[8], and the Nuclear Suppliers Group (NSG).[9] However, the difficulty of controlling the intangible transfer of technology (ITT) [10] can jeopardise the effectiveness of these exports control regimes.

As mentioned before, sensitive information, with varying degrees of difficulty, can be available to an organisation with criminal purposes. If, on top of this, we add the possibility of materialising this information into something physical, we find ourselves facing a major challenge from a security point of view. For instance, regarding nuclear proliferation, fissile material cannot be manufactured through a 3D printer, but in the future, and as metal 3D printing is developed[11], centrifuges or missile warheads could begin to be manufactured.

With regard to chemical weapons proliferation, 3D printers also offer the possibility at its nascent stage of combining different reagents to create a chemical product. This development is being carried out mainly in the pharmaceutical industry, as it allows drugs manufacturing on the spot. This option has the advantage of offering a wider geographical availability at a lower cost, thus facilitating their supply to developing countries. However, it also opens the door to the synthesis of compounds capable of being used as chemical weapons in return.[12]

In the field of biology, the 3D bioprinters offer endless possibilities. Much has been accomplished already in the printing of tissues such as human skin, parts of the intestines, bones, and heart, auguring well for the future of organ transplantation and the curing of diseases.[13] Moreover, there exists the possibility of creating cheapest and more accessible vaccines, which is a major step forward for developing countries looking to stop disease outbreaks.

The benefits are undeniable and yet the same process can be employed maliciously,

[7] http://www.australiagroup.net/en/controllists.html
[8] http://www.mtcr.info/english/trade.html
[9] http://www.nuclearsuppliersgroup.org/es/
[10] Intangible Technology Transfer
[11] Galamas F. 3D Printing_ WMD Proliferation an Terrorism Risks. Available at http://www.academia.edu/11289295/3D_Printing_WMD_Proliferation_and_Terrorism_Risks
[12] http://www.ibtimes.com/3d-printing-risks-not-just-plastic-guns-military-parts-drugs-chemical-weapons-1275591
[13] http://www.dtic.mil/dtic/tr/fulltext/u2/a577162.pdf

since synthetic biology opens the door to the creation of new pathogens or the modification of the existing ones in order to make them more resistant to medicines.[14]

Bioprinter
Source: http://envisiontec.com/3d-printers/3d-bioplotter/

The current price of bioprinters (about 200,000 dollars[15]) constitutes a barrier to immediate accessibility to this technology, as it is well above the price of conventional 3D printers. But this is just a temporary barrier which will break down as technology is further developed and prices start falling. Meanwhile, the Do It Yourself phenomenon (DIY) is also spreading out across the bioprinters field. In this regard, it is worth mentioning a group of *biohackers* part of an organisation called "BioCurious"[16], which is composed of scientists and defined by them as the first world's "hacker space" in the field of biology. Their philosophy is based on the assumption that biological developments should be available for everyone. One of the most relevant successes achieved by this group is the transformation of an HP 5150 inkjet printer into a bioprinter capable of creating live cells.[17]

[14] Cique A. Documento Marco: Retos y desafío de la biología sintética. IEEE 2015. Available at http://www.dtic.mil/dtic/tr/fulltext/u2/a577162.pdf
[15] http://3dprintingindustry.com/2015/08/26/top-10-bioprinters/
[16] Further information at http://biocurious.org/
[17] http://www.instructables.com/id/DIY-BioPrinter/

Conclusions

In contrast to the positive impact of globalisation, global interconnectedness, and technological advances are the new risks derived from the accessibility to information. Through 3D printing, WMD proliferation is harder to control because the problem transcends the physical access to the materials and is transferred to the field of the information that produces them, taking a qualitative and quantitative leap towards a new dimension such as the ITT, which is extremely hard to control. The dual-use exports control must adapt to reflect the technological developments on information technologies that are currently taking place.

Research centres in the 21st century are becoming a key element for security, given the fact that any transfer of sensitive information towards the outside can endanger international security. In order to avoid a voluntary or involuntary malicious use of the technological and scientific breakthroughs, it will be necessary to promote a security culture among the scientific community.

Technology and information related to WMD proliferation are currently more accessible to non-State actors. These agents can acquire the capability to manufacture, even in a rudimentary way, chemical, biological, radiological, or even nuclear weapons, with no need for major infrastructure. This accessibility to information boosts the emergence of the DIY phenomenon in the field of biology and chemistry. Paradoxically, many of them actually follow a selfless logic with the purpose of breaking down barriers in the scientific field and achieving universal access to technology. However, lack of experience and suitable facilities together with poor security measures can turn into a serious threat to international and national security, especially in the biotechnology field.

Threats are becoming less predictable in the 21st century, but even more dangerous is the fact that the international legal framework which has been supporting the international security architecture in regard to non-proliferation might no longer be useful to face the new risks derived from the ITT. For that, the battle against WMD proliferation must advance co-ordinately with the mechanisms they design to control cyber threats.

Mª del Mar Hidalgo García
IEEE Analyst