Groningen Journal of International Law, vol 6(1): Terrorism and International Law

Closing the 'Intangible Technology Transfer' Gap within the Existing Legal Frameworks: Time for an Additional Protocol(s)?

Katja LH Samuel[*]
Cassius Guimarães Chai[**]

DOI: 10.21827/5b51d53eb39b2

Keywords
INTERNATIONAL LAW; TERRORISM; ORGANISED CRIME; INTANGIBLE TECHNOLOGY TRANSFER; DUAL USE TECHNOLOGY; 3D PRINTING

Abstract

The current terrorism landscape poses increasing, diverse levels of threat, with accompanying complex and challenging counter-terrorism responses, as terrorist groups (TGs) become more global in their reach, creative in their methods, as well as more connected to organized criminal groups (OCGs). One concerning trend, in at least some geographical regions, is increased cooperation between OCGs and TGs or even convergence whereby the level of integration between the two groups is such that it is difficult to discern the parameters between them. Such cooperation or convergence can put existing applicable legal frameworks under strain, highlighting or even creating normative gaps in the process. In turn, these may hinder effective international cooperation, including in the domains of legal terrorism prevention and criminal justice responses to organized criminal and terrorist activities, thereby posing significant threats to international peace and security.

The related risks, together with the accompanying challenges and complexities for the international community to effectively counter such threats, are increasing exponentially via rapid technological advances, notably "emerging technologies". These are aggravated by the fact that applicable legal instruments (international, regional and national) have generally not managed to keep pace with such technological advances and associated risks. One such area relates to intangible technology transfer (ITT) by OCGs and TGs, which incorporates manufacturing techniques, technical know-how and intellectual property, and can take a number of forms such as the electronic transfer of weapons blueprints.

A particular issue, considered in this article, relates to the potential for OCGs/TGs to acquire "dual use" technology (i.e., technology with the potential to be used for both

[*] Director, Global Security and Disaster Management Limited (GSDM) (director@gsdm.global). The authors are very grateful for the undertaking of an excellent literature review of a number of issues explored in this article, with some accompanying suggestions, by Dr Jed Odermatt, University of Copenhagen and GSDM associate. This article is based on a paper given at a conference organised by the United Nations Office on Drugs and Crime and Qatar University, 'International Academic Conference: Exploring and Countering the Linkages between Organized Crime and Terrorism', Qatar 25–26 April 2018. The authors were most grateful for the opportunity to participate in this timely conference as well as for the feedback received on the draft paper. Informative comments were also received from Dr Elizabeth Chadwick (Nottingham Trent University) and Dr Bahram Ghiassee (University of Surrey), both GSDM associates. Any errors remain the sole responsibility of the authors.

[**] Ministério Público do Estado do Maranhão, state prosecutor in organized crime; Universidade Federal do Maranhão CCSo/Direito/PPGDIR, Brazil (cassiuschai@hotmail.com).

legitimate civil/military as well as illicit criminal purposes), for instance 3D printers, together with the software and/or blueprints necessary (e.g., obtained through cybercrime) to print weapons. In terms of the risks posed by ITT, though it is not possible to 3D print fissile, chemical, explosive etc materials, nonetheless the defence and security sector is reporting the rapid development of technology towards the 3D printing of the component parts of missiles, for instance, by military troops who are operationally deployed. Clearly, if such technology were to fall into the hands of OCGs/TGs, catastrophic consequences could ensue.

Somewhat surprisingly, despite the associated, foreseeable peace and security risks, such issues have attracted only modest research or even political attention to date from a legal perspective, resulting in significant knowledge gaps in relation to the development of policy, law and practice governing emerging technologies related challenges. More worrying are the gaps which appear to be present within existing criminal justice and anti-terrorism instruments governing OCG and TG activities. As this article reveals, minimal, if any, criminalization of ITT related activities exist. Instead, two primary gaps appear to exist: first, existing treaties do not generally criminalize the transfer of intangible technology as an asset for criminal purposes, whether for financial gain or to perpetrate terrorist acts; second, the existing frameworks do not criminalize the utilization of technology for the transfer of intangible technology assets by OCGs or TGs.

The article concludes with a number of recommendations as to how some of the identified weaknesses might be addressed.

Introduction

The current terrorism landscape poses increasing and diverse levels of threat, with accompanying complex and challenging counter-terrorism responses, as terrorist groups (TGs) become more global in their reach, creative in their methods, as well as more connected to organized criminal groups (OCGs). One concerning trend, which appears to be growing in at least some geographical regions, is increased cooperation between OCGs and TGs (such as the 'outsourcing' of certain criminal services, e.g., hostage-taking or the provision/movement of firearms, on a 'pay as you go' basis) or even convergence whereby the level of integration between the two groups is such that it is difficult to discern the parameters between them. Indeed, in some instances TGs may immerse themselves in traditionally OCG activities in order to fund their terrorist objectives and activities.[1]

That said, it is equally acknowledged that the exact nature and parameters of increased cooperation or convergence remain unsettled and contentious, with some commentators disputing the existence of these trends at all due to such factors as, for example, differing ideologies and goals, or the fact that association of an OCG with a TG

[1] On such themes see further, for example, West Sands Advisory LLP, "Europe's Crime Terror Nexus: Links Between Terrorist and Organized Crime Groups in the European Union" (2012), Directorate General for Internal Policies, Policy Department C: Citizens' Rights and Constitutional Affairs (2012), *at* <europarl.europa.eu/RegData/etudes/etudes/join/2012/462503/IPOL–LIBE_ET(2012)462503_EN.pdf> (accessed 4 April 2018); Kessels, E, and Hennessy, O, "Examining the Nexus between Terrorism and Organized Crime: Linkages, Enablers and Policy Implications" in H Glaser (ed), *Talking to the Enemy: Deradicalization and Disengagement of Terrorists* (Nomos 2017); T Makarenko, 'The Crime–Terror Continuum: Tracing the Interplay between Transnational Organised Crime and Terrorism' 6 *Global Crime* (2004) 129–145, *at* <iracm.com/wp–content/uploads/2013/01/makarenko–global–crime–5399.pdf> (accessed 4 April 2018); United Nations Security Council (UNSC) Res 2368 (2017) Preamble.

may make it more exposed and vulnerable to counter-terrorism and criminal justice efforts. It can also be difficult to access reliable research data; typically, only limited, anecdotal evidence is available due to the clandestine nature of OCG and TG criminal activities.[2] What is equally true, though, is that the line between the criminal activities and goals of OCGs and TGs can be a thin one.[3]

When cooperation or convergence does occur, be it between OCGs or TGs and/or their traditional domains of criminal activities, it can put the existing applicable legal frameworks under more strain, highlighting or even creating normative gaps in the process. In turn, these may hinder effective international cooperation, including in the domains of legal terrorism prevention and criminal justice responses to both organized criminal and terrorist activities. Any such constraint can be especially worrisome when the criminal activities engaged in pose significant threats to international peace and security, such as attempts by non-State actor groups to acquire weapons of mass destruction (WMDs).[4] Access to more conventional weapons and explosives remain a primary source of concern too as the normal 'modus operandi' of TGs.

The related risks, together with the accompanying challenges and complexities for the international community to effectively counter such threats, are increasing exponentially via rapid technological advances. These are aggravated by the fact that the relevant legal instruments (international, regional and national) have generally not managed to keep pace with such technological advances and accompanying risks, which is the primary focus here. Specifically, this article focuses on related issues regarding intangible technology transfer (ITT) by OCGs and TGs, which incorporates manufacturing techniques, technical know-how and intellectual property. ITT can take different forms, such as the oral transfer of technical know-how between persons, or the transfer of technology - e.g., blueprints for conventional or non-conventional weapon systems (including WMDs) - through intangible means (e.g., through emails, social media, software uploads or document downloads). Somewhat surprisingly, considering the threats to international peace and security posed by the risk of OCGs and TGs being engaged in ITT for illicit or terrorist purposes, which are likely to increase exponentially rather than diminish, such issues have attracted only modest research, scholarship or even political attention to date.[5] Of particular note here, the research

---

2 See, e.g., Howard RD and Traughber C, "The Nexus of Extremism and Trafficking: Scourge of the World or So Much Hype?" *Joint Special Operations University Report* 13–6 (October 2013), Introduction, *at* <socom.mil/JSOU/JSOUPublications/13–6_Howard_Nexus_FINAL.pdf> (accessed 4 April 2018). For diverse OCG/TG case studies, see Rollins J, Wyler LS and Rosen S, 'International Terrorism and Transnational Crime: Security Threats, U.S. Policy, and Considerations for Congress' (Congressional Research Service, 5 January 2010) including at 13, *at* <fas.org/sgp/crs/terror/R41004–2010.pdf> (accessed 4 April 2018).

3 See, e.g., Fatić A, *Osnovni aspekti borbe protiv organizovanog kriminala na Balkanu* (tr *The Basic Aspects of Combating Organized Crime in the Balkans*), LVII (2005) at 82, cited in Prokić, A, "The Link between Organized Crime and Terrorism" 15 *Law and Politics* (2017) 85, 88.

4 See, e.g., UNSC Res 2370 (2017).

5 See further on this, e.g., National Consortium for the Study of Terrorism and Responses to Terrorism, "Motivations, Mechanisms and Determinants of Terrorist Technology Transfer", *Research Brief* (October 2017), *at* <start.umd.edu/pubs/START_MotivationsMechanismsDeterminantsOfTechnologyTransfer_ ResearchBrief_Oct2017.pdf> (accessed 4 April 2018), which has begun some pilot research in this regard.

that has been undertaken has tended to be technical rather than legal in focus.[6] As such, major gaps are present within existing legal scholarship on ITT related issues, including from national/international criminal justice and security perspectives regarding the criminal activities of OCGs and TGs. This article seeks to make a modest contribution towards closing this research lacuna whilst also urging the international community to put these pressing issues more squarely onto its serious crime prevention as well as peace and security agendas.

To this end, the article is framed around three central research questions: (1) what relevant gaps exist within the current international criminal justice frameworks governing organized crime and terrorism?; (2) what are some of the implications of these gaps on international cooperation, focussing especially on the prevention and prosecution of involved non-State actors?; and (3) what steps might be taken to address such gaps? In terms of its methodology, the article starts from the premise that on the evidence available there are in fact such gaps, and analyses existing international organized crime and anti-terrorism conventions, together with other relevant instruments (especially those of the United Nations (UN) Security Council (UNSC)), within the context of weapons proliferation and ITT advances, to substantiate that conclusion. In terms of structure, the article commences with a discussion of what threats to international peace and security may ensue from current technological advancements, specifically regarding ITT and weapons proliferation, together with existing responses by the international community to these threats. It then examines each of the three posed research questions in turn, leading to some proposals regarding possible future steps to address identified weaknesses within the current applicable international legal architecture.

I. Framing the Problem

A. Potential threats to international peace and security posed by emerging technology, especially ITT

One significant issue of growing concern to international peace and security – including regarding the proliferation of conventional or non-conventional weapons by OCGs/TGs – relates to 'emerging technologies'. These are 'science-based innovations [… which] can arise as an entirely new technology or have a more incremental character, resulting from an existing technology or the convergence of several existing technologies'.[7] In the context of WMDs, for instance, not only do such technologies have the potential to facilitate the development of new pathways, as well as to augment existing ones, but they may 'lead to a meaningful paradigm shift in how policymakers define WMD, view the threat of WMD, and counter WMD in the future'.[8]

One specific area of 'emerging technology' risk that is attracting increasing attention in relation to OCG/TG cooperation or convergence concerns 'dual-use' technologies which may be used for alternative deadly criminal (for example, terrorist) purposes in addition to

---

6 See, e.g., EEF and AIG (in partnership with RUSI), 'Cyber Security for Manufacturers' *Report* (2018), *at* <eef.org.uk/resources–and–knowledge/research–and–intelligence/industry–reports/cyber–security–for–manufacturers> (accessed 30 April 2018).

7 Bajema, NE, and DiEulis, D, "Peril and Promise: Emerging Technologies and WMD: Emergence and Convergence Workshop Report, 13–14 October 2016" (National Defense University Press, May 2017) 1, *at* <wmdcenter.ndu.edu/Portals/97/Documents/Publications/Articles/2016%20Workshop%20Report%20FINAL%205–12–17.pdf?ver=2017–05–12–105811–853> (accessed 4 April 2018).

8 Bajema and DiEulis (n 9).

the legitimate (civilian/military) applications for which they were originally developed. Certainly, some OCGs/TGs, including the so-called Islamic State of Iraq and the Levant (ISIL), are already engaged in manufacturing smaller arms, a process which could broaden in scope if emerging technology were to become available to them.[9] Those dual-use technologies currently considered to pose the greatest risk in this respect comprise 'biotechnology, information technology, the development of new energy sources, and nanotechnology'.[10] The related threats are illustrated here by information technology, namely the dual-use of 3D printers. In terms of the key components of this 'additive manufacturing' process, they are 'the manufacturing device or printer, the materials, and the digital blueprint'.[11] One way in which it has been suggested that security concerns may arise is in the following manner:

> In theory, 3D printing will allow state and non-state actors to circumvent the need for engineers and scientists with tacit knowledge. Digital blueprints, designed and tested by scientists and engineers, would embed a certain level of technical expertise in electronic form. This 'embedded expertise' would allow people without traditional manufacturing skills to produce parts or objects by simply loading up a 3D printer with the required raw materials and then pressing the print button. Of course, these blueprints do not include post print finishing or assembly, but a digital build file could come with instructions for finishing and assembly.[12]

It has been further suggested that: '[t]he 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[13] and the illicit trafficking in conventional arms.'[14] From a security perspective, though, for instance, 'fissile material cannot be manufactured through a 3D printer, [...] in the future, and as metal 3D printing is developed, centrifuges or missile warheads could begin to be manufactured'.[15] Nor is this possibility fanciful since, for instance, the US defence community is developing the capability to 3D-print non-nuclear components, potentially in the field, to support its nuclear arsenal.[16]

Similarly, this technology could facilitate the development of other Chemical, Biological, Radiological and Nuclear (CBRN) capabilities such as the production of

---

[9] Lubrano, M, "Emerging technologies: when terrorists print their own weapons", Global Risk Insights (16 January 2018), *at* <globalriskinsights.com/2018/01/terrorism–additive–manufacturing–weapons/> (accessed 4 April 2018).

[10] del Mar Hidalgo García, M, IEEE, "3D printing: A challenge to the battle against WMD proliferation", Analysis Document 17/2016 (15 March 2017) 3, *at* <ieee.es/en/Galerias/fichero/docs_analisis/2016/DIEEEA17–2016_Impresoras_3D_MMHG_ENGLISH.pdf> (accessed 4 April 2018).

[11] Lubrano (n 11). For a description of additive manufacturing processes see, e.g., Bajema and DiEulis (n 9) 7.

[12] Bajema and DiEulis (n 9) 8–9. Potentially too, components for uranium enrichment programmes may be reverse–engineered (ibid, 9). See too Fey, M, "3D Printing and International Security: risks and challenges of an emerging technology" *in* Hessische Stiftung Friedens–und Konfliktforschung, *PRIF Reports* (Frankfurt am Main 2017), 144, *at* <nbn–resolving.de/urn:nbn:de:0168–ssoar–51867–8 pp1–34> (accessed 30 April 2018).

[13] Equally of smaller arms, where the utilization of technology such as 3D printing is most likely, at least initially. Blueprint designs for some weapons are readily accessed through the internet. Lubrano (n 11).

[14] García (n 12) 3.

[15] García (n 12) 4. Similarly see Bajema and DiEulis (n 9) 10.

[16] Bajema and DiEulis (n 9) 12.

detonators for a Radiological Dispersal Device,[17] or the development of chemical weapons.[18] Though the ability to utilise additive manufacturing to produce WMDs still remains theoretical, the capability to use 3D printers to produce (advanced) conventional weapons is moving ever closer to becoming a reality. For instance, Raytheon – a leading company in defence and security technology and innovation – has stated that it now has the capability to print more than 80% of a guided missile's components, the ultimate goal being that operationally deployed military forces could 3D-print more missiles as and when needed.[19] Clearly there is an accompanying risk, however, that such highly sensitive 'build files' could fall into the hands of OCGs/TGs with potentially catastrophic consequences.[20] Worryingly, a recently published report on cyber security 'pinpoint[ed] the susceptibility of manufacturers to cyber risk, revealing that 41 percent of [manufacturing] companies do not believe they have access to enough information to even assess their true cyber risk. And 45 percent feel that they do not have access to the right tools for the job'.[21] Nor are such risks limited to more advanced weapon systems. 3D printing technology has already been used to manufacture firearms in, for example, Australia and Sweden though it is not yet entirely clear if/how they might function.[22] At the very least, such early attempts demonstrate the existence of criminal intent to exploit such technologies for illicit activities.

B. Limitations inherent within existing international approaches

There is broad consensus across many parts of the international community, including within the forum of the UNSC, that increasing cooperation or convergence between OCGs and TGs currently poses a significant threat to international peace and security.[23] Such recognition of a nexus between OCGs and TGs is not, however, new. For example, UN General Assembly Resolution 55/25 (2000), which adopted the UN Convention against

---

[17] Lubrano M, "Emerging technologies: implications for CBRN terrorism", *Global Risk Insights* (4 February 2018), <globalriskinsights.com/2018/02/emerging–technologies–cbrn–terrorism/> (accessed 4 April 2018). Perhaps a more likely scenario is the hacking into critical infrastructure facilities, such as a nuclear power plant or chemical plant, causing the facility itself to become a WMD.

[18] Similarly, see Bajema and DiEulis (n 9) 10–11: "Additive manufacturing is being used to make miniaturized fluidic reaction ware devices that can produce chemical syntheses in just a few hours. This may enable state and nonstate actors to more easily develop chemical agents in the future."

[19] Bajema and DiEulis (n 9) 8–9. Potentially too, components for uranium enrichment programmes may be reverse–engineered (ibid, 9–10).

[20] Bajema and DiEulis (n 9) 9–10.

[21] 'Cyber Security for Manufacturers' report (n 8).

[22] See, e.g., "3D printing, UAVs, and dark web could give terrorists access to WMDs, says UN official", *3D printer and 3D printing news* (29 June 2017), *at* <3ders.org/articles/20170629–3d–printing–uavs–and–dark–web–could–give–terrorists–access–to–wmds–says–un–official.html> (accessed 4 April 2018). Similarly, in Hong Kong where 3D printers were used for weapon modification – Lubrano, M, 'Emerging technologies: when terrorists print their own weapons', *Global Risk Insights* (16 January 2018), *at* <globalriskinsights.com/2018/01/terrorism–additive–manufacturing–weapons/> (accessed 4 April 2018).

[23] See, e.g., UNSC Res 2322 (2016); UNSC Res 2370 (2017). Also, e.g., UNSC Res 2388 (2017) which, while focusing on the trafficking of persons more generally, acknowledges the nexus between OCGs and TGs; more generally too in UNSC Res 2368 (2017). A primary issue is commonly "the need to take measures to prevent and suppress the financing of terrorism, individual terrorists, and terrorist organizations, including from the proceeds of organized crime".

Transnational Organized Crime (UNCTOC), 'call[ed] upon all States to recognize the links between transnational organized criminal activities and acts of terrorism' (para. 6).[24]

Some more recent observations made in the context of a UNSC non-proliferation meeting in June 2017 are revealing in this respect. Izumi Nakamitsu, High Representative for Disarmament Affairs, referred to the relative ease with which those with criminal intent could access 'many of the technologies, goods and raw materials required to produce weapons of mass destruction and their delivery systems [since these] were available through legitimate producers'.[25] Regarding the reality and gravity of any accompanying threats to international peace and security, Joseph Ballard, Senior Officer at the Office of Strategy and Policy at the Organisation for the Prohibition of Chemical Weapons (OPCW), during the same meeting further stated how 'the rising threat posed by non-State actors, the pace of economic development and the evolution of science and technology were all shaping the future of the global disarmament and non-proliferation regimes. Moreover, the use of chemical weapons by non-State actors was no longer a threat, but a chilling reality'.[26] Notably, in terms of specific issues of concern, he emphasized that '[p]reventing non-State actors from acquiring dual-use materials, equipment and technologies was of critical importance to maintaining the global norm against the use of chemical weapons and in favour of international peace and security.'[27]

These concerns are, to some extent, reflected within outputs of the UNSC, illustrated by Resolution 2370 (2017) which stressed the 'paramount need to prevent illegal armed groups, terrorists and other unauthorized recipients from, and identify the networks that support them in, obtaining, handling, financing, storing, using or seeking access to *all types of explosives*'.[28] Such language reflects how the landscape of risk and security threats is evolving regarding the proliferation of WMDs or more conventional weapons by non-State actor groups, including since the creation in 2004 of the non-proliferation regime under UNSC Resolution 1540 (2004) aimed at preventing the proliferation of WMDs by non-State actors. The broader context in which Resolution 2370 was adopted recognized that: 'In tackling drones, 3D printing, the dark web and other emerging threats hindering non-proliferation efforts, States must bolster their efforts as well as technological advances in order to combat the spread of weapons of mass destruction and keep them out of the hands of terrorists and other non-State actors'.[29] More generally, there is recognition of the threats posed by 'the growing nexus between weapons of mass destruction, terrorism and cybersecurity'.[30]

Notably, brief mention is made in Resolution 2370 to the key role played by technology in facilitating the illegal activities of OCGs and TGs, with concern being expressed 'at the increased use, in a globalized society, by terrorists and their supporters of

---

[24] UN General Assembly, *United Nations Convention against Transnational Organized Crime*, 15 November 2000, A/RES/55/25. ('UNCTOC')

[25] UN, 'States Must Step Up Efforts to Check Spread of Deadly Weapons as Non–State Actors Exploit Rapid Technological Advances, Speakers Tell Security Council', Press Release SC/12888 (28 June 2017), *at* <un.org/press/en/2017/sc12888.doc.htm> (accessed 4 April 2018).

[26] UN Press Release SC/12888 (n 26).

[27] UN Press Release SC/12888 (n 26).

[28] UNSC Resolution 2370 (2017), Preamble (emphasis added).

[29] UN Press Release SC/12888 (n 26).

[30] UN, 'Eliminating Weapons of Mass Destruction Only Way to Prevent Non–State Actors from Acquiring Them, Deputy Secretary–General Tells Security Council', Press Release DSG/SM/1035–SC/12629–DC/3678 (15 December 2016) *at* <un.org/press/en.2016/dsgsm1035.doc.htm> (accessed 4 April 2018).

new information and communications technologies, in particular the Internet, to facilitate terrorist acts, as well as their use to incite, recruit, fund, or plan terrorist acts'.[31] This is expanded a little more within the body of the resolution where Member States are urged 'to act cooperatively to prevent terrorists from acquiring weapons, including through information and communications technologies'.[32] In terms of what is being referred to, though no further guidance is given by Resolution 2370, some of the comments made prior to the resolution's adoption are informative.

For instance, Emmanuel Roux, Special Representative of the International Criminal Police Organization (INTERPOL) to the UN, expressly identified the use of 'new technologies such as 3D printing to access and use weapons' as an important area of concern.[33] More generally, he commented on the fact that: '"Today's threat landscape is one of unprecedented complexity" […] noting the convergence between organized crime and terrorism, between old and new technologies and between military and law enforcement efforts.'[34] In response to such challenges, he highlighted the importance of 'strengthening and implementing strong national legislation',[35] a common theme of the representations made. In the context of ITT, however, fully realising such legislative priorities is made more difficult by the seeming lack of recognition of the existence of the criminal justice gaps explored in this article. In a similar vein to INTERPOL's perspective, Jehangir Khan, Officer in Charge of the UN Office of Counter-Terrorism, observed that in the context of '[t]he possibility of terrorists obtaining lethal technologies and new weapons, including weapons of mass destruction', particular areas of concern include '[t]he illicit manufacture and uncontrolled flow of arms', noting that '[t]errorists had also improved their capabilities to design and manufacture improvised explosive devices out of commercially available dual-use components'.[36]

Overall, though preventing the acquisition by OCGs/TGs of conventional weapons remains crucial as comprising the most commonly used means of perpetrating terrorist acts,[37] the paucity of express references to technology within UNSC outputs - such as Resolution 2322 (2016) and Resolution 2370 (2017) - is nonetheless noticeable and surprising considering the growing threats attributable to technological advances including ITT. It is evident from the text of Resolution 2322 and Resolution 2370 that the principal focus is still on threats posed by tangible rather than intangible assets and technology, such as 'the illicit trafficking in small arms and light weapons' which are more commonly acquired and/or used by OCGs and TGs. For instance, the term 'transfer' in relation to weapons or materials which could be used to manufacture weapons[38] is being used in the sense of the prevention and control of physical weapons rather than the transfer of intangible

---

31 UNSC Res 2370 (2017) Preamble; repeating UNSC Res 2322 (2016) Preamble.
32 UNSC Res 2370 (2017) Para. 13.
33 UN, 'Security Council Urges Greater Collective Effort to Prevent Terrorists from Acquiring Weapons, Unanimously Adopting Resolution 2370 (2017)', Press Release SC/12938 (2 August 2017), *at* <un.org/press/en/2017/sc12938.doc.htm> (accessed 4 April 2018).
34 UN Press Release SC/12938 (n 32).
35 UN Press Release SC/12938 (n 32).
36 UN Press Release SC/12938 (n 32).
37 See, e.g., comment by Fedotov, Y, Executive Director of the United Nations Office on Drugs and Crime regarding the adoption of UNSC Res 2370, UN Press Release SC/12938 (n 32).
38 E.g., UNSC Res 2322 (2016) para 11.

technology which could facilitate the illicit manufacture of weapons.[39] Furthermore, the primary focus of the resolution is still on those areas on which OCG and TG related instruments have traditionally focused and which continue to pose the most commonly recurring challenges, namely on States strengthening their judicial, law enforcement and border-control capacities.

A similar approach to ITT related issues and accompanying threats is reflected too in the context of weapons non-proliferation. For instance, in its most recent report to the UNSC, the 1540 Committee

> took note of the *increasing risks of proliferation in relation to non-State actors* arising from developments in terrorism and *in relation to the potential for misuse arising from the rapid advances in science, technology and international commerce* and the need for States to pay constant attention to these developments to ensure effective implementation of the resolution.[40]

Interestingly too, the report noted a number of academic initiatives regarding complexities attributable to the transfer of intangible technology.[41] This is important, especially since the issue of ITT was not envisaged at the time of adoption of Resolution 1540. That said, and despite the potentially considerable security risks posed by the current lacunae within the legal framework, the report takes a noticeably 'light touch' on these issues, perhaps reflective of accompanying political sensitivities. Certainly, this is evident in the tone of Resolution 2325 (2016) on nuclear, chemical and biological threats (for example, at para. 7) illustrated by the language of '*[e]ncourag[ing] States, as appropriate*, to control access to *intangible transfers of technology* and to information that could be used for weapons of mass destruction and their means of delivery'.[42]

The discussion now turns to examining each of the three research questions posed at the outset, starting first with an examination of existing international instruments governing the criminal activities of OCGs and TGs, including terrorism related ones, to determine whether any gaps exist regarding the illicit acquisition of conventional or non-conventional weapons through ITT.

II. Identifying Gaps Concerning ITT within the Existing Applicable International Legal Frameworks

Where cooperation or convergence occurs between OCGs and TGs and/or their traditional domains of activities for criminal financial gain or terrorist purposes, including in relation to ITT activities, it may not be immediately apparent whether the OCG and/or TG international legal framework should apply. Therefore, both are considered here together

---

[39] UNSC Res 2322 (2016) paras 5–7.

[40] UN, 'Letter dated 9 December 2016 from the Chair of the Security Council Committee established pursuant to resolution 1540 (2004) addressed to the President of the Security Council', UN Doc S/2016/1038 (9 December 2016) paras 34, 35 and 174, *at* <un.org/en/ga/search/view_doc.asp? symbol=S/2016/1038> (accessed 4 April 2018) (UNSC Report pursuant to Res 1540 (2004)) (emphasis added). Similarly, this concern was repeated in UNSC Res 2325 (2016), e.g., at para 7, on nuclear, chemical and biological threats.

[41] UNSC Report pursuant to Res 1540 (2004) para 156. An example of such an academic initiative is Bajema and DiEulis (n 9).

[42] UNSC Res 2325 (2016), para. 13 (emphasis added)

with UNSC resolutions, which should also be regarded as forming part of the wider applicable legal framework, especially Resolutions 1373 (2001) and 1540 (2004) which were adopted under Chapter VII of the UN Charter.

A. Current legal framework governing OCGs

The primary instruments governing the activities of OCGs on firearms and weapon related issues are the UN Convention against Transnational Organized Crime 2000[43] (UNCTOC); and its accompanying Protocol against the Illicit Manufacturing of and Trafficking in Firearms, Their parts and Components and Ammunition, which supplements the 2000 Convention (UNCTOC Protocol).[44]

In order for OCGs or TGs to fall within the scope of the UNCTOC, it is necessary that they satisfy the four-limb test established by Article 2(a) UNCTOC: (1) they form 'a structured group[45] of three or more persons, existing for a period of time'; (2) the group 'acts in concert'; (3) the group has 'the aim of committing one or more serious crimes[46] or offences' created by UNCTOC; and (4) and the group exists 'to obtain, directly or indirectly, a financial or other material benefit'. There are four offences created by the UNCTOC: participation in an organized criminal group for the commission of 'serious crime' (Article 5); laundering the proceeds of crime (Article 6); corruption (Article 8); and the obstruction of justice (Article 23).

In terms of the convergence of criminal activities between OCGs and TGs, in some circumstances it is possible that TGs may fall within the scope of the UNCTOC, especially since TGs will normally satisfy the first two limbs of Article 2(a) ('structure group' and 'acting in concert'). An example could be Al Qaeda's alleged criminal activities in the illicit diamond trade in order to fund its ideological terrorist activities[47] since, e.g., money laundering is a prohibited crime under the Convention and the prohibited activities could be linked to a 'financial benefit'. More problematic, however, is where a 'financial benefit' is not clear or present, meaning that the alleged criminal activities must fall within the scope of the undefined 'or other material benefit'. Though this provision has 'the potential of being interpreted very broadly to include non-economically motivated crimes such as

---

43 UNGA Res 55/25 (15 November 2000).

44 UNGA Res 55/255 (31 May 2001). For a similar approach see Organisation of American States, Inter–American Convention against the illicit manufacturing of and trafficking in firearms, ammunition, explosives, and other related materials (adopted in Washington, 14 November 1997).

45 Article 2(c) defines "structured group" as meaning "a group that is not randomly formed for the immediate commission of an offence and that does not need to have formally defined roles for its members, continuity of its membership or a developed structure".

46 Article 2(b) defines "serious crime" as meaning "conduct constituting an offence punishable by a maximum deprivation of liberty of at least four years or a more serious penalty".

47 There are differing views on this. E.g., though the 9/11 Commission did not find persuasive evidence in this regard. "Others contend that Al Qaeda used African diamonds to convert cash into an anonymous transportable form of wealth that could be used to launder funds". 9/11 Commission, *Final Report of the National Commission on Terrorist Attacks Upon the United States*, (2004) 170, <https://www.9–11commission.gov/report/911Report.pdf> accessed 5 April 2018; Rabasa et al.; 'For a Few Dollars More: How Al Qaeda Moved into the Diamond Trade' *Global Witness* (April 2003), *at* <globalwitness.org/sites/default/files/import/Few%20Dollars%20More%200–50.pdf> (accessed 5 April 2018).

environmental or politically-motivated offenses',[48] this is unlikely to be the case. It was understood at the time of the UNCTOC's adoption – including to address the concerns of some States (particularly Iran, India and Pakistan) – that the Convention would not be used as a supplementary anti-terrorism tool, but would only deal with TGs when acting as OCGs in seeking financial gain.[49] Certainly, due to the more controversial nature of terrorism related offences, the risk existed that the effectiveness of UNCTOC might be hindered if it extended to terrorism related offences also. Ultimately though, it remains for these issues to be tested in court.

With respect to ITT related activities which, for instance, enable weapons technology to come into the possession of TGs who intend to use it for terrorist purposes, there are two primary hurdles to these activities falling within the scope of UNCTOC. The first is that such transfer of intangible technology would be for non-financial criminal purposes, which do not seem to fall within the scope of Article 2(a) UNCTOC for the reasons already given. The second is that ITT activities are not criminalized under the UNCTOC either as one of the four specified offences provided for under the Convention, or as a 'serious crime' if it is correct that serious terrorism-related crimes are excluded from the Convention's parameters. Though the definition of 'property' as defined by Article 2(d)[50] could extend to intangible technological assets, the concept of 'property' is approached in a narrow manner within the UNCTOC. Significantly, it does not form the basis of a specifically provided for international crime in and of itself; instead, it is used in the context of either being a facilitator for the commission of another expressly provided for crime, such as money laundering (Article 6);[51] or else in the context of the freezing, seizure and confiscation of property[52] following the conviction of persons engaged in activities criminalized under the Convention (Articles 12-14).

In relation to the UNCTOC Protocol again, at first glance, this could extend to ITT related activities. Article 2 states that: 'The purpose of this Protocol is to promote, facilitate and strengthen cooperation among States Parties in order to prevent, combat and eradicate the illicit manufacturing of and trafficking in firearms, their parts and components and ammunition'. Furthermore, the scope of the Protocol extends to 'the prevention of illicit manufacturing of and trafficking in firearms' (Article 4(1)). Both, the illicit manufacturing and trafficking in firearms are criminalized under Article 5 of the Protocol. However, from the definitions and scope of the Protocol, as provided for in Article 3, it is clear that it was intended to cover physical rather than intangible firearms et al. As to whether the Protocol could extend to situations of, for example, 3D printing resulting in the 'illicit manufacturing'

---

48 Orlova AV and Moore JW, "'Umbrellas' or 'Building Blocks'?: Defining International Terrorism and Transnational Organized Crime in International Law" 27 *Houston Journal of International Law* (2005) 267, 283.

49 Orlova and Moore (n 48) 286.

50 Article 2(d) UNCTOC defines "property" as meaning "assets of every kind, whether corporeal or incorporeal, movable or immovable, tangible or intangible, and legal documents or instruments evidencing title to, or interest in, such assets".

51 E.g., Article 6(1)(a)(i) UNCTOC provides one of the criminal offences as being: "The conversion or transfer of property, knowing that such property is the proceeds of crime, for the purpose of concealing or disguising the illicit origin of the property....". Similarly, see Article 6(1)(b)(i) UNCTOC.

52 Article 2(f) UNCTOC "freezing" or "seizure" of property; and Article 2(g) "confiscation" of property. Such property could include intangible property such as software and patents.

of weapons, this seems unlikely under the Protocol due to its narrow scope as defined by Article 3(d):[53]

> 'Illicit manufacturing' shall mean the manufacturing or assembly of firearms, their parts and components or ammunition:
> (i) From parts and components illicitly trafficked;
> (ii) Without a licence or authorization from a competent authority of the State Party where the manufacture or assembly takes place; or
> (iii) Without marking the firearms at the time of manufacture, in accordance with article 8 of this Protocol;

As such, it would appear that the scope of the Protocol is limited to physical firearms which were the product of illicit manufacturing or the parts and components which were subsequently illicitly trafficked once manufactured, but not to the prior transfer of enabling intangible technology, for instance, weapon blueprints or software codes, which facilitated the manufacture of these weapons.

These findings are unsurprising given that the security and technological contexts in which the texts of the UNCTOC and its 2001 Protocol were agreed and adopted, some 18 and 17 years ago respectively, were markedly different to those prevailing today. Certainly, the post 9/11 era has seen the increasing globalization of OCG and TG activities as well as of their ambitions, together with the pace of parallel technological developments, they have far exceeded expectations since the turn of the millennium. Though the text of the UNCTOC, including its broad definitions, was intended to cover existing and future not yet envisaged scenarios of organized crime - and some would argue that the Convention remains successful in this objective - it is respectfully submitted here that 'if' the commission of a 'serious crime' excludes terrorist crimes then it cannot extend to situations of OCG/TG cooperation or convergence for terrorist purposes regarding the use of ITT. Nor does the transfer of intangible assets, such as weapons blueprints, or the use of technology for ITT purposes *per se* currently constitute 'serious crimes' within the existing international criminal justice framework governing organized criminal and terrorist acts. A central argument of this article is that such activities should urgently be criminalized due to the serious threats to international peace and security they pose.

B. Current legal framework governing TGs

The examination now turns to considering whether ITT may fall within the scope of the universal anti-terrorism instruments. The potential applicability of the TG legal framework is of especial importance where the activities of TGs do not fall within the scope of the OCG framework and/or it is, for instance, politically expedient to prosecute certain crimes under an anti-terrorism rather than organised crime legal regime.

A survey of the 19 international legal instruments aimed at preventing terrorist acts adopted since 1963 – categorized as (a) civil aviation, (b) protection of international staff, (c) the taking of hostages, (d) nuclear material, (e) maritime navigation, (f) explosive materials, (g) terrorists bombings, (h) financing of terrorism, and (i) nuclear terrorism – reveals a similar finding as for the OCG framework: very few of these instruments – including those

[53] Similarly, Article 3(e) UNCTOC definition of "illicit trafficking" would seem to be limited in scope to physical weapons.

newer treaties governing terrorist bombings, the financing of terrorism or nuclear terrorism – make provision which potentially could extend to the criminalization of ITT, whether under national or international law.

With respect to terrorist bombings, the 1997 International Convention for the Suppression of Terrorist Bombings[54] (Terrorist Bombings Convention) is concerned with criminalizing the unlawful and intentional use of explosives and other lethal devices in, into, or against various defined public places with intent to kill or cause serious bodily injury or to cause extensive destruction of a public place (for example, Articles 2 and 4). It does not, however, provide for (and therefore criminalize) how terrorists acquired the weapons or technology necessary to carry out such acts.

In relation to nuclear security[55] and threats of nuclear terrorism, generally those instruments adopted under the auspices of the International Atomic Energy Agency (IAEA) regulate physical activities and threats. For instance, the parameters of the 1980 Convention on the Physical Protection of Nuclear Material[56] are limited to criminalizing the unlawful possession, use, *transfer* or theft of nuclear material and threats to use nuclear material to cause death, serious injury or substantial property damage. As the Convention's title indicates, its focus is on the protection of *physical, rather than intangible*, nuclear assets.

Similarly, the 2005 International Convention for the Suppression of Acts of Nuclear Terrorism (Nuclear Suppression Convention)[57] was adopted under the auspices of the UN as one of the most recent universal anti-terrorism instruments. It covers a broad range of serious criminal acts, such as threats or attempts to attack nuclear power plants and nuclear reactors (for example, Article 2), as well as dealing with the aftermath of such an attack, bringing perpetrators to justice and so forth. It does not, however, expressly criminalize the means or methods by which TGs are able to acquire or manufacture the weapons needed to perpetrate such crimes. That said, potentially, ITT could fall within the parameters of Article 7(1)(a) which envisages cooperation between States Parties including in the form of criminalizing on their territories inter alia 'illegal activities of persons, groups and organizations that encourage, instigate, organize, knowingly finance or *knowingly provide technical assistance or information* or engage in the perpetration of those offences'. This could catch OCG or TG activities during the preliminary stages of an attack, namely the transfer of technical know-how to TGs who subsequently use it for acts of terrorism prohibited under the Convention. Certainly, none of the definitions specified by Article 1 would appear to impede this.

The same is true of the 2005 Protocol to the Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation (2005 SUA Protocol).[58] The Protocol was adopted under the auspices of the International Maritime Organization and

---

[54] UN General Assembly, *International Convention for the Suppression of Terrorist Bombings*, 15 December 1997, A/RES/52/164.

[55] The term "nuclear security" is generally taken to mean: "the prevention and detection of, and response to, theft sabotage, unauthorized access, illegal transfer or other malicious acts involving nuclear material, other radioactive substances or their associated facilities". International Atomic Energy Agency, 'The International Legal Framework for Nuclear Security' IAEA International Law Series No. 4 (IAEA, Vienna 2011).

[56] United Nations, *Convention on the Physical Protection of Nuclear Material* (1980) 1459 UNTS 124.

[57] United Nations, *International Convention for the Suppression of Acts of Nuclear Terrorism* (2005) 2445 UNTS 89.

[58] International Maritime Organisation, *Protocol of 2005 to the Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation*, 14 October 2005.

aims to strengthen the existing 1988 Convention of the same name,[59] including regarding the possible use of biological, chemical or nuclear weapons. Though the Protocol extends to both conventional and non-conventional weapon types, once again it is clear from the text (for example, Article 4 of the 2005 Protocol regarding Article 3*bis* of the 1988 Convention) that its primary focus is on physical weapons and substances rather than intangible technological assets. The only provision of the Protocol, which potentially may apply to ITT is Article 3*quater*(e). This states that any person who 'contributes to the commission of one or more offences set forth in article 3, 3*bis* [...] or subparagraph (a) or (b) of this article' also commits an offence within the scope of the 1988 Convention. Under Article 3*bis*:

> (1) Any person commits an offence within the meaning of this Convention if that person unlawfully and intentionally:
> (a) when the purpose of the act, by its nature or context, is to intimidate a population, or to compel a government or an international organization to do or to abstain from doing any act:
> [(i)-(iv) detail prohibited acts]
> .....
> (iv) any equipment, materials or *software or related technology that significantly contributes to the design, manufacture or delivery* of a BCN weapon, with the intention that it will be used for such purpose.[60]

Potentially, this provision could at least indirectly capture ITT. One way could be in circumstances involving the physical transportation of a device, such as a 3D printer – with or without any accompanying software – with the intention of using it to print components for the manufacture or delivery of a BCN weapon subsequently used to perpetrate a terrorist attack against or from a 'ship' (as defined by Article 1 of the Convention and amended by Article 2 of the Protocol). There is no suggestion from the text of the SUA Convention or Protocol that a link must exist between the transporting ship and the ship from which a subsequent attack was launched or a ship that was itself the object of an attack. With respect to ITT, it is unclear from the Convention's provisions, which do not define 'software', as to whether or not this might extend to an intangible technology asset such as a weapons blueprint. In any event since both technological blueprints and software are copyright protected, an analogy could be made. Furthermore, intangible assets would normally be understood as comprising 'certain types of knowledge [which would include blueprints], technical assistance, *technology and software*.'[61]

Notably too, a provision similar to Article 3*bis* of the SUA Convention exists under Article 1(i)(4) of the 2010 Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation[62] applicable to the civil aviation transportation context. Furthermore, it mirrors Article 3*quater* with a broad 'catch-all' provision in Article 5(b):

---

[59] UN General Assembly, *Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation* (1988) 1678 UNTS 201.

[60] Emphasis added.

[61] SIPRI, "SIPRI hosts workshop on Intangible Transfers of Technology" (27 February 2018), <sipri.org/news/2018/sipri–hosts–workshop–intangible–transfers–technology–itt> (accessed 30 April 2018).

[62] International Civil Aviation Organisation, *Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation*, (2010) 974 UNTS 177.

'contributing in any other way to the commission' of the offences specified under the Convention. Potentially, these provisions could apply similarly to ITT in the manner explained regarding the SUA Convention and its 2005 Protocol.

More generally, it is arguable that the IAEA's pivotal role of 'helping States to build capacity to prevent terrorists from accessing nuclear or radiological materials'[63] could extend to ITT related issues, including advising on how the legal gaps and issues that would benefit from further clarification identified here might be addressed at the national legislative level.[64] Ultimately, nuclear, etc., safety, including in relation to terrorist acts, is the responsibility of States.

C. UNSC Chapter VII resolutions

The two UNSC resolutions of especial relevance here are Resolutions 1373 (2001) and 1540 (2004), both of which were adopted under Chapter VII of the UN Charter. Such resolutions are regarded by many to be quasi-legislative in nature as they are binding upon all Member States under Article 25 UN Charter.[65]

With respect to Resolution 1373, its principal focus has been on preventing and suppressing the financing of terrorist acts;[66] ensuring that States do not 'provid[e] any form of support, active or passive, to entities or persons involved in terrorist acts, including by […] eliminating the supply of weapons to terrorists';[67] preventing the commission of terrorist acts;[68] and '[d]eny[ig] safe haven to those who finance, plan, support, or commit terrorist acts, or provide safe havens.' To such ends, Resolution 1373 requires States - using the language of '*[d]ecides* that all States shall' - to take a number of actions, including national legislative action where necessary to criminalize the 'financing, planning, preparation or perpetration of terrorist acts'.[69]

In this context, the related challenges posed by 'traffic in arms, explosives or sensitive materials; use of communications technologies by terrorist groups; and the threat posed by the possession of weapons of mass destruction by terrorist groups' were acknowledged,[70] but without the imposition on States of accompanying obligations by the resolution. Instead, the language of '*[c]alls* upon all States' is used. Significantly, though the resolution referred to the use of 'communications technologies by terrorist groups' – as with subsequent resolutions aimed at preventing terrorism and strengthening criminal justice responses – the primary

---

[63] UN General Assembly, *The United Nations Counter–Terrorism Strategy*, 8 September 2006, A/RES/60/288, Annex Part III.9.

[64] This would be consistent with the obligations of States under UN Security Council, Res 1540 (para. 2) whereby the UNSC "[d]ecide[d] also that all States, in accordance with their national procedures, shall adopt and enforce appropriate laws which prohibit any non–State actor to manufacture, acquire, possess, develop, transport, transfer or use nuclear, chemical or biological weapons and their means of delivery, in particular for terrorist purposes, as well as attempts to engage in any of the foregoing activities, participate in then as an accomplice, assist or finance them".

[65] On such issues see further, e.g., Talmon, S, "The Security Council as World Legislature" 99 *American Journal of International Law* (2005) 175; Martinez, LMH, "The Legislative Role of the Security Council in its Fight against Terrorism: Legal, Political and Practical Limits" 57 *International Constitutional Law Quarterly* (2008) 333.

[66] UNSC Res 1373, para. 1(a).

[67] Ibid, para. 2(a).

[68] Ibid, para. 2 (b).

[69] Ibid, paras. 1 (b), 2(e).

[70] Ibid, para. 3(a).

focus here is on their utilization to 'incite, recruit, fund, or plan terrorist acts'[71] rather than on the pivotal role such technologies may play in the transfer of intangible technology, such as via the Internet or satellite, to facilitate terrorist attacks. Notably too, the nexus was recognized between 'international terrorism and transnational organized crime, […] illegal arms- trafficking, and illegal movement of nuclear, chemical, biological and other potentially deadly materials' thereby necessitating enhanced coordination of efforts at the national, subregional, regional and international levels 'to counter such criminal activities'. Despite the gravity of these activities being recognized in terms of their 'accompanying threats to international peace and security',[72] once again it is intriguing, or indeed perturbing, that such threats are merely '*[n]ote[d]* with concern' with no accompanying requirements upon States to take necessary action to prevent or counter them.

Three years later, Resolution 1540 (2004)[73] sought to further respond to such threats through addressing an identified gap within the existing international framework. It requires all Member States to adopt and enforce laws that criminalize non-State actors who 'manufacture, acquire, possess, develop, transport, transfer or use nuclear, chemical or biological weapons and their means of delivery, in particular for terrorist purposes',[74] while also prohibiting States from assisting non-State actors in this regard.[75] Of particular relevance to the current discussion is the fact that Resolution 1540 is primarily concerned with the physical proliferation of WMDs and, as such, does not engage with issues such as ITT. Consequently, the framework provided under Resolution 1540 is now considered by at least some to be 'insufficient' on its own to respond to current global threats.[76] Indeed, when Izumi Nakamitsu briefed the UNSC in June 2017, she further highlighted the fact that 'terrorists groups had evolved into cyberspace and, alongside other non-State actors, exploited loopholes to access the technology they needed'.[77] Indeed, as another commentator has observed:

> 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.[78]

---

71 See, e.g., UNSC Res 2370 (2017) Preamble; UNSC Res 2368 (2017) Preamble, para 23; UNSC Res 1624 (2005) Preamble, para 3.

72 UNSC Res 1373, para 4.

73 UNSC Res 1540 is reviewed and reviewed periodically, most recently for a period of 10 years by UNSC Res 1977 (2011) which extended the mandate of the Committee until 25 April 2021.

74 UNSC Res 1540 (2004), para. 2; see also, para. 3.

75 Ibid, para 1.

76 See, e.g., the related comments of the Russian Federation. UN Press Release SC/12888 (n 26).

77 UN Press Release SC/12888 (n 26).

78 García (n 12) 6.

Some might argue that Resolution 1540 (2004) extends to proliferation threats posed by ITT - such as 3D printers - through its broad definition of 'related materials'[79] (preamble, forming part of the non-operative and therefore non-legally binding part of the Resolution). Even if this is correct, as the earlier discussion (section II.B) of the universal anti-terrorism legal framework revealed, the potential circumstances in which ITT may be covered by existing legal provisions are, at best, relatively few and narrow in scope.

III. Impact of ITT Gaps on International Cooperation

As the OCG and TG conventions, together with other key instruments such as UNSC resolutions,[80] testify, effective international cooperation lies at the core of the current international architecture governing organized criminal activities and terrorist crimes. Such cooperation reflects the same identified priorities mentioned previously, such as prosecuting or extraditing 'any person who supports, facilitates, participates or attempts to participate in the financing, planning, preparation or commission of terrorist acts or who provides safe havens'.[81]

From a criminal justice perspective – which aims to prevent the perpetration of these serious crimes and to bring to account those persons who do commit them, ensuring too that no 'safe haven' exists – judicial and law enforcement cooperation is critical. This is especially true in the areas of extradition (*aut dedere aut judicare*) and mutual legal assistance, which are central to, and the most common forms of cooperation under, the existing OCG and TG legal frameworks.[82] International cooperation is also important in other respects, such as 'at the bilateral, regional and international levels to prevent, combat and eradicate the illicit manufacturing of and trafficking in firearms, their parts and components and ammunition'.[83]

Any such international cooperation is, however, premised on the requirement that the activities in question are criminalized. If they are not, and regardless of how significant a threat to international peace and security certain activities might pose, then transnational criminal justice cooperation will not be possible and other forms of cooperation, such as intelligence sharing, may lack the necessary political will and accompanying resources to be effective. With respect to ITT, with the possible and limited exceptions identified regarding the existing TG legal framework (section II.B), there are two principal areas where international cooperation is needed, but not provided for under the existing legal frameworks governing OCGs and TGs. First, existing treaties do not criminalize the transfer of intangible technology as an asset for criminal purposes, whether for financial gain or to perpetrate terrorist acts. Second, the existing frameworks do not criminalize the utilization

---

[79] UNSC Res 1540 defines "related materials" broadly to mean "materials, equipment and technology.... which could be used for the design, development, production or use of nuclear, chemical and biological weapons and their means of delivery".

[80] For example, UNSC Res 2370 (2017) para 15; UNSC Res 2322 (2016) para 14; UNSC Res 1540 (2004) paras 3(d), 8(c), 9 and 10; UNSC Res 1566 (2004) para 2; UNSC Res 1373 (2001) para 3.

[81] UNSC Res 1566 (2004) para 2.

[82] The UNCTOC, its 2001 Protocol, as well as universal anti–terrorism instruments all have extensive provisions regarding international cooperation, including extradition, mutual legal assistance and police cooperation. Other primary areas for international cooperation are the transfer of criminal proceedings, execution of foreign sentences, recognition of foreign criminal judgements, confiscation of the proceeds of crime, as well as collection and exchange of information between intelligence and law enforcement services.

[83] Article 13(1) UNTCOC Protocol.

of technology – such as cyberspace – for the transfer of intangible technology assets by OCGs or TGs. The implications of these gaps, together with the accompanying inability of States to cooperate fully on these matters, are likely to increase in parallel (and therefore exponentially) with rapidly developing technologies including those relevant to ITT, with the accompanying growing threats to international peace and security.

IV. Possible Solutions and Future Steps

In response to the identified and important gaps in coverage within the existing international legal frameworks governing organized crime and terrorism, a number of possible solutions and future steps are explored here, each of which merits further research and consideration in its own right.

A. UNSC Resolution

The identified gaps represent significant threats to international peace and security, including due to their ability to facilitate the proliferation of both conventional and Chemical, Biological, Radiological and Nuclear weapons by criminal non-State actor groups. Other gaps exist too in the areas of information and communication technologies, regarding matters such as *knowledge trafficking or trading intended inter alia to support or to otherwise assist OCGs or TGs.*

Such gaps are likely to widen in size and effects in parallel with rapid technological advances and increased cooperation and convergence between OCGs and TGs. Accordingly, the Security Council should be apprised of these issues with immediate effect. Specifically, it is strongly recommended that the Security Council consider the adoption of a Chapter VII resolution, in a similar style and format to Resolutions 1373 (2001) and 1540 (2004), which seeks explicitly to address current gaps and complexities attributable to developing technologies, including matters of ITT and related dual-use technologies.

In this way, the focus and reach of existing UNSC resolutions would be extended beyond the current primary focus on issues of incitement, recruitment, financing and planning acts of terrorism which remain important but, by themselves, are insufficient for responding adequately to current and emerging technological sources of threat to international peace and security. Such a resolution would have the further benefit of taking immediate effect. It would require States to not only ratify and implement existing applicable conventions (some of which may have limited application to ITT contexts as previously outlined in Section II), but also to take any necessary legislative action at the national level to criminalize such acts as serious offences. This could be achieved whilst the political appetite for additional protocols is explored (see section IV.B below) and any subsequent treaty negotiations take place. Such a resolution may also serve to further incentivize States to progress the adoption of additional protocols as the preferred longer-term solution for closing current treaty gaps.

If such a UNSC resolution is adopted, then it is strongly recommended that it provides clear definitions of key terms, such as ‘intangible’, ‘technology’, ‘transfer’, ‘dual-use’ and so forth, from the outset to provide adequate levels of legal certainty and to ensure that the existing gaps are closed as fully as is possible. As Orlova and Moore have observed, ‘[w]ithout precise definition, ambiguities are created that allow terrorists and organized crime members to “slip through the cracks” in the law. States, too, can take advantage of

legal uncertainties to expand their room for maneuver'.[84] This would also go some way towards avoiding a repetition of the situation created by Resolution 1373 whereby States were required to take anti-terrorism legislative action in the absence of a working definition of 'terrorism' which was not provided until three years later by Resolution 1566 (2004) in its paragraph 3. One of the unfortunate consequences of this was that States adopted often inconsistent approaches to criminalizing terrorist offences with the potential to impede rather than facilitate international cooperation and rule of law compliance, including on criminal justice issues. Certainly, such an approach would be reflective of ongoing discussions and reform within the European Union (EU) towards the development of common legal definitions and approaches on cybersecurity, including the increased harmonization of national legislative approaches towards countering the use and transfer of technology for criminal purposes.[85]

B. Additional protocol(s) to existing OCG and TG related conventions

As has just been mentioned, the preferred, longer-term, solution is for the international community, through existing UN mechanisms, to explore the feasibility of new protocol(s) to both the UNCTOC as well as to relevant universal anti-terrorism instruments, which address the significant gaps identified in this article. These gaps are the need to criminalize: (1) the transfer of intangible technology as an illicit asset; and (2) the utilization of technology for illicit ITT purposes, where either or both of these activities are intended to be for organized criminal or terrorist purposes. The adoption of such protocols would afford an opportunity to address any other identified gaps (for example, as suggested in Section IV.A) or to provide further definitional clarity for instance concerning the scope of the UNCTOC regarding TGs, particularly where OCG/TG convergence occurs and existing definitional lines and motivations between organised crime and terrorism may become blurred.

Due to the different scopes and underpinning rationales of the UNCTOC compared with anti-terrorism instruments, namely for criminal financial gain opposed to ideological terrorist purposes respectively (see further Section II.A), separate protocols would be needed for the OCG and TG related treaties. As Shelley and Picarelli concluded, though 'transnational criminal organizations and terrorist groups often adopt similar methods, they are inherently striving for divergent ends. Crime is primarily an economically driven enterprise, while terrorism remains rooted in political pursuits'.[86]

Furthermore, as the current UNCTOC and anti-terrorism convention definitional approaches illustrate, the adoption of an 'umbrella approach' in an attempt to develop 'all-inclusive legal definitions of international terrorism and transnational organized crime' has not been entirely successful. This, in part, has been attributable to the inability of the

---

[84] Orlova and Moore (n 48) 269.

[85] See, e.g., Council of Europe, "Reform of cyber security in Europe", *at* <http://www.consilium.europa.eu/en/policies/ cyber–security/> (accessed 5 April 2018); European Commission, Proposal for a Regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification, Corrigendum, COM(2017) 477 final/2 (4 October 2017).

[86] Shelley, L and Picarelli, J, "Methods Not Motives: Implications of the Convergence of International Organized Crime and Terrorism" 3 *Police Practice and Research* (2002) 305, 305. Similarly, see E Mylonaki, E, "The Manipulation of Organised Crime by Terrorists: Legal and Factual Perspectives" 2 *International Criminal Law Review* (2002) 213, 213–14 about not lightly conflating the OCG and TG phenomena.

international community to secure universal definitional consensus. Most notably here of the term 'terrorism' as illustrated by the continuing 'stalemate' to finalise the text of the draft UN Comprehensive Convention on International Terrorism. Further, the international community appears to struggle to reach political compromises during treaty negotiations. This is illustrated by the weaknesses inherent in the definitions of Article 2 of the UNCTOC, which were not high priority issues during the Palermo treaty negotiations. They are consequently criticised as being both 'overly broad....[and] at the same time under-inclusive'.[87] In contrast, as, for example, the anti-terrorism sectoral convention approach demonstrates, 'narrow operational legal definitions of specific terrorist and organized criminal conduct' can be more successful,[88] and constitute an approach which could be applied to the drafting of additional protocols to ensure that they are tailored towards the specific needs of the OCGs and TGs contexts in a manner that is more politically acceptable.

In any event, it is further suggested here that it would not be beneficial or desirable to seek to deal with these matters by means of one protocol, including to cover situations of OCG and terrorist convergence – even if technically possible within the parameters of the existing instruments, which is questionable (see further section II.A). Doing so would further complicate the prosecution of related crimes and would be likely to hinder international law enforcement and judicial cooperation too. For instance, not only would linkages between alleged terrorist crimes and an OCG have to be proven, which, evidentially, can already be very difficult to establish, but furthermore, any additional ideological/political element required for the terrorist element of an offence would add a further layer of complexity and difficulty for all parties engaged in criminal justice processes and proceedings.

C. Ratification and implementation of existing OCG and TG treaty instruments

In parallel, it is essential to sustain momentum and existing efforts, such as capacity development, aimed at exhorting and enabling States to ratify and effectively implement as well as enforce the existing UNCTOC and universal anti-terrorism treaty regimes, including as required to by paragraph 3 of UNSC Resolution 1373 and paragraph 8 of Resolution 1540.

Of especial relevance to the current discussion are those limited number of anti-terrorism treaties, discussed in section II.B, which may potentially encompass ITT related crimes, albeit in a limited way. Although the Terrorist Bombings Convention is widely ratified,[89] the current ratification status of the Convention for the Suppression of Acts of Nuclear Terrorism is relatively low.[90] Similarly, the ratification status of the Protocol to the SUA Convention is very poor.[91] The Beijing Convention has yet to come into effect.[92]

---

87 Orlova and Moore (n 48) 284, see more widely on this issue pp. 281–87.

88 Orlova and Moore (n 48) 269.

89 170 State Parties out of a possible 193 UN Member States. Ratification status available *at* <treaties.un.org/pages/ViewDetails.aspx?src=IND&mtdsg_no=XVIII–9&chapter=18&clang=_en> (accessed 5 April 2018).

90 Only 113 State Parties. Ratification status available *at* <treaties.un.org/pages/ViewDetailsIII.aspx?src=TREATY&mtdsg_no=XVIII15&chapter=18&Temp=mtdsg3 &clang=_en> (accessed 5 April 2018).

91 SUA Convention 1988 has 156 State Parties, but there are only 36 State Parties to the SUA Protocol 2005. Ratification status available *at* <imo.org/en/About/Conventions/StatusOfConventions/Documents/StatusOfTreaties.pdf> (accessed 5 April 2018).

92 Ratification status available *at* <www.icao.int/secretariat/legal/List%20of%20Parties/Beijing_Conv_EN.pdf?TSPD_101_R0=cc59c7a4f7af26cade6d2dd7dc7fff78n5m00000000000000008e895dd1ffff000000000000000000000000000005ac50d0100d0280238> accessed 5 April 2018.

Perhaps an increased realisation by States of the potentially catastrophic consequences of terrorist attacks facilitated through ITT may assist in re-energizing their current ratification and implementation efforts. Notably, the current ratification status of the UNCTOC is almost universal,[93] though that of the UNCTOC Protocol is still relatively low.[94]

D. Increased regulation

Ultimately, due to their gravity including from an international peace and security perspective, illicit ITT and related issues should be expressly criminalized as 'serious' international offences, falling therefore within the auspices of international as well as national criminal law, as proposed above (sections IV.A and B).

In addition, a number of further proposals are made which would also go some way towards strengthening the existing legal architecture governing OCG and TG activities. Indeed, binding national or regional regulations, as well as effective 'soft law' instruments (discussed next in section IV.E below), can act as stepping stones towards the development of binding international obligations under treaty and customary international law whilst also placing these issues more prominently on national and international agendas.

With respect to increased regulation,[95] the EU is probably the most advanced (at least institutionally) in relation to dual-use items of which it controls the export, transit and brokering.[96] Certainly, it has developed principles, together with some limited jurisprudence by the Court of Justice of the EU,[97] which could inform the substantive content of any subsequent UNSC resolution and additional protocols, as well as national law, policy and practice on these issues. Its principal instrument is Council Regulation (EC) No 428/2009 of 5 May 2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items.[98] To ensure consistency of approach throughout the EU's

---

93 189 State Parties. Ratification status available *at* <treaties.un.org/pages/ViewDetails.aspx?src=TREATY&mtdsg_no=XVIII–12&chapter=18&clang=_en> (accessed 5 April 2018).

94 115 State Parties. Ratification status available *at* <treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=XVIII–12–c&chapter=18&clang=_en> (accessed 5 April 2018).

95 See, e.g., Lubrano (n 11) regarding the pressing need for increased regulation for additive manufacturing.

96 Interestingly though, the current EU plan for fighting serious and organised crime (2017–2021) does not identify OCG/TGs linkages as one of its 10 priorities. See European Council, "The EU fight against organised crime", *at* <consilium.europa.eu/en/policies/eu–fight–against–organised–crime–2018–2021/> (accessed 5 April 2018).

97 The case law of the Court of Justice of the EU, while dealing with technology transfer in the context of sanctions regimes, has mostly focused on matters regarding financial assistance and association with regimes and entities. Some principles developed within the context of cases dealing with 'support' for certain political regimes could potentially be applied, by analogy, to the context of transferring technology to those bodies. See, e.g., CJEU, C–385/16 P *Sharif University of Technology v Council* [2017], EU:C:2017:258; CJEU, C□348/12 P *Council of the European Union v Manufacturing Support & Procurement Kala Naft Co.* [2013], EU:C:2013:776; CJEU, C□72/15 *Rosneft Oil Company OJSC v Her Majesty's Treasury, The Secretary of State for Business, Innovation and Skills, The Financial Conduct Authority* [2017], EU:C:2017:236.

98 Official Journal 2009 L 134/1–269. On occasion, country specific regulations have been adopted too which incorporate "dual–use" technology, e.g., Council Regulation (EU) No 833/2014 of 31 July 2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine, OJ L229/1; Council Common Position 2006/795/CFSP of 20 November 2006 concerning restrictive measures against the Democratic People's Republic of Korea Decision 2012/635/CFSP amending Decision 2010/413, OJ L282/58. See too Common Military List of the European Union (adopted by the Council on 11 March 2013) (equipment covered by Council Common Position 2008/944/CFSP defining common rules

Membership together with more effective implementation and enforcement, Council Regulation 428/2009 establishes common EU control rules, a common EU list of dual-use items as well as coordination and cooperation mechanisms. That said, the EU has not yet fully resolved OCG/TG convergence issues within its own normative framework, with proposals currently under review regarding updating its existing legislative framework to better regulate technological developments such as 3D printers.[99]

Existing EU approaches reflect broader international commitments of both itself and its Member States, especially under multilateral export control regimes, aimed at countering inter alia the criminal activities of OCGs and TGs. These include 'dual-use' material and weapon export legal agreements (governing conventional weapons as well as WMDs), notably under the Australia Group, the Missile Technology Control Regime, the Nuclear Suppliers Group, and the Wassenaar Arrangement,[100] reflecting too WMD non-proliferation obligations under UNSC Resolution 1540 as well as relevant treaty instruments. Under current arrangements, both the exporter and importer of such technologies are obligated to give full details regarding all possible final uses of the products involved in order to reduce the likelihood of their being used for criminal purposes. That said, even these agreements have not all been kept fully up-to-date with technological advancements. For example, it was recently noted that '[c]urrently, there are no explicit controls on [additive manufacturing] devices or 3D printers in the [Missile Technology Control Regime] control lists. To date, the [Wassenaar Arrangement] is the only multilateral export control regime that has introduced control list items mentioning [additive manufacturing].'[101] Significantly though, these existing trade agreements also do not criminalize the ITT activities of OCGs/TGs explored in this article and, therefore do not currently assist in addressing the identified legal gaps.

There are, though, corresponding risks accompanying any increased regulation which need to be adequately considered and addressed, including to avoid unintended consequences.[102] These may apply similarly to the criminalization of some ITT related issues in the context of the adoption of a further UNSC resolution or additional protocol, as well as the development of any 'softer' framework (section IV.E). One such issue is the related challenges for exporters/importers to be able to determine or anticipate all possible uses of

---

governing the control of exports of military technology and equipment, OJ C18/1) which lists certain military equipment and technology but does not contain a separate definition of "technology".

99 See, e.g., European Parliament, "Control of trade in dual–use items: Council Regulation 428/2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual–use items", Briefing (September 2016), *at* <europarl.europa.eu/RegData/etudes/BRIE/2016/587340/EPRS_BRI%28 2016%29587340_EN. pdf> (accessed 5 April 2018); also, Communication to the Council and the European Parliament, "The Review of export control policy: ensuring security and competitiveness in a changing world", *at* <trade.ec.europa.eu/doclib/docs/ 2014/april/tradoc_152446.pdf> (accessed 5 April 2018).

100 For further details, see García (n 12) 4.

101 Brockmann, K, and Bauer, S, "3D printing and missile technology controls", SIPRI Background Paper (November 2017) 10, <sipri.org/publications/2017/sipri–background–papers/3d–printing–and–missile–technology–controls> (accessed 5 April 2018). As to whether or not further export control regulation of 3D printers is needed see, e.g., Project Alpha, *Export Controls and 3D Printing*, 21 June 2013, *at* <projectalpha.eu/export–controls–and–3d–printing/> (accessed 5 April 2018).

102 E.g., United States Supreme Court, *Holder v Humanitarian Law Project*, 130 S Ct 2705 (2010) regarding the reach of national legislation adopted pursuant to UNSC Res 1373 extending to humanitarian activities. See further Pantuliano, S, Mackintosh, K, and Elhawary, S, with Metcalfe, V, "Counter–terrorism and humanitarian action: Tensions, impact and ways forward", Humanitarian Policy Group Policy Brief 43 (October 2013), *at* <alnap.org/system/files/content/resource/ files/main/7347.pdf> (accessed 5 April 2018).

'dual technology' with the accompanying risks that any further regulation may hinder or even undermine technological innovation and international trade. Consequently, there is a pressing need for increased legal certainty regarding how to deal with the potential for new technologies to be used illicitly, including by OCGs and TGs. In this regard, it could be helpful to draw a direct analogy between intellectual property and information technology regarding the principle of 'technological neutrality'.[103] With this approach, blame for any illicit use of technology lies with its users rather than with the technology itself which is not at fault as a 'neutral' entity even if it has dual-use (legitimate and illicit) potential.[104] Indeed, as part of the EU's efforts to recast its Dual-use Regulation, intended to ensure increased certainty regarding the application of ITT controls, there have been recurring calls from different commercial sectors for greater 'legal clarification of the coverage of ITT controls and practical guidelines to help with compliance'.[105] To this end, the review of the EU Dual-Use regulation has proposed new guidelines premised on international human rights law, international humanitarian law and terrorism as a tool for States when making assessments on licence applications. This would be accompanied by due diligence obligations on companies 'to establish whether any unlisted dual-use goods that they are planning to export will be used in any of the situations covered by the catch-all clause'.[106]

Another, more sinister, possibility relates to the aggravated consequences of such highly sensitive know-how falling into the hands of OCGs or TGs.[107] Nor are such risks hypothetical as the theft through hacking of 40,000 documents, including 60 classified military files, from Daewoo Shipbuilding & Marine Engineering Co. Ltd, recently acknowledged by the Ministry of National Defense of the Republic of Korea, illustrates. The potential for these stolen intangible technology assets to be utilized for criminal purposes was addressed in the subsequent Report of 5 March 2018 of the Panel of Experts established pursuant to Resolution 1874 (2009) in the following terms: 'The Panel views such activity as constituting evasion of the arms embargo, given that such technological information could directly contribute to the development of the operational capabilities of the armed forces of the Democratic People's Republic of Korea.'[108]

A final area of tension, is how to strike the balance between responding appropriately and effectively to security imperatives, not unduly restricting legitimate trade, whilst also not unduly restricting legitimate fundamental freedoms, such as freedom of expression via the

---

[103] The principle aim of "technology neutrality" is to "promot[e] statutory longevity and adap[t] the law to new technologies". In practice, however, it can be problematic, e.g., by being "over–inclusive and speak[ing] poorly to unforeseen technologies. It also, in turn, ... increases uncertainty about whether and how the law will be or should be applied". Greenberg, BA, "Rethinking Technology Neutrality" Minnesota Law Review (2016) 1495, 1562.

[104] An early case on technological neutrality in intellectual property law, regarding which ITT may overlap, is CBS Songs Ltd v Amstrad Consumer Electronics Plc (1988) UKHL15.

[105] S Bauer, K Brockmann, K, Bromley, M, and Maletta, G, "Challenges and Good Practices in the Implementation of the EU's Arms and Dual–Use Export Controls: A cross–sector analysis" (SIPRI, July 2017) 46, *at* <sipri.org/sites/default/files/2017–07/1707_sipri_eu_duat_good_ practices.pdf> (accessed 30 April 2018).

[106] Again, in intellectual property law terms, the case of *A&M Records, Inc. v. Napster, Inc.*, 239 F.3d 1004 (2001) illustrates well the perceived 'aggravated consequences' of peer–to–peer technology. See also Bauer et al (n 91) 9, also 38.

[107] García (n 12) 3–4.

[108] UN Doc S/2018/171 (5 March 2018) 47, specifically, its 'submarine–launched ballistic missile programme'.

Internet and other forms of social media.[109] There is a parallel concern to also ensure that exported 'dual-use' technology, such as for cyber-surveillance, is not misused to suppress and undermine human rights protections.[110]

E. Development of new framework of guiding principles/standards

The final proposal made here is for the possible development of a non-binding legal framework (such as guiding principles, or a Code of Practice) which could assist in progressing law and policy development on ITT and related issues, whilst also facilitating, or at least encouraging, greater consistency by States regarding their national approaches.

Certainly, at least historically, opportunities to develop such a framework have been missed, or at least not fully seized. For example, it may be time to put the idea of an International Code of Conduct on the Transfer of Technology, originally negotiated within the UN Conference on Trade and Development following the adoption of UNGA Resolution 32/88 (1977) and Resolution 32/45 (1977), back on the agenda.[111] Although it would not per se be binding or result directly in the criminalization of ITT related crimes committed by OCGs or TGs, it might assist in clarifying related international norms and complexities, as well as in paving the way for a legally binding instrument such as an additional protocol as proposed by this article.

For the development of such a framework, there are a number of existing legal sources which could be drawn upon, notably in the domains of intellectual property, competition and trade regulation, cyber security[112] and cyber financing, as well as terrorist financing and money laundering on which well-developed guidelines, principles, regulations and laws exist at the national, regional and international levels. For example, many of the principles and best practices developed regarding the appropriate use and monitoring of cyber space, tackling crime on the 'dark web' and curbing terrorist financing would be readily transferrable and adaptable to the ITT and related contexts.

In addition, there are a number of collaborative initiatives such as Europol's European Cybercrime Centre (EC3) which aims to assist and strengthen national law enforcement authorities in the EU Member States. These initiatives are identifying and developing good practices, sharing information and so forth which could also be drawn upon.

Conclusion

In conclusion, important gaps have been identified within the existing legal frameworks governing OCGs and TGs which pose significant threats to international peace and security in relation to the proliferation of both conventional and NCBR weapons as well as the increased potential to facilitate terrorist attacks of catastrophic proportions. Such gaps are

---

[109] Bauer, S, and Bromley, M, "The Dual–Use Export Control Policy Review: Balancing Security, Trade and Academic Freedom in a Changing World", EU Non–Proliferation Consortium, Non–Proliferation Papers No 48 (March 2016), *at* <sipri.org/sites/default/files/EUNPC_no–48.pdf> (accessed 5 April 2018).

[110] See, e.g., 'Export Controls: The Next Frontier in Cybersecurity?', Microsoft EU Policy Blog (13 April 2017), *at* <blogs.microsoft.com/eupolicy/2017/04/13/export-controls-the-next-frontier-in-cybersecurity/> (accessed 5 April 2018).

[111] See, e.g., Zuijdwijk, TJM, "The UNCTAD Code of Conduct on the Transfer of Technology" 24 *McGill Law Journal* (1978) 562.

[112] E.g., Council of Europe's Convention on Cybercrime, ETS No. 185, adopted Budapest 23 November 2001, came into effect 1 July 2004.

likely to widen in parallel with increased convergence between the two types of criminal groups as well as rapidly evolving technological advancements including on ITT related issues.

A number of concrete proposals have been made here as to how to plug these gaps both in the shorter and longer term. Ultimately, however, whether and to what extent such proposals are progressed is dependent on the existence of the requisite levels of political will, both nationally and internationally. As one commentator recently observed, in relation to security risks and challenges attributable to emerging technology including 3D printing:

> [T]he largest hurdle for comprehensive measures is a lack of political will. Most of these proposals would have adverse effects on the wider [additive manufacturing] industry and will thus probably not resonate well. […] [T]he political will to add [additive manufacturing] machines to dual-use control lists is anything but universal. For one, the technology advances in such a rapid pace […] that the export control regimes would constantly have to chase such developments and amend the control lists. But more importantly, there is no sense of urgency within the regimes, as [additive manufacturing] is still being considered as lacking the maturity for posing serious proliferation challenges. The overview provided in this Report over the technology's state of the art and its global diffusion should at least invite some questions as to whether this is still a valid assessment.[113]

Certainly, it is respectfully submitted here, that an urgent step-change is required, especially in the context of NBCR threats, from the current approach of 'encouraging' to 'requiring' States 'as appropriate, to control access to *intangible transfers of technology* and to information that could be used for weapons of mass destruction and their means of delivery'.[114] The livelihoods, wellbeing and perhaps very existence of many thousands, if not millions, of people may depend upon it.

*

[113] Fey (n 14) 33.
[114] See, e.g., UNSC Res 2325 (2016) para 13.