How Effectively does the United Nations Security Council Regulate the International Use of Force?

Josephine Carver

Leicester Law Review
Spring 2018

After the atrocities of World War I and II, the victor states ratified the United Nations Charter in 1945 creating the UN Security Council to prevent such grave conflict from ever repeating itself. Fast forward to 2018 and the type of conflict has significantly changed. 'World War' appears to be a relic of the past and states now use 'force' by alternative means to achieve their goals. This article critically examines the effectiveness of the United Nations Security Council in regulating the international use of force and its ability to adapt to new landscapes and types of conflict. The UN Security Council's most important articles, Article 2(4) and Article 51, are critically analysed in an effort to identify how states may sidestep the prohibition on the use of force, without a UN Security Council mandate. Current examples from the past decade are used to highlight the Security Council's lack of control in the international cyber-sphere and analyse how sufficiently grave cyber-attacks may prompt future armed conflict.

The United Nations Security Council was formed in 1945 when the victors of World War II ratified the United Nations Charter 'to save succeeding generations from the scourge of war' and 'to unite our strength to maintain international peace and security'.[1] However, the landscape and type of war has significantly changed since 1945 and the Security Council's ability to adapt to this is disputable. This article will examine how effectively the Security Council upholds and enforces the prohibition on the use of international armed force, contained in Article 2(4) of the United Nations Charter.[2] The exceptions to Article 2(4),[3] including the Article 51 right to self-defence, arguing implied authority,[4] interpretive issues posed by Article 2(4) and the use of non-traditional cyber force, will be used to demonstrate states' abilities to sidestep Article 2(4) and pursue their own agendas.[5] The United States' arguable abuse of the right to self-defence after 9/11, the alleged Russian interference in the 2017 US Presidential election and international cyberattacks on Estonian government facilities and Sony will be used to highlight the Security Council's lack of international control.[6] The article will conclude that the collective nature of the United Nations (UN), a fundamental goal of the UN Charter, no longer exists and states simply pursue their own agendas making the Security Council a redundant feature of the United Nations.[7]

The law of international cooperation and coexistence stems from the 1945 UN Charter. Its creators sought to uphold international peace and security, and to avoid another major conflict after World War II. The Charter seeks to collectivise the use of force through Article 2(4):

> all members of the UN shall refrain from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations.[8]

[1] United Nations Charter 1945, Preamble.
[2] United Nations Charter 1945.
[3] ibid.
[4] ibid.
[5] ibid.
[6] United Nations Charter 1945, Article 51.
[7] United Nations Charter 1945.
[8] United Nations Charter 1945, Article 2(4).

Waxman explains the interpretive issues posed by Article 2(4):[9] 'the paragraph is complex in its structure, and nearly all of its key terms raise questions of interpretation', in his journal on international cyber-attacks.[10] There is much academic debate on the definition and scope of 'force' and how it may threaten the 'territorial integrity' and 'political independence' of a state. Is 'force' limited to just physical force? The dominant view is that the prohibition of force and the right to self-defence under Article 51 apply to physical armed force only.[11] This is supported by the preamble to the Charter which states that 'armed force shall not be used save in the common interest'.[12] The word 'armed' suggests that only soldiers marching on the ground, bombing campaigns and general kinetic force would be prohibited under Article 2(4). Cyber-interference such as hacking email accounts, disrupting government operations or the collection of information through cyber espionage could not be defined as 'armed' force. This argument is so dominant because the UN Charter was ratified in 1945 and so the creators could not have foreseen the emergence and effectiveness of non-traditional cyber-force, economic and political coercion and alternatives to the type of World War conflict seen before. However, when deciding which interpretation to follow one should consider whether the initial aims of the Charter should prevail or whether the Charter should be interpreted to adapt to current international conflict and alternative means of 'force'.

An alternative interpretation is that Article 2(4) broadly prohibits coercion in any form. The Soviet Union attempted to advance this theory during the Cold War, arguing that 'force' includes forms of pressure like economic and political coercion that threatens state autonomy and territorial integrity, referenced in Article 2(4).[13]

The third interpretation offered is that Article 2(4) and Article 51 prohibit any violation of a state's sovereignty.[14] It can be argued that one of the fundamental aims of Article 2(4) was to uphold state sovereignty and this should be followed even if the means to which territorial integrity may be threatened, have changed since 1945. As such, any illegitimate interference with states' rights, including cyber interference in the sovereignty of a state would be prohibited.

The Charter gives the Security Council principal responsibility for the maintenance of international peace and the power of authorisation for a state's use of force. Article 25 outlines the member states' obligation to carry out the decisions of the Council and Article 39 grants the Council the sole power to determine the existence of 'any threat to the peace, breach of the peace, or act of aggression'.[15] Article 42 gives the Security Council the authority to mandate 'such action by air, sea, or land forces as may be necessary', where non-enforceable measures, contained in Articles 40 and 41, are insufficient.[16] This is the first exception to the prohibition on the use of force.

The second exception to the prohibition in Article 2(4), is the right to self-defence found in Article 51: '[n]othing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member State of the United Nations'.[17] Self-defence can be exercised individually by a state, or collectively by a group of states upon request by the victim state.[18] The requisite legal conditions are that the force taken in self-defence must be necessary and proportionate, but it does not require prior Security Council authorisation due to the presumed urgency of a situation where the right to self-defence would arise. The scope of this Article is one of the most contested areas of international law because, like Article 2(4),[19] it poses several questions about interpretation, including what defines an 'armed attack', the level of intensity required, and whether private actors may commit an armed attack. In the *Nicaragua* case,[20] the International Court of Justice outlined possible definitions of an armed attack:

> 'It may be considered to be agreed that an armed attack must be understood as including not merely action by regular armed forces across an international border, but also the sending by or on behalf of a State of armed bands, groups, irregulars or mercenaries, which carry out acts of armed force against another State of such gravity as to amount to an actual armed attack…'

It is now widely accepted that private actors, such as the Al Qaeda terrorist organisation, may perpetrate an armed attack, triggering a right to self-defence against these private actors. However, the right to self-defence is conditioned on the 'unwilling or unable' doctrine, whereby the victim state may only take self-defence action against the private actor if their host state is unwilling or unable to stop the private actor.

The duration for which this right to self-defence exists is also a contested issue. The US responded to the 9/11 attacks with the emergence of the pre-emptive self-defence doctrine, dubbed the 'Bush doctrine' by the media and academics. The US has used this defence to justify over a decade of force and many academics argue that the right to self-defence was extinguished when the leader of the Al Qaeda movement, Osama bin Laden, was killed in 2011. The US has arguably used their right to self-defence to sidestep the Article 2(4) prohibition on the use of force in order to pursue their own military agenda, without a United Nations Security Council mandate.[21]

Additionally, states have been able to sidestep Article 2(4) by arguing that they have implied authority

[9] United Nations Charter 1945.
[10] Matthew Waxman, *'Cyber attacks and the Use of Force: Back to the Future of Article 2(4)'* (Yale Journal of International Law 2011).
[11] United Nations Charter 1945, Article 51.
[12] United Nations Charter 1945.
[13] ibid.
[14] ibid.
[15] ibid.
[16] ibid.
[17] United Nations Charter 1945, Article 51.
[18] The North Atlantic Treaty 1949, Article 5.
[19] United Nations Charter 1945.
[20] *Nicaragua* v *United States of America* [1986] ICJ 1.
[21] United Nations Charter 1945.

from the UN Security Council.[22] This was evident when the US and the UK invaded Iraq in 2003. The Security Council had implemented sanctions for Iraq's failure to work with UN weapons inspectors for over ten years. The Council then implemented a renewed inspection regime through Resolution 1441 which Iraq did not comply with, yet again.[23] The US and UK interpreted this as further evidence that Iraq was uncooperative, giving rise to the notion of implied authority from the Security Council to use force against Iraq. Thus, the US and UK invaded Iraq using armed force without a clear Security Council mandate. Similarly, in March 2011, the Security Council authorised the establishment of a 'no-fly-zone' over Libya and the use of 'all necessary measures' to protect civilians in response to the Muammar Gaddafi regime. Following the 'Arab Spring' uprisings from 2010 to 2011, Gaddafi used chemical weapons against his civilians which President Obama had previously stated would be crossing a 'red line.' NATO used this UN authorisation to justify its lengthy bombing campaign that led to the collapse of the Gaddafi regime, but several states, including China and Russia, argued that this exceeded the bounds of the mandate. This demonstrates the breakdown of the 'collective' nature of the UN Security Council as states largely followed their own strategies due to the ambiguity of 'all necessary measures.' The UN Security Council appears redundant because it failed to limit or define the level of force permitted by 'all necessary measures' that caused other states to dispute the legitimacy of NATO's actions.

The use of force in cyberspace is another grey area that lacks sufficient regulation by the Security Council. This largely unregulated area allows for the use of non-traditional force through cyber means, which can have equally devastating effects to that of physical force. The traditional reading of Article 2(4) interprets force as kinetic or physical force, as aforementioned.[24] However, there have been several cyber-attacks that should arguably fall under the legal scope of force under Article 2(4).[25] Firstly, during diplomatic tension between Estonia and Russia in 2007, cyber-attacks on Estonia significantly disrupted government and commercial operations.[26] Similarly, the computer code, Stuxnet, allegedly created and operated by the US or Israel, significantly damaged Iran's uranium programme between November 2009 and January 2010.[27] Whilst lives were not lost during these attacks, they clearly demonstrate the destructive nature of cyber force.

Furthermore, the alleged Russian interference in the 2016 US Presidential election is an example of cyber espionage interfering in the 'political independence' of a state, which would be prohibited under the third reading of Article 2(4) aforementioned.[28] The hackers group Fancy Bear, believed to be closely aligned with the Russian government, hacked the email account of Hillary Clinton's campaign manager, John Podesta, and passed confidential emails to WikiLeaks for publication, in an attempt to influence the outcome of the election. The emails covered several damning topics including suggestions that big corporations were able to buy access to the former President, Bill Clinton, private comments about Hillary Clinton's 'poor instincts' from the inner-circle of the campaign team, claims of a Justice Department 'collusion' and further confidential information. This may have influenced the US electorate since the leaked information likely damaged Clinton's reputation and character. Therefore, this is arguably a violation of US state sovereignty because the US should be able to conduct free and fair elections without outside undue influence from Fancy Bear and the Russian government.[29] This demonstrates how the type of conflict has significantly changed since 1945 as states can threaten another state's autonomy and territorial integrity by cyber means. There was no physical 'force' involved in any of these incidents proving the damaging effects of cyber-force and its ability to threaten international peace. The UN Security Council did not take action in any of these incidents proving its lack of international control in the cyber-sphere and its outdated role as international peacekeeper.

Moreover, there is not a clear international legislative authority on whether cyber-attacks may trigger a right to self-defence. It can be argued that if a cyber-attack may amount to an "armed attack" under Article 2(4), then there should be a right to responsive self-defence under Article 51.[30] In 2014, Sony Pictures Entertainment reported it had been the victim of a cyber-attack that damaged systems and stole personal and commercial data. The group 'Guardians of Peace' claimed responsibility for the attack and stated that it was in response to the production/screening of *The Interview*, a political comedy that mocked the North Korean regime under Kim Jong Un. The group threatened Sony, various cinemas and any individual that sought to watch the film. The US responded by implementing serious sanctions against North Korean government officials and the defence industry, despite North Korea denying any involvement.[31] This was the first time that a state officially recognised a cyber-attack and adopted counter measures. This was a relatively low level cyber-attack and so it would not be considered grave enough to constitute an 'armed attack' and prompt a right to self-defence.[32] However, the use of responsive smart sanctions by the US demonstrates how seriously states view cyber-attacks. This raises the question of whether sufficiently grave cyber-attacks in the future may prompt a victim state to take physical self-defence force for which they technically would not need Security Council permission. Thus, this

[22] ibid.
[23] European Council Resolution 1441 [2003].
[24] United Nations Charter 1945.
[25] ibid.
[26] Damien McGuinness, 'How a cyber-attack transformed Estonia' (*BBC*, 27 April 2017) <http://www.bbc.com/news/39655415> accessed 15 January 2018.
[27] Kim Zetter, 'An unprecedented look at Stuxnet, the world's first digital weapon' (*Wired*, 11 March 2014) <https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/> accessed 20 January 2018.
[28] United Nations Charter 1945.
[29] '18 revelations from Wikileaks' hacked Clinton emails' (BBC, 27 October 2016) <http://www.bbc.com/news/world-us-canada-37639370> accessed 21 January 2018.
[30] United Nations Charter 1945.
[31] Andrea Peterson, 'The Sony Pictures hack, explained' (*The Washington Post*, December 18 2014) <https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained/?utm_term=.e9d0ba2a436b> accessed 21 January 2018.
[32] United Nations Charter 1945, Article 2(4).

demonstrates how the UN Security Council will not be able to control future conflict within the international cyber-sphere prompting physical armed force.

Waxman argues that the lack of state action on regulating this area stems from states aligning legal line-drawing with strategy. States are reluctant to condemn cyberattacks and implement legal regulation in this area because they will, first and foremost, pursue their own agenda.[33] This was shown by then President Obama opting not to publicly condemn the Clinton email hacking as cyber-espionage because the US pursues its own cyber espionage programme and would not want to curtail this.[34] Several states, including China, see cyber tools as a means of levelling the power playing field where states may lack in military force, but will compensate with cyber force.[35] The UN Charter is arguably outdated and the Security Council is redundant in this area because it fails to regulate and prohibit the use of cyber force interfering in the political independence and territorial integrity of a state.

In conclusion, the United Nations Security Council is currently an ineffective regulator of states' use of force. The dominant outdated interpretation of Article 2(4) defines 'force' as armed kinetic force only.[36] This allows states to sidestep the prohibition on the use of force by using non-traditional means in the cyber-sphere that can equally threaten state autonomy and territorial integrity. Article 2(4) needs to adapt to the changing landscape of conflict if the UN Security Council wishes to be an effective international peacekeeper. Similarly, ambiguous terms in Article 51 have allowed states to pursue their own agenda and use force without a clear Security Council mandate.[37] The cyber-sphere desperately needs international regulation if the Security Council wants to maintain international peace and that using force should be a last resort.

Bibliography

Primary Sources

Table of Cases

Nicaragua v United States of America [1986] ICJ 1

Table of Legislation

United Nations Charter (1945)

North Atlantic Treaty (1949)

Secondary Sources

Journal Articles

Henriksen A, 'Jus ad bellum and American Targeted Use of Force to Fight Terrorism Around the World' (2014) Journal on the Conflict and Security Law

Henriksen A and Schack M, 'The Crisis in Syria and Humanitarian Intervention' (2014) Journal on the Use of Force and International Law

Henriksen A, 'Lawful State Responses to Low-Level Cyber Attacks' (2015) Nordic Journal of International Law

Henriksen A, 'Politics and the development of legal norms in cyberspace' (2016) Routledge

Waxman M, 'Cyber attacks and the Use of Force: Back to the Future of Article 2(4)' (2011) Yale Journal of International Law

Internet Sources

Damien McGuinness, 'How a cyber-attack transformed Estonia' (BBC 27 April 2017) <http://www.bbc.com/news/39655415> accessed 15 January 2018

Kim Zetter, 'An unprecedented look at Stuxnet, the world's first digital weapon' (*Wired,* 11 March 2014) <https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/> accessed 20 January 2018

'18 revelations from Wikileaks' hacked Clinton emails' (BBC, 27 October 2016) <http://www.bbc.com/news/world-us-canada-37639370> accessed 21 January 2018

Andrea Peterson, 'The Sony Pictures hack, explained' (*The Washington Post,* December 18 2014) <https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained/?utm_term=.e9d0ba2a436b> accessed 21 January 2018

Aruna Viswanatha and Joseph Menn, 'Obama's response to the Sony hack says a lot about US cyber policy' (*Business Insider,* January 14 2015) <http://www.businessinsider.com/r-in-cyberattacks-such-as-sony-strike-obama-turns-to-name-and-shame-2015-1?r=US&IR=T&IR=T> accessed 15 January 2018

[33] Matthew Waxman, '*Cyber-attacks and the Use of Force: Back to the Future of Article 2(4)*' (Yale Journal of International Law 2011).

[34] Aruna Viswanatha and Joseph Menn, 'Obama's response to the Sony hack says a lot about US cyber policy' (*Business Insider,* January 14 2015) <http://www.businessinsider.com/r-in-cyberattacks-such-as-sony-strike-obama-turns-to-name-and-shame-2015-1?r=US&IR=T&IR=T> accessed 15 January 2018.

[35] Matthew Waxman, '*Cyber-attacks and the Use of Force: Back to the Future of Article 2(4)*' (Yale Journal of International Law 2011).

[36] United Nations Charter 1945.

[37] ibid.