1

Security Agendas and International Law: the case of new technologies

NIGEL D. WHITE

> You will not apply my precept,' he said, shaking his head. 'How often have I said to you that when you have eliminated the impossible, whatever remains, *however improbable*, must be the truth?[1]

I. INTRODUCTION

'Security' as a concept would provide a serious challenge to Sherlock Holmes in terms of detecting any definite meaning, any core of truth within it. In terms of the international legal order, 'security' is not viewed as a legal principle but is seen as the 'primary' purpose of the principal inter-governmental organisation of the post-1945 legal and political order.[2] It is worth considering the relevant provisions of the UN Charter in greater detail because they contain within a tension between security and justice, by placing security (partly) within the framework of international law. Article 1 of the Charter declares that the purposes of the UN are:

1. To maintain international peace and security, and to that end: to take effective measures for the prevention and removal of threats to the peace, and for the suppression of acts of aggression or other breaches of the peace, and to bring about by peaceful means, and in conformity with the principles of justice and international law, adjustment or settlement of international disputes or situations which might lead to a breach of the peace;

[1] Sherlock Holmes to Doctor Watson in A Conan-Doyle, *The Sign of Four* (London, Penguin, 1982) 51, emphasis in original.

[2] *Certain Expenses of the United Nations* (Advisory Opinion) [1962] ICJ Rep 151 at 168 where the Court stated that 'the primary place ascribed to international peace and security is natural, since the fulfilment of the other purposes will be dependent upon the attainment of that basic condition'.

2. To develop friendly relations among nations based on respect for the principle of equal rights and self-determination of peoples, and to take other appropriate measures to strengthen universal peace;
3. To achieve international co-operation in solving international problems of an economic, social, cultural or humanitarian character, and in promoting and encouraging respect for human rights and for fundamental freedoms for all without distinction as to race, sex, language, or religion; and
4. To be a centre for harmonizing the actions of nations in the attainment of these common ends.

International lawyers tend to focus their attention on the principles of the UN Charter contained in Article 2, which include principles applicable to the UN, of sovereign equality and non-intervention, and duties upon states, primarily the obligation to settle disputes peacefully and the duty to refrain from the threat or use of force. However, article 1(1), is important for international law more broadly because it sets the UN the task of pursuing peaceful settlement of disputes in accordance with international law but, read literally, it does not subject the UN's collective measures taken to tackle threats to, or breaches of, the peace to the same legal framework. The prospect of UN security action unbound by international law runs like a red line through the Charter: the principle that the UN should not intervene in domestic affairs does not prejudice action taken by the Security Council under Chapter VII.[3] The ban on the use of force allows for only two exceptions – self-defence against an armed attack and military action taken to combat threats to and breaches of the peace as authorised by the Security Council under Chapter VII.[4] The content of the Charter seems to favour 'security', especially the collective coercive type found in Chapter VII, over 'law'.

The achievement of peace and security is the raison d'etre for the establishment of the UN, and international law is instrumental or secondary to that. However, paragraphs 2, 3 and 4 of Article 1 contain the basis for the development of a much more impressive legal architecture that could, potentially, provide a robust framework for security action by placing both the development of self-determination of peoples and the promotion of respect for individual human rights as purposes of the UN, alongside the achievement of peace and security. Within the human rights legal framework subsequently created by the UN in

[3] Article 2(7) UN Charter 1945.
[4] Articles 2(4), 51 and 42 of the UN Charter 1945.

instruments and treaties that followed the Charter,[5] freedoms and rights are curtailed by considerations of security, both national and human. While security was born free in 1945, it has gradually been shackled by legal constraints. However, those shackles are not strong enough to prevent the Security Council from behaving as if it remained unbound by international law.

Rather than focus this chapter on the Security Council, a topic covered in detail in many books and articles,[6] the focus will be on the shifting ground of security agendas and those communities established to deliver them. The chapter then considers whether this has involved the application or development of international laws to constrain potential threats, using the example of new technologies. Essentially, the chapter reviews whether, in the 21st century, the UN tackles new security threats in an executive manner through the Security Council, or whether it has (also) addressed these issues through legal frameworks and constraints. The relationship between security and law is one that is played out at all levels, from local, to national, to regional and then international. It is a delicate one – too greater emphasis on security erodes rights and freedoms and may lead to despotism, while too greater emphasis on law may prevent action necessary to tackle existential threats.

In the 1960s, international lawyers had come to view the 'harnessing of technology by public international institutions' as opening 'encouraging prospects for the control and direction of social change'. However, that view has changed so that today 'technology is no longer seen predominantly as promise but often rather a threat' and, furthermore, concern is widespread that the 'ability of public international organizations to manage technological change has been very limited'.[7] New technologies seem to be a long way ahead of specific legal regulation, especially at the international level where consensus is difficult to achieve, and yet, without such regulation, they represent possible threats to peace and security when, with effective legal controls, they have the potential to enhance both peace and security.

II. THE PROLIFERATION OF SECURITY AGENDAS

[5] Universal Declaration of Human Rights (adopted 10 December 1948) UNGA Res 217 A(III) and the International Human Rights Covenants of 1966.
[6] Eg V Lowe, A Roberts, J Walsh and D Zaum (eds), *The United Nations Security Council and War* (Oxford, Oxford University Press, 2010); ND White, 'The Security Council, the Security Imperative and International Law' in M Happold (ed), *International Law in a Multipolar World* (Abingdon, Routledge, 2012) 4.
[7] M Koskenniemi, *The Gentle Civilizer of Nations* (Cambridge, Cambridge University Press, 2002) 512.

Drawing on the work of the Copenhagen School, 'security' can be best understood as the absence of existential threats against states, other security actors, peoples and individuals.[8] The development of international relations to encompass 'collective security' and 'human security' has not meant that 'state security' is no longer important. What it does mean is that we have different, often competing, conceptions of security. Realist understandings of state or national security have prevailed for much of the twentieth century. The focus of Realism is on the safety of the nation-state, which results in placing national interests over collective interests and, thereby, national security over both collective security and human security, unless they coincide.[9] The Realist vision of security is still strong and has survived the Cold War confrontation between two heavily armed superpowers. Several factors can be pointed to explain its survival. Firstly, states clearly still represent threats to other states, particularly those possessing nuclear weapons or other weapons of mass destruction (WMD). Secondly, what were once mainly domestic threats, such as terrorism, have become transnational and, more generally, globalisation has led to internal security-focused politics becoming increasingly externalised.[10] This means that national security issues are increasingly played out on a global scale, as evidenced by the terrorist attack on the United States of 11 September 2001 that led the US to wage a 'war on terror', more specifically a war against al-Qaeda, impacting around the globe (as shall be seen below when 'drone wars' are considered).

Nonetheless, despite the continuing strength of national security, the concept of security has not only widened to include non-military threats, such as those arising from food or environmental insecurity, but has also deepened to encompass human security.[11] Richard Falk defines 'security' in a very 'human' way as the 'negation of insecurity as it is specifically experienced by individuals and groups in concrete situations'.[12] The focus of international debate is increasingly on human security, which has been defined to include 'economic, environmental, social and other forms of harm to the overall livelihood and well-being of individuals'.[13] Clear evidence of the widening understanding of security is found in the pivotal post-Cold War UN Security Council summit held in January 1992. As an organ

[8] B Buzan, O Waever and J de Wilde, *Security: A New Framework for Analysis* (Boulder, Lynne Rienner, 1998) 5.
[9] H Morgenthau, *Politics Among Nations* (A Knopf, 1972) 973.
[10] P Hough, *Understanding Global Security* (Abingdon, Routledge, 2008) 2.
[11] ibid 8.
[12] R Falk, *On Humane Governance: Toward a New Global Politics* (Polity, 1995) 147.
[13] FO Hampson, 'Human Security' in PD Williams (ed), *Security Studies: An Introduction* (Abingdon, Routledge, 2008) 229, 231.

that is built on Realist foundations, requiring agreement amongst its five permanent members (China, France, Russia, UK, and USA) for any substantive decision, the UN Security Council had hitherto almost exclusively concerned itself with state and military security. However, at its summit it declared that the 'absence of war and military conflicts amongst States does not itself ensure international peace and security' and that 'non-military sources of instability in the economic, social, humanitarian and ecological fields have become threats to peace and security'.[14]

As noted by Don Rothwell, the 'traditional view of security defines it in military terms with the primary focus on state protection from threats to national interests'. However, with the end of the Cold War, 'security discourse has expanded beyond the traditional military domain with the proliferation of security agendas including economic security, environmental security, food security, bio-security, health security and human security'.[15] As identified by Hitoshi Nasu, during the Cold War 'national security from external military attacks and threats was recognised as the ultimate raison d'etre of sovereign states'.[16] The Security Council supplemented this with the concept of international security in the post-Cold War period, evidenced by its authorisation to coalitions of willing states, starting with Coalition action against Iraq,[17] to undertake military actions to deal with threats to and breaches of international peace.

Attempts to understand security as a fixed concept fail to capture the securitisation of many aspects of daily life. Rather, security should be understood, according to the Copenhagen School, as a 'shared understanding of what is considered a threat'.[18] As Ronald Dannreuther explains, this reflects the turn towards 'constructivism' in the theorisation of security 'with its focus on subjective ideas and intersubjective understandings', which 'accords a greater weight of how ideas and perceptions influence and structure international reality'.[19] The constructivist approach of the Copenhagen School shifts 'attention away from an objectivist analysis of threat assessment to the multiple and complex ways in which security threats are internally generated and constructed'.[20] Furthermore, the Copenhagen

[14] UNSC 'Security Council Summit Statement Concerning the Council's Responsibility in the Maintenance of International Peace and Security' (31 January 1992) UN Doc S/23500.
[15] DR Rothwell, KN Scott and AD Hemmings, 'The Search for Antarctic Security' in AD Hemmings, DR Rothwell and KN Scott (eds), *Antarctic Security in the Twenty-First Century: Legal and Policy Perspectives* (Abingdon, Routledge, 2012) 3.
[16] H Nasu, 'Law and Policy for Antarctic Security' in Hemmings et al, ibid, 19.
[17] UNSC Res 678 (29 November 1990), UN Doc S/RES/678 (1990).
[18] ibid 25; Buzan, Waever and de Wilde (n 7), 23-6.
[19] R Dannreuther, *International Security: The Contemporary Agenda* (Polity, 2007) 40.
[20] ibid 42.

School moves the study of security away from the narrow confines of the Realist neo-scientist 'rationally calculating the multiple security threats', towards a more democratic construction of security based on shared understandings found in organisations, governments, civil society and other non-state actors, including individuals.[21]

The Copenhagen School identifies those objects that are existentially threatened as 'referent objects'.[22] The referent object for security has 'traditionally been the state and, in a more hidden way, the nation'. This signifies that 'for a state, survival is about sovereignty, and for a nation, it is about identity'. However, following the constructivist approach, 'securitising actors can attempt to construct anything as a referent object'.[23] For the Copenhagen School, the 'referent object' is traditionally the state, although with new security agendas developing all the time the object can be collective concepts, such as the environment or regions, such as Antarctica, and this is reflected in the UN Security Council's expansion of the concept of threat.[24] These ideas are very helpful in understanding the fact that security has expanded, although it remains largely state-centric, and that it is best viewed through a constructivist lens as being founded on inter-subjective understandings within legitimate fora, such as the UN Security Council, UN General Assembly, and regional organisations, such as the OAS, AU, EU, Arab League and ASEAN.

III. SECURITY COMMUNITIES AND THE ACHIEVEMENT OF AGREEMENTS

In 1957, Karl Deutsch, having considered various historical arrangements of states that had succeeded in removing conflict within their membership, defined a 'security community' as 'one in which there is a real assurance that the members of that community will not fight each other physically, but will settle their disputes in some other way'. He went on to say that 'if the entire world were integrated as a security-community, wars would be automatically eliminated'. By integration, he did not mean amalgamation into one state, rather the attainment of a 'sense of community and of institutions and practices strong enough and widespread enough to assure, for a long time, dependable expectations of peaceful change'.[25] 'Whenever states become integrated to the point that they have a sense of community' there

[21] ibid.
[22] Buzan, Waever and de Wilde (n 7) 36.
[23] ibid.
[24] Nasu (n 15) 25-6.
[25] K Deutsch, *Political Community and the North Atlantic Area: International Organization in the Light of Historical Experience* (Greenwood, 1957) 5-6.

is 'assurance that they will settle their differences short of war'.[26] Community building is a product of 'shared understandings, transnational values and transaction flows' and, once established, a security community generates stable expectations of peaceful change.[27]

Although the UN collective security organisation has not approached Karl Deutsch's concept of a security community, evidenced by the continuation of regular and frequent conflicts in the post-1945 world order, it has helped humankind to achieve the basic condition of any security community – survival.[28] There is evidence that the UN emerged from the Second World War as a form of 'security community' in order to consolidate the hard won peace by continuing the alliance that had defeated Germany and Japan. Ian Brownlie considered that the prosecution of the Second World War by the Allies against the Axis powers went beyond collective defence and became a war of sanction, the purpose of which was to remove a danger to world peace by extirpating the source of aggression. He stated that such a war of sanction in the UN period no longer has any place unless it is an 'organized community action'. Indeed, Brownlie views the prosecution of the Second World War as linking into the creation of the United Nations, even though the organisation was not formally created until the War's end, as the 'majority of states entered the war against the Axis Powers on the basis of the United Nations Declaration of 1942 and the Moscow Declaration of 1943'.[29] Following this line of argument, a security community was constituted in 1945 when the UN was established, but its origins can be traced back to 1942 when the Allied powers proclaimed themselves the 'United Nations' not only to defend themselves from Axis aggressors, but to defeat them completely and then shape a global peace.[30]

The UN certainly was a much improved collective security organisation when compared to the League of Nations, with the founding states of the UN collectively giving the smaller 'executive' or 'governing body', the Security Council of 15 states (increased from 11 in 1965), 'primary responsibility' in the realm of restoring or maintaining international peace and security.[31] The Security Council's powers are specified under Chapters VI and VII of the UN Charter, with the former containing a range of recommendatory powers in relation to the peaceful settlement of disputes or situations that might endanger the peace, including fact-

[26] E Adler and M Barnett, 'Security Communities in Theoretical Perspective' in E Adler and M Barnett (eds), *Security Communities* (Cambridge, Cambridge University Press, 1998) 4.
[27] ibid 4-6.
[28] Deutsch (n 24) 3.
[29] I Brownlie, *Principles of Public International Law*, 7th edn (Oxford, Oxford University Press, 2008) 332-3.
[30] But see JW Wheeler-Bennett and A Nicholls, *The Semblance of Peace: The Political Settlement After the Second World War* (Macmillan, 1972) 528-53.
[31] Article 24(1) UN Charter.

finding and recommending methods of adjustment or terms of settlement.[32] The powers contained in Chapter VII to demand provisional measures, such as cease-fires, to take a range of non-forcible measures, including economic sanctions, and to take military action,[33] are contingent upon the Council making a determination of a 'threat to the peace', 'breach of the peace' or 'act of aggression'.[34] The Security Council has adopted an expansive interpretation of 'threat to the peace' to include not only threats of force and threats to inter-state security, but also to cover internal violence and conflicts that have the potential to spill over into neighbouring states, as well as threats from terrorists and pirates.[35]

The concentration of power in the hands of the Security Council has led to a continuing debate as to where competence lies, if at all, if the Council is unable to act due to collective inaction or, as was the case during the Cold War, due to the pernicious use of the veto. While the voting rules of the Security Council were an improvement on the requirements of unanimity in the League of Nations' Covenant,[36] they still require consensus within the P5.[37]

The veto was so prevalent during the Cold War, cast primarily by the Soviet Union (who used its veto 77 times in the first 10 years of the UN) and later by the US, that the UN was often reduced to a bystander (as during the war in Vietnam 1959-75) or, at best, to a forum for diplomacy between the superpowers (for example during the Cuban Missile Crisis of 1962). The veto is evidence that the Security Council was not fashioned as an automatic 'instrument of action' rather, as Inis Claude pointed out, its basic function is as a forum for negotiation and diplomacy.[38] It follows that it is fallacious to argue that the UN had failed simply because it was unable to take action against the US and Soviet Union during the Cuban Missile Crisis. The UN still served as a forum for negotiation between the two superpowers, enabling both to climb down from their position of near nuclear confrontation. If the Council fails to fulfil even its basic function as a forum for diplomacy, then it can be argued that it has not carried out its primary role for the maintenance of international peace

[32] Articles 34, 36, 37, 38 UN Charter.
[33]Articles 40, 41, 42 UN Charter.
[34] Article 39 UN Charter.
[35] For example UNSC Res 1373 (28 September 2001) UN Doc S/RES/1373 (2001) re terrorism; and UNSC Res 1846 (2 December 2008) UN Doc S/RES/1846 (2008) re piracy. See generally C Henderson, 'The Centrality of the United Nations Security Council in the Legal Regime Governing the Use of Force', in ND White and C Henderson (eds), *Research Handbook on International Conflict and Security Law* (Elgar, 2013) 120.
[36] Article 5 Covenant of the League of Nations 1919.
[37] Article 27(3) UN Charter requires decisions to be 'made by an affirmative vote of nine [originally seven] members including the concurring votes of the permanent members'.
[38] I Claude, 'The Security Council' in E Luard (ed), *The Evolution of International Organization* (Thames and Hudson, 1966) 83-8.

and security, as placed upon it by the UN Charter,[39] and authority must therefore pass to another security community, either to the UN General Assembly or, arguably, to established and competent regional security organisations.

Having outlined security agendas and communities, this chapter now considers how the advent of new technologies has affected security and how the UN has responded to these developments by helping to shape a normative framework for regulating new technologies and for dealing with any emerging threats. At this stage, it should be reiterated that the response to new technologies should be a combination of normative development (by the General Assembly and other norm-making bodies within the UN) and executive action dealing with immediate existential threats. Although that executive action is not confined to responding to breaches of international law, the legitimacy of such action is enhanced if it does indeed amount to an enforcement of existing law.

IV. THE UN AS A SECURITY COMMUNITY ON NEW TECHNOLOGIES

Bearing in mind that a security community is not simply concerned with creating a normative framework within which to tackle disputes and threats, nonetheless it is surprising that, in general terms at least, the UN has struggled to produce a normative framework for new technologies. In other areas of international relations, UN soft law, in the form of declarations, has eventually led to UN hard law, in the form of binding treaties. This has happened in human rights law, environmental law and, to a more diffuse extent, arms control law, but we see little of this development as regards new technologies, for example on the issue of cyber security. It is not that the UN is unaware of the issue – in 1999, for instance, the General Assembly adopted a resolution calling upon states to 'promote at multilateral levels the consideration of existing and potential threats in the field of information security' and went on to invite states to inform the Secretary General on the advisability of 'developing international principles that would enhance the security of global information and telecommunications systems to help to combat information terrorism and criminality'.[40] The cagey language of this resolution reflects a profound disagreement between the membership of the UN, specifically within the P5 of the Security Council. As related by Mary Ellen O'Connell, Russia has promoted a treaty along the lines of the Chemical Weapons

[39] Article 24(1) UN Charter.
[40] UNGA 'Developments in the field of information and telecommunications in the context of international security' Res 53/70 (4 December 1998), UN Doc A/RES/53/70.

Convention to regulate cyberspace, which it viewed as a similar dual use issue – 'Russia's proposed treaty would ban a country from secretly embedding malicious codes or circuitry that could be later activated from afar in the event of war'. The US, however, differed in its approach following the success of the Stuxnet worm cyber-attack on Iran.[41]

It is difficult to construct a treaty or other legal regulatory mechanism that governs something as complex and multidimensional as the use of cyberspace. Achieving consensus on something that can be seen both as an important modern form of freedom of information and as a threat to security is one of the greatest challenges facing the UN. The item on 'developments in the field of information and telecommunication in the context of international security', first placed on the agenda of the General Assembly in 1999, has remained there as an annual item, though little progress has been made. In 2010, the General Assembly identified that there were a number of existing and potential threats in the field of information security. The Assembly urged states to develop 'strategies' to address 'threats emerging in the field, consistent with the need to preserve the free flow of information'. Intriguingly, the Assembly also considered that the 'purpose of such strategies could be served through further examination of relevant international concepts aimed at strengthening the security of global information and telecommunications systems'. The Assembly went on to invite states to look at the recommendations contained in the Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, in particular both the aforementioned 'concepts' as well as 'measures' that might be taken to strengthen information security.[42] Unfortunately, the Report did not develop the 'concepts' that might constitute a normative framework to shape the use of cyberspace. States' responses to the Assembly's request contain some discussion of relevant 'concepts'. The Australian government stated that 'existing international law provides a framework for protection from information security threats arising from a variety of actors', mentioning a range of existing international legal principles applicable to the use of cyberspace (sovereign equality, the prohibition on the use of force and international humanitarian law), but admitted that greater discussion among states was necessary to refine the scope of applicability of these principles to threats emanating from the cyber realm.[43] The United States stated that principles of the *jus ad bellum* and *jus in bello* were applicable, while the UK used the more modern terminology of the law governing the

[41] ME O'Connell, 'Cyber Security without War', (2012) 17 *Journal of Conflict and Security Law* 187, 205-6.
[42] UNGA Res 65/41 (8 December 2010) UN Doc A/RES/65/41.
[43] UN Disarmament Study Series 33, 'Developments in the Field of Information and Telecommunication in the Context of International Security' (UN, 2011), 22-23.

use of force and armed conflict.[44] A further Governmental Expert Group Reports has followed,[45] but with a similar lack of content that does not address the suggested limitations in state responses to laws governing the use of force and armed conflict. Such an approach narrowly confines security threats to cyber-warfare in a literal sense, when many non-kinetic cyber-operations and cyber-crimes do not reach that level and yet may still constitute security threats.

One problem is to convert new understandings of threats to security into legal concepts, principles and rules that together will shape a legal regime, the purpose of which is to enable organisations and states, and other security actors, to address such threats. One of the barriers to this is the way international law is divided into subject areas. New technologies raise concerns as a cross-cutting issue of security in a number of areas. General principles and specific norms from various specialist areas of international law may be applicable: arms control law, human rights law, international humanitarian law and international environmental law, to name the most obvious. However, when new technologies are used to destabilise states, such as cyber-attacks on another state's internet capabilities, as happened in Estonia in 2007, specialist legal regimes give way to discussions revolving around general principles of international law, such as non-intervention,[46] which can have limited traction in international affairs. Furthermore, the problems of identifying the origins of such attacks, moreover, of attributing such attacks in terms of state responsibility, adds to the problems of regulation. The strict rules on attribution of acts of private individuals to states, as embodied in the Articles on the Responsibility of States for Internationally Wrongful Acts of 2001,[47] as well as in the jurisprudence of the International Court of Justice,[48] do not assist in inducing states to stop the acts of private individuals that interfere in the security of other states. However, more recognition should be given to the underdeveloped general principle of due diligence found in international law, initially raised by the International Court of Justice in the *Corfu Channel* case in 1949 when it pointed to 'every State's obligation not to allow

[44] ibid 35-6, 56.
[45] UNGA Res 68/243 (27 December 2013) UN Doc A/RES/68/243; UN Doc A/68/98 (2013) paras 16-25. See further UN Doc A/66/359 circulated at the request of the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan, containing a draft international code of conduct for information security, which was subsequently co-sponsored by Kazakhstan and Kyrgyzstan.
[46] R Buchan, 'Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?', (2012) 17 *Journal of Conflict and Security Law* 212.
[47] Article 8 of which states that 'the conduct of a person or group of persons shall be considered as an act of State under international law if the person or group of persons is in fact acting on the instructions of, or under the direction or control of, that State in carrying out that conduct'.
[48] *Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America)* (Merits) [1986] ICJ Rep 14, 62-4; *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro)* (Merits) [2007] ICJ Rep 43, para 406.

knowingly its territory to be used for acts contrary to the rights of other States'.[49] At least this establishes that states have some positive obligations to prevent cyber-attacks being launched from their territories against other states, even though the territorial state might not be behind the attack.

Furthermore, within the UN there are a number of 'security communities': the 'hard' security community of the Security Council, with its mixture of executive and legislative competences; the 'softer' human rights focused competence of the General Assembly; and the specialist organs and regimes on matters such as disarmament, telecommunications, space, air and human rights. Often then, as regards new technologies, there is a lack of a clear UN 'security community' within which inter-subjective agreement can be forged.

More broadly, the role of science and technology in the context of international security and disarmament was added to the General Assembly's disarmament agenda in 1988. In introducing a draft resolution in the First Committee, the Indian delegate, in a remarkably prescient speech, recounted that increasing resources were being devoted to developing new weapons systems, such as the graduated use of nuclear explosive power, miniaturisation and large-scale computing capabilities, and fuel and laser technology, all of which were all transforming the security environment. He stated that because of these technological developments, work should be initiated to develop a shared perception of the problems involved and to make concerted efforts to resolve them.[50]

Thus, the UN had the opportunity at the outset of the upcoming Revolution in Military Affairs (RMA),[51] unleashed towards the end of the Cold War, to put in place some soft law. It must not be forgotten that the UN had responded to earlier technological revolutions by creating enduring legal regimes for airspace (following the huge growth of civilian aviation at the end of the Second World War)[52] and outer space in the 1950s and 1960s (in response to the launch of the first Sputnik satellite by the USSR and the imminent large scale utilisation of outer space).[53]

---

[49] *Corfu Channel Case (UK v Albania)* (Merits) [1949] ICJ Rep 4, 22.
[50] UN Office for Disarmament Affairs, 'The Role of Science and Technology in the Context of International Security and Disarmament' http://www.un.org/disarmament/topics/scienceandtechnology/.
[51] See generally CS Gray, *Strategy for Chaos: Revolution in Military Affairs and the Evidence of History* (Abingdon, Routledge, 2004).
[52] See Chicago Convention on International Civil Aviation 1944, laying down the principles of air law and constituting an effective regulatory organisation – the International Civil Aviation Organisation (ICAO).
[53] See UNGA Res 1962, 'Declaration of Legal Principles Governing the Activities of States in the Exploration and Use of Outer Space' (13 December 1963) UN Doc A/RES/1962 (XVIII); Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies (1967).

Unfortunately, the UN General Assembly did not seize the opportunity. The 1988 Assembly resolution requested that the Secretary General follow future scientific and technological developments, especially those which had potential military applications, to evaluate their impact on international security and to submit a report on this to the Assembly in 1990.[54] The Report of the Secretary General of 1990 was a product of meetings, reports and a conference involving scientific and other experts. It consisted of a general overview of technological advances and their implications for international security. Mention was made of 'mini-nukes', laser and particle beams, space technology, materials technology, information technology and biotechnology, but all of these were seen as 'evolutionary and largely incremental' rather than revolutionary.[55] In other words, these technological developments were viewed as developments of existing technologies and, therefore, the implication was that there was adequate existing regulation. Reference was made in the Report to existing arms control treaties, but little analysis of their inadequacies or gaps between them was made, which is suggestive of a lack of legal expertise in the compilation of the Report. Bearing in mind that the Report came at the end of the Cold War, the opportunity to start shaping new law was lost. Some statements in the Report show that new technologies or new developments in existing technologies would prove to be problematic, especially in the area of information technology, which was seen as 'extraordinarily pervasive technology' that could be harnessed by the military sector. 'Advanced computers', 'artificial intelligence' and 'robotics' were all envisaged in the Report, but their potential negative impacts were not considered, although the positive ones in terms of disarmament verification were.[56] The Assembly simply took note of the Report and vowed to give the matter on-going attention.[57]

The matter remains on the UN agenda, but normative development has not occurred. In 2007, the Assembly adopted a resolution that expressed concern about the development of unilateral export control regimes emplaced to prevent the export of dual use goods and technologies, which tend to impede the economic and social development of developing countries, urging the development of multilateral 'non-discriminatory guidelines for international transfers of dual-use goods and technologies and high technologies with military applications'. There was no consensus on this resolution.[58]

[54] UNGA Res 43/77A (7 December 1988) UN Doc A/RES/43/77A, 129-7 with 14 abstentions.
[55] UN Doc A/45/568 (1990), para 83.
[56] ibid para 65.
[57] UNGA Res 45/61 (4 December 1990) UN Doc A/RES/45/61, adopted without a vote.
[58] UNGA Res 61/55 (6 December 2006), UN Doc A/RES/61/55, 108-54 with 16 abstentions.

There is no doubt that outside the highly charged atmosphere of the UN's political organs, the UN does significant work on identifying and analysing new technologies. For example, the UN Institute for Disarmament Research (UNIDIR) has looked at existing legal frameworks for cyber war. A report by Nils Meltzer on 'Cyberwarfare and International Law' in 2011 is a good example, although the legal focus is again restricted to the *jus ad bellum* and the *jus in bello.* Clearly, these are important areas of law which, as Meltzer concludes, mean that 'the phenomenon of cyberwarfare does not exist in a legal vacuum, but is subject to well established rules and principles'. He goes on to say:

> That being said, transposing these pre-existing rules and principles to the new domain of cyberspace encounters certain difficulties and raises a number of important questions. Some of these questions can be resolved through classic treaty interpretation in conjunction with a good measure of common sense, whereas others require a unanimous policy decision by the international legislator, the international community of states.[59]

Meltzer perhaps understates the problem here – while the rules regulating the use of force and conduct of warfare may be applicable to cyber operations, they fail to capture their essence and, therefore, a great deal of cyber threats are not caught by those frameworks since they neither constitute the use of armed force nor are used in wartime. Thus, while the cyber operations that occurred during the Russian intervention in Georgia in 2008 were probably covered by the *jus in bello* and *jus ad bellum*, those conducted against Estonia in 2007 were not. The cyber operations of the type used against Estonia are more likely to be the norm than those conducted as an aspect of a military operation.

Although the *jus ad bellum* and *jus in bello* are important areas of law that act as possible constraints on what can be called cyber-warfare, the regulation of cyberspace at levels falling short of war, use of force, or armed conflict remains to be achieved. At this level, one might expect the legal framework to be centred on human rights law as the use of cyberspace not only raises security concerns, but also concerns about freedoms of thought, opinion and expression, and the rights to association and privacy. The way human rights law is structured, however, leads to problems of extraterritorial application of protection when a state interferes with the rights of citizens in another state. The UN Human Rights Council adopted a resolution on 'the promotion, protection and enjoyment of human rights on the

[59] N Meltzer on 'Cyberwarfare and International Law' (UNIDIR, 2011) 36.

internet' in 2012, which affirmed that the 'same rights that people have offline must also be protected online, in particular freedom of expression, which is applicable regardless of frontiers and through any media of one's choice' in accordance with common Article 19 Universal Declaration of Human Rights 1948 and International Covenant on Civil and Political Rights 1966.[60]

The UN General Assembly has also concerned itself with the use of the internet, but mainly from the perspective of inequality between developed and developing states in terms of access to and usage of the internet – what it terms a 'digital divide'.[61] Other UN agencies (for example the ITU, UNESCO) have the internet on their agenda, but from a more specialised or technical angle.[62] Little of this helps us to tackle the fact that freedom of expression, although guaranteed by human rights norms, can, by the very terms of human rights treaties, be subject to restrictions that are provided by law and necessary for the protection of 'national security'.

In its 1988 General Comment on Article 17 International Covenant on Civil and Political Rights (right to privacy) the Human Rights Committee stated that to be lawful interference with the right, the relevant national legislation must 'specify in detail the precise circumstances in which such interferences may be permitted'. Furthermore, a 'decision to make use of such authorised interference must be made only by the authority designated under the law, and on a case-by-case basis'.[63] This indicates that the sort of blanket covert surveillance of email and SMS messages undertaken in recent times by the US and UK is not in conformity with Article 17. Such jurisprudence has not stopped the massive trawling of internet traffic by the US (the National Security Agency's Prism Operation) or UK (GCHQ's Tempora Operation), nor, even more worryingly, does it appear robust enough to state clearly that such interference is unlawful. Both states have defended their actions as being lawful on the basis that they are necessary and proportionate counter-terrorism measures. This can be seen as an argument for 'security' prevailing over 'human rights' or, more accurately, that human rights are qualified and not absolute and allow for 'security' to be taken into consideration, but such arguments have to be tested and should not be accepted at face value.

[60] A/HRC/RES/20/8, 5 July 2012, adopted without a vote. See also A/HRC/RES/12/16, 2 Oct 2009, adopted without a vote.
[61] UNGA Res 66/184, 22 December 2011, UN Doc A/ UN Doc A/66/184, adopted without a vote. But see broader Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion or expression on the Internet UN Doc A/66/290 (2011); also UNGA Res 68/167 (18 December 2013) UN Doc A/RES/68/167, on the right to privacy in a digital age.
[62] ibid.
[63] Human Rights Committee GC 16, 8 April 1988, para 8. Interference, to be justified, also has to be 'proportionate' and 'necessary', *Antonius Cornelis Van Hulst v Netherlands*, HRC 2004, para 7.8 and 7.10.

V. DRONES, INTERNATIONAL LAW AND THE UN

With the odd exception, such as the regulation of outer space, international law tends to develop as a reaction to change. In this way it might be anticipated that new non-kinetic technologies that can be used to disable computer networks, or to carry mass covert surveillance of e-mail traffic, may take decades to bring within a clear legal framework, depending on how quickly states come to realise that it is in their mutual self-interest to effectively regulate cyber-space. It may, in any case, prove to be an impossible task as it raises the question of whether states can actually regulate something that has escaped the confines of sovereignty – it may simply be too late to put the genie back into the bottle. In this scenario, states will fall back on general principles of international law, such as the norm prohibiting intervention in a state's political or economic affairs, which will not prevent cyber operations but will enable selective condemnation in the General Assembly and, occasionally, executive responses to particular threats by the Security Council.

However, when it comes to new technologies that seem to provide straightforward improvement in military efficacy, such as Unmanned Aerial Vehicles (UAVs), commonly known as drones, it should be expected that existing international law will be adequate. Indeed, this is quite commonly the argument made in the literature, given that drones are seen as mere 'platforms' for the launch of weapons such as missiles and not new weapons per se.[64] Furthermore, drones are portrayed by their users and supporters as upholding the value of security rather than undermining it.[65] Nonetheless, the increasing use of drones does raise security concerns for a number of reasons. When they are used for surveillance they are potential threats to personal security and privacy. When used for targeting purposes they not only raise security concerns for civilians potentially caught in the blast (the problem of collateral losses), but they also seem to either extend the battlefield, thereby bringing the instability inherent in war, or constitute the extraterritorial application of force for the purposes of some extreme form of law enforcement. Under this model of law enforcement, capture, arrest and trial are replaced by summary execution. All of these conceptions of

[64] D Turns, 'Droning On: Some International Humanitarian Law Aspects of the Use of Unmanned Aerial Vehicles in Contemporary Armed Conflicts', in C Harvey, J Summers and ND White (eds), *Contemporary Challenges to the Laws of War* (Cambridge, Cambridge University Press, 2014) 199.
[65] For critical evaluation see C Gray, 'Targeted Killings: Recent US Attempts Obama to Create a Legal Framework' (2013) *Current Legal Problems* 1.

drone use challenge the notion that they represent a new era of clean, clinical and legitimate use of force.

Drones are being increasingly used for surveillance, normally as part of domestic law enforcement operations. As with the exponential growth of surveillance cameras generally, the usage of drones is accepted as a benign and acceptable form of security. As is oft-stated by politicians and law-abiding citizens, 'if you're not doing anything wrong, there is no reason to object' to such surveillance.[66] Indeed, it is possible to see such measures as upholding basic rights. Both the International Covenant on Civil and Political Rights 1966 and the European Convention on Human Rights 1950 guarantee the 'right to liberty and security of person'.[67] Surveillance in order to stop crime, especially violent crime, can be argued to be an aspect of a government's positive duties to prevent human rights violation and provide security. Indeed, there is plenty of jurisprudence that allows the state a wide margin of appreciation for secret surveillance, as a measure 'necessary in a democratic society in the interests of national security',[68] provided that there are measures in place to prevent abuse.[69] Nonetheless, this conception of security can lead to a very intrusive state where the prioritisation of security in all aspects of life erodes other rights and freedoms expected in a democratic society, for example, the right to privacy.[70] The European Court of Human Rights has provided a general definition of privacy, which should raise concerns about the growing use of state surveillance, including by drones. According to the Court, privacy includes a 'zone of interaction of a person with others, even in a public context, which may fall within the scope of "private life"'. In addition, the Court opined that a 'person's reasonable expectations as to the privacy may be a significant, though not necessarily conclusive factor' to be considered when determining whether a person's private life is affected by measures taken outside a person's home or private premises.[71]

Despite this tentative protection of public spaces from state intrusion, it must be born in mind that a margin of appreciation is found within the definitions of the rights themselves.

---

[66] William Hague, UK Foreign Secretary, stated in 2013 that 'If you are a law-abiding citizen of this country going about your business and your personal life you have nothing to fear – nothing to fear about the British state or intelligence agencies listening to the contents of your phone calls or anything like that', 'Prism: Claims of GCHQ Circumventing law are "Fanciful Nonsense", says Hague', *The Guardian*, 9 June 2013.
[67] Article 5 Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended) (ECHR); Article 9(1) International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171 (ICCPR).
[68] *Klaas and others v Germany* (ECtHR 6 September 1978) para 451.
[69] L Doswald-Beck, *Human Rights in Times of Conflict and Terrorism* (Oxford, Oxford University Press, 2011) 451.
[70] Article 8(1) ECHR; Article 17(1) ICCPR.
[71] *Gillan and Quinton v United Kingdom* Judgment, 12 January 2010, para 61.

For instance, in protecting the right to a 'private life' the European Convention goes on to declare that 'no interference with the exercise of this right' by the government is permitted except 'in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of rights and freedoms of others'.[72] Perceptions and assertions of security by governments are difficult for the courts to resist, particularly in times of terrorism that are characterised by random attacks against civilians, even when government actions to protect the lives and security of its citizens may appear to tread on the very freedoms it is fighting to protect. Due diligence obligations upon governments are obligations of conduct, rather than result, and so a failure by government to prevent specific acts of terrorism is not necessarily an indication that the state has failed to fulfil its duties under human rights law. The random nature of many terrorist actions means that it is very difficult to prevent each and every one. When considering how these obligations have been interpreted by the Human Rights Committee in the context of the rights to life and security under the International Covenant on Civil and Political Rights,[73] it is clear that states must take reasonable and appropriate measures to protect individuals within their jurisdiction who are subject to known threats to their lives.[74] The European Court of Human Rights has similar jurisprudence, stating in one judgment that a government that 'knew or ought to have known … of a real and immediate risk to the life of an identified individual or individuals from the criminal acts of a third party', must take 'measures within the scope of their powers, which, judged reasonably, might' be 'expected to avoid that risk'.[75] As has been stated in reviewing this jurisprudence:

> Applying this jurisprudence by analogy to terrorist attacks creates some challenges: the bombing of civilians on aircraft or commuter trains and the hijacking of aircraft suggests a random choice of victims, rather than the selection of an 'identified individual or individuals' as victims.[76]

When drones are used outside of a state's jurisdiction, whether for surveillance or for targeting purposes, and when lethal force is used against individuals, the human rights issues

[72] Article 8(2) ECHR.
[73] Articles 6 and 9 ICCPR.
[74] *Delgado Paez v Columbia,* Human Rights Committee Communication No 195/1985, 12 July 1990, para 5.5.
[75] *Osman v United Kingdom* (1998) 29 EHRR 245.
[76] ES Bates, *Terrorism and International Law: Accountability, Remedies and Reform* (Oxford, Oxford University Press, 2011) 83-4.

become more complex. While human rights obligations apply to individuals within a state's territory, there is considerable debate about when they apply to individuals outside its territory but, arguably, within its jurisdiction. When considering the use of armed force from a drone against a terrorists suspect, the question is whether the individual is within the jurisdiction of the state using force. Although there is some Inter-American case-law that supports the application of the right to life in these circumstances,[77] there is contrary European jurisprudence.[78] Rather than considering whether the state using force has enough control over the targeted individual for the purposes of evaluating whether there is an assertion of jurisdiction in these circumstances, it would be better for the Courts to focus on the fact that the operator of the drone, often a distance away from the target, is clearly under the control of the state using force.[79]

If jurisdiction is established, such uses of targeted force from drones, when taken outside of armed conflict, are violations of the right to life as there is usually no imminent threat to the state to justify its use of force as a last resort.[80] Indeed, the use of lethal force from drones seems to be an extreme and, paradoxical as it may sound, unlawful version of law enforcement where it is easier to kill suspects than to capture them (particularly as capturing suspects would put them clearly within the capturing state's jurisdiction).[81]

Furthermore, the use of drones for targeting suspected terrorists appears to be an attempt to externalise a state's security measures to counter terrorism by taking out targets in another state's territory before they have chance to hit the drone state's territory or nationals. The US has tried to justify this by arguing what is the ultimate justification for using lethal force – that there is a global armed conflict against terrorists or, at the very least, a transnational armed conflict against Al Qaeda and its associates. This argument is an attempt to justify a lower standard for when lethal force can be used as, in simple terms, a use of lethal force is allowed in an armed conflict if the target is either a military objective, a combatant, or a civilian who is directly participating in hostilities, and the anticipated collateral damage ('incidental loss of civilian life') is not excessive in relation to the expected

[77] *Armando Alejandre Jr, Carlos Costa, Mario de la Pena and Pablo Morales v. Cuba (Brothers to the Rescue)*, Case 11.589, Report No. 86/99, 28 September 1999, para. 25.
[78] *Bankovic and others v. 17 NATO States*, Admissibility Decision (Grand Chamber), 12 December 2001, paras. 52-3.
[79] F Hampson, 'The Scope of the Extra-Territorial Applicability of International Human Rights Law' in G Gilbert, F Hampson and C Sandoval (eds), *The Delivery of Human Rights: Essays in Honour of Sir Nigel Rodley* (Abingdon, Routledge, 2011) 181-2.
[80] P Alston, 'Study on Targeted Killings', Report to the Human Rights Council, UN Doc A/HRC/14.24/Add.6 (2010) paras 85-6.
[81] *Ocalan v Turkey* App No 46221/99 (ECtHR, 12 March 2003) para 125.

military advantage.[82] The US has interpreted these rules liberally: to carry out 'signature' strikes on the basis that the targeted individual is performing suspicious activities; to target funerals where there is a concentration of Taliban leaders; to target drug lords (who are criminals not combatants); and sometimes to order strikes outside of a conflict-zone, for example, in Yemen in 2002 and again in 2011.[83]

It seems that after the devastating attacks on the US of 11 September 2001, governments (and not just the US) have re-assessed their security priorities, have reasserted national security (often on the basis that this is the best way to protect human security) and have acted in violation of basic norms governing when coercion can be used by the state against individuals to protect the majority of its citizens. This has either been as a result of the extension of the battlefield or the extension of law enforcement. While the majority of states may support this, or, more accurately, remain supine in the face of these erosions, the securitisation of post-9/11 life has meant that (the right to) security has been elevated to a pre-eminent position in political rhetoric and action in contradistinction to its position as one of a number of human rights and protections provided by international law.[84]

Thus, while there are international norms applicable to drone use, a great deal of it is underdeveloped, indeterminate or ineffectual. The UN itself has not tackled drone usage in any meaningful way. Although this is probably to be expected in the executive body, it is disappointing to see that the plenary body has also failed to fulfil its functions as a security community with the ability to shape normative frameworks, confining itself instead to exhortation in general resolutions to the effect that counter-terrorism efforts by states should be undertaken in conformity with international human rights law, refugee law and international humanitarian law.[85]

VI. CONCLUSION

The UN system has confronted the issue of new technologies since the late 1980s, but has made limited progress on either consolidating applicable law or developing new laws and mechanisms. The fact that new technologies bring in aspects of many areas of policy and law

[82] Article 55, Additional Protocol I 1977; Turns (n 62) 207.
[83] S Casey-Maslen, 'The Use of Armed Drones, in S Casey-Maslen (ed), *Weapons under International Human Rights Law* (Cambridge, Cambridge University Press, 2014) 400-3.
[84] See generally L Lazarus, 'The Right to Security – Securing Rights or Securitising Rights?' in R Dickinson, E Katselli, C Murray and OW Pederson (eds), *Examining Critical Perspectives on Human Rights* (Cambridge, Cambridge University Press, 2012) 87.
[85] Eg UNGA Res 68/178 (18 December 2013) UN Doc A/RES/68/178.

– arms control, human rights, conflict, peace and security – means that specific frameworks need to be shaped by the UN Security Council, General Assembly, Secretary-General and other UN bodies. The uncertainty as to how to accommodate different security agendas within the framework of international law produces its own insecurity, so that we are caught in what appears to be a spiralling security dilemma in which one state's uncensored increase in security measures leads another state to increase theirs to a point where they feel more secure, which, in turn, leads the first state to further increase their security preparation. Clarification of the applicable law and law-making can, of course, take place outside the UN, but as such it will be uneven, piecemeal and will lack the universality and legitimacy that the UN brings. The ever-growing use of cyber measures and drones are just two examples of how technology is outstripping law. We make not be able to determine the truth as to the legal meaning of 'security' in a logical Holmesian manner, but we should be able to achieve agreement on what it means in the case of new technologies.