Research Article

Cyberwarfare and the Challenges it Poses to the International Governance of Armed Conflict

Hannah Gray[1*]

Received: 24 January 2024 / Accepted: 2 August 2024

Abstract

Cyberwarfare is an emerging form of conflict in the 21st Century. Whether it is considered a domain, a field of weaponry, or capable of being a completely new and separate type of conflict, the international governing community must find a way to protect citizens from its potential damage. International law may be able to do so. Still, there are plot holes in existing international law governing armed conflicts involving cyber-attacks, particularly regarding attributability, distinction, and self-defence. This paper uses two case studies, the 2008 Russo-Georgian War and the ongoing Russia-Ukraine War, to discuss the practical application of international law to cyber warfare.

Keywords cyber warfare • International law • armed conflicts • attributability • cyber-attacks

INTRODUCTION

Cyberwarfare is arguably a 'fifth domain' of warfare following land, sea, air, and space.[2] Given this and its relative novelty in the legal areas of armed conflict, it is important to understand the challenges it presents to its governance by international law. Several

[1] Hannah Gray graduated with a First Class Honours degree in International Relations and International Law at the University of Edinburgh. Having developed an interest in the governance of emerging security issues and how these relate to migration and human rights, she is hoping to pursue a masters in international security in Europe.
[2] Mohan B. Gazula, 'Cyberwarfare Conflict Analysis and Case Studies'. *Cybersecurity Interdisciplinary Systems Laboratory (CISL), Sloan School of Management,* MIT (2017).

key concepts of international law are directly relevant to the emergence of cyberwarfare. These roles of non-state actors and the ethics of war have been translated into law – specifically, the principles of *distinction* and *attributability*. Once we understand these concepts about cyberwarfare, we can look at two notable case studies of cyberwarfare: the 2008 Russo-Georgian War and the 2022 cyber attacks in the Russia-Ukraine War. These can help us analyse how international law functions, or does not function, in governing cyberwarfare in relation to the above key concepts. I conclude that the position of cyberwarfare in today's international law system needs reanalysis to ensure that attacks do not go ungoverned. This is particularly noted in recognising the role of non-state actors, ensuring the principle of distinction is abided by, and addressing the future possibility of instances where cyber warfare may occur without kinetic warfare.

THE 'NON-STATE ACTOR' CONCEPT

A non-state actor in international law is an actor who 'without representing states, can operate at the international level and be relevant to international law and relations'.[3] Non-state actors in contemporary conflicts are often terrorist organisations or resistance groups who are not officially acting on behalf of the state itself, or might even be embroiled in conflict with state authorities. Essentially, this means that the field of international law and rules governing state relations do not inherently apply to them. This has produced an era of warfare that is more complex and ungoverned than the 'traditional' warfare that has come before.

This is directly applicable to the challenges of cyberwarfare because cyber attacks are often carried out by non-state actors like private expert cyber companies, terrorist organisations, or civilian hackers. This creates similar challenges for the governance of cyberwarfare as those faced in armed conflicts which involve insurgent groups or 'private' aggressors. It is also relevant to classifying whether something is an 'act of

[3] Said Mahmoudi, Non-State Actors and the Development of International Environmental Law: A Note on the Role of the CEDE, *Yearbook of International Environmental Law*, Volume 30, Issue 1, 2019, Page 68, https://doi.org/10.1093/yiel/yvaa073.

force' warranting a self-defence response to a cyber attack.[4] An 'act of force' is the threshold an attack must meet for the target state to engage in legal acts of self-defence, and it involves the 'act of force' being conducted by a state actor.

This brings into the discussion Articles 2(4) and 51 of the UN Charter and customary international law, which the Tallinn Manual aimed to address in relation to cyber.[5] Article 2(4) outlines the prohibition of threat or use of force in international relations. In contrast, Article 51 refers to the ability of a state to engage in self-defence if such instances occur.[6] As this paper moves through the case studies, it will become apparent that, in general, international law often needs to be developed more and must pay attention to the presence of non-state actors,[7] and that this shortcoming is especially apparent in the emerging cases of cyber warfare.

ETHICS OF WAR IN INTERNATIONAL LAW

Attribution

The *principle of attributability* is linked to the challenges of governing cyberwarfare, particularly regarding the aforementioned non-state actors. Attributing attacks to certain actors in cyberspace is difficult as other actors are often present in the virtual battlefield, and third-party servers are used.[8] The Tallinn Manual states that for a cyberattack to be considered a use of force, a non-state actor's actions must be *attributable* to a state.[9] Furthermore, there is ongoing discussion about a modernised version of the Caroline Test as to whether anticipatory or pre-emptive self-defence can be permissible in the

[4] Michael Schmitt, 'Cybersecurity and International Law', in Nils Melzer and Robin Geiss (eds.) *The Oxford Handbook of the International Law of Global Security,* Oxford University Press, 2021. p 674.
[5] United Nations, *Charter of the United Nations*, 1945, Articles 2(4) & 51.; Michael Schmitt, 'Cybersecurity and International Law', in Nils Melzer and Robin Geiss (eds.) *The Oxford Handbook of the International Law of Global Security,* Oxford University Press, 2021: pp 673-675.
[6] United Nations, *Charter of the United Nations*, 1945, Articles 2(4) & 51.
[7] Nicholas Tsagourias and Russell Buchan, 'Cyber-Threats and International Law' in Mary Footer et al. (eds.), *Security and International Law*, Hart Publishing, 2016. p388.
[8] Giesen, K-G. "Towards a Theory of Just Cyberwar." *Journal of Information Warfare* 12, no. 1 (2013): 25. https://www.jstor.org/stable/26486996.
[9] Michael Schmitt, 'Cybersecurity and International Law', in Nils Melzer and Robin Geiss (eds.) *The Oxford Handbook of the International Law of Global Security,* Oxford University Press, (2021): 674-675.

case of cyberattacks.[10] The Caroline Test refers to the criteria a state must meet if it wishes to employ anticipatory self-defence against a supposed upcoming threat: “a necessity of self-defence, instant, overwhelming, leaving no choice of means, and no moment for deliberation.”[11] Such acts of self-defence are inextricably linked to the ability to determine attributability. Attribution is important not only for the law of self-defence but also for holding actors accountable in systems like the International Criminal Court (ICC) or International Court of Justice (ICJ) if the time comes. Giesen argues that because of the complexity of attribution in cyberspace, a ‘probabilistic approach’ should prevail, where whilst there may not be absolute certainty, we can require a 99% probability.[12]

Distinction

Distinction, a principle in the ethics of war and International Humanitarian Law, is also important in discussions of cyberwarfare. It lays out who and what can be targeted in warfare and designates that civilians and combatants must be distinguished.[13] Cyber attacks target public services or websites affecting civilians’ daily lives. They can also aim to spread disinformation and perpetrate psychological warfare, which fails to distinguish between civilian and combatant targets clearly. Eitan points out that many cyber targets have dual civilian and military usage, making this principle even more complex in its applicability to cyber warfare and attacks.[14] However, this dual usage places them in the legal category of a military target.[15] This means the extent to which

[10] John Dever, and James Dever. “Cyberwarfare: Attribution, Preemption, and National Self Defense.” *Journal of Law & Cyber Warfare* 2, no. 1 (2013): 25–63. http://www.jstor.org/stable/26441240. p37.
[11] Daniel Webster, Case of the Caroline, *Niles’ National Register*, (September 1842): 57. Quoted in John Dever, and James Dever. “Cyberwarfare: Attribution, Preemption, and National Self Defense.” *Journal of Law & Cyber Warfare* 2, no. 1 (2013): 25–63. http://www.jstor.org/stable/26441240. p37.
[12] K-G Giesen, “Towards a Theory of Just Cyberwar.” *Journal of Information Warfare* 12, no. 1 (2013):25. https://www.jstor.org/stable/26486996.
[13] International Committee of the Red Cross, ‘Principle of Distinction. How Does Law Protect in War?’ Accessed: https://casebook.icrc.org/law/principle-distinction
[14] Eitan Diamond. “Applying International Humanitarian Law to Cyber Warfare.” Edited by Pnina Sharvit Baruch and Anat Kurz. *Law and National Security: Selected Issues*. Institute for National Security Studies, 2014. P77. http://www.jstor.org/stable/resrep08957.8.
[15] ibid.

cyberinfrastructure is considered a legitimate military target is significant, making the discussion of distinction crucial in the international governance of cyber warfare.

CASE STUDY 1: 2008 RUSSO-GEORGIAN WAR

The 2008 Russo-Georgian War set the first precedent for using cyber warfare alongside boots-on-the-ground military operations.[16] It engaged questions of the role of non-state actors' attributability in cyber attacks and other rules of war. In August 2008, cyber attacks from Russia targeted the Georgian '.ge' internet domain by flooding the servers with large amounts of web traffic.[17] This caused the national phone network to go offline, disrupted other public services like banking, and hindered the Georgian government's communication ability.[18] In total, 54 websites, including those hosting the news, government sites, and financial services, were targeted, defaced and/or experienced denial of service disruptions.[19]

Regarding attributability, whilst Russia benefited greatly from the cyber attacks and the organisers of the attacks appeared to have strong knowledge of the ground war and assistance in such organising, they denied state responsibility for the cyber attacks.[20] These cyber attacks have linked questions of attributability and the role of non-state actors. These attacks were attributed to pro-Russia volunteers and hackers, who are essentially skilled individuals likely located in the Russian state.[21] These are sometimes referred to as 'hacktivists'.[22] Many of the attacks can also be traced back to a Russian cybercriminal group called RBN.[23] Thus, in this example, we face non-state actors as individual hackers and a more organised cybercriminal group.

---

[16]Andria Gotsiridze, The Cyber Dimension of the 2008 Russia-Georgia War. Rondeli Foundation. 2019.
[17] Geoff Van Epps, "Common Ground: U.S. and NATO Engagement with Russia in the Cyber Domain." *Connections* 12, no. 4 (2013): 30. http://www.jstor.org/stable/26326340
[18]ibid.
[19] Sarah P White. 'Understanding Cyber Warfare: Lessons from the Russia-Georgia War', *Modern War Institute.* (March 2018): 1.
[20] Geoff Van Epps. "Common Ground: U.S. and NATO Engagement with Russia in the Cyber Domain." *Connections* 12, no. 4 (2013): 30. http://www.jstor.org/stable/26326340
[21] Andria Gotsiridze, The Cyber Dimension of the 2008 Russia-Georgia War. Rondeli Foundation. (2019).
[22] Paulo Shakarin. 'The 2008 Russian Cyber-Campaign Against Georgia'. *Military review*. (2011): 64.
[23]Andria Gotsiridze, 'The Cyber Dimension of the 2008 Russia-Georgia War.' *Rondeli Foundation*. (2019)

The Russo-Georgian war provides empirical evidence of how cyber warfare allows the 'empowerment of third-party non-state actors in modern conflict'.[24] One report stated, 'there is no need for the state machine in modern cyber warfare'.[25] If we consider this true, the future of international law in governing warfare, particularly concerning attributability and, therefore, protection of civilians, is one concern. The argument for legal self-defence following a cyber-attack is also made complex, as the Tallinn Manual lays out, for an action to be counted as a 'use of force', it must be attributable to the state (so the victim state can therefore engage in self-defence against that perpetrating state).[26] In this case, Georgia was already engaged in self-defence as there was kinetic warfare alongside the cyber attacks. However, the issues of attributability of cyberattacks raise concerns about future claims of self-defence when only facing cyberwarfare.

As previously mentioned, the principle of distinction designates what constitutes a legal target in wartime and what does not. In this context, it can be applied to the fact that the attacks had informational and psychological effects on the state of Georgia, as they worked to establish a lone Russian narrative of the war, isolating Georgia from the outside world.[27] The principle of distinction is part of International Humanitarian Law and states that military operations must target objects of military value, sparing citizens as much as possible.[28] In this case, the attacks engaged in psychological warfare, targeting populations rather than military forces.[29] Cyber attacks of this nature purposely targeted civilian infrastructure, meaning that the Russian use of cyber warfare potentially violated International Humanitarian Law, at least about distinction. The link between the

[24] Sarah P White. 'Understanding Cyber Warfare: Lessons from the Russia-Georgia War', *Modern War Institute.* (March 2018): 5.
[25] Sarah P White. 'Understanding Cyber Warfare: Lessons from the Russia-Georgia War', *Modern War Institute.* (March 2018): 8
[26] Michael Schmitt, 'Cybersecurity and International Law', in Nils Melzer and Robin Geiss (eds.) *The Oxford Handbook of the International Law of Global Security,* Oxford University Press, (2021): 674-675.
[27] Paulo Shakarin. 'The 2008 Russian Cyber-Campaign Against Georgia'. *Military review.* (2011): 63.
[28] International Committee of the Red Cross, 'Principle of Distinction. How Does Law Protect in War?'. Accessed: https://casebook.icrc.org/law/principle-distinction
[29] Sarah P White. 'Understanding Cyber Warfare: Lessons from the Russia-Georgia War', *Modern War Institute.* (March 2018): 1-5.

infrastructure and military use would have to be analysed, as well as hackers' intent to disrupt military operations or civilian capabilities. This could, therefore, encourage a review of the principle of distinction and where the line blurs between civilian and combatant, as cyberwarfare is inherently likely to target infrastructure with dual military and civilian purposes.

In the case of the Russo-Georgian war and the argument for pre-emptive self-defence, the first cyberattack took place before the kinetic warfare began.[30] This means that if Georgia had sought to undertake a pre-emptive act of self-defence in response to the cyber attack, they would have needed prior knowledge of it, arguably more challenging in the cyber domain. However, this did not take place, and in this case, Georgia did not take pre-emptive action but instead engaged in self-defence in the kinetic warfare sense, allowing it to fit under existing international law of armed conflict.

A brief discussion of the Caroline Test, a debated rule in international law allowing for pre-emptive self-defence, may be useful. White argues that, in learning from the Russo-Georgian war, there is an 'erroneous notion' that cyberspace is too technically complex for the traditional war community to understand.[31] She writes that whilst cyberattacks can unfold more quickly, they are based on long processes of identifying vulnerabilities and maintaining access - a cyberattack requires months if not years of planning.[32] Therefore, if methods of cyber warfare are to be used more commonly, there is arguably a possibility that pre-emptive self-defence could be legitimate even when operating only in cyberspace, as knowledge of an imminent attack could be uncovered before it happens. This would then engage the principles of necessity and proportionality, legal principles referring to the unavailability of other response options and using only force proportional to the threat faced and the objective pursued.[33] These

[30] Andria Gotsiridze, 'The Cyber Dimension of the 2008 Russia-Georgia War.' *Rondeli Foundation.* (2019). Accessed: https://gfsis.org.ge/blog/view/970
[31] Sarah P White. 'Understanding Cyber Warfare: Lessons from the Russia-Georgia War', *Modern War Institute.* (March 2018): 11.
[32] Sarah P White. 'Understanding Cyber Warfare: Lessons from the Russia-Georgia War', *Modern War Institute.* (March 2018): 13
[33] Dapo Akande, and Thomas Liefländer. "Clarifying Necessity, Imminence, and Proportionality in the Law of Self-Defense." *The American Journal of International Law* 107, no. 3 (2013): 563–70. https://doi.org/10.5305/amerjintelaw.107.3.0563.

are inherently more difficult to prove when the act of self-defence is pre-emptive, and should Georgia have wanted to act in self-defence purely regarding the cyber attacks, they would have had to employ these principles. However, the broader scope of the war meant that this question did not need to be deeply engaged.

CASE STUDY 2: RUSSIA-UKRAINE 2022

A more recent example of the use of cyber warfare in armed conflict is the case of the Russia-Ukraine war. This case provides further evidence and supports the points raised by the Russo-Georgian War, leading to similar conclusions about international governance challenges. Throughout the conflict, Russian cybercriminals and government groups have targeted civilian services such as government agencies, television stations, and energy substations.[34] This continued until more recently when, in February 2023, the attack ATK256 (UAC-0056) targeted several Ukrainian public bodies.[35]

Similar questions around attributability and non-state actors are raised here, as in the discussion of the Russo-Georgian war. For example, since the start of the conflict, 61% of all cyberattacks occurring worldwide have been perpetrated by pro-Russian hacktivist groups.[36] Once again, we see the Russian state engaging through non-state actors, complicating attributability to the state. The same waterfall effect occurs where it becomes difficult to consider cyberattacks as an act of force attributable to a state, making self-defence difficult to claim under international law.

Furthermore, the principle of distinction in relation to Russia-Ukraine is important to consider. A focus should be placed on ensuring that only military targets are targeted,

[34] John Sakellariadis and Maggie Miller. 'Ukraine Gears up for a New Phase of Cyberwar with Russia'. *Politico.* (February 2023). Accessed: https://www.politico.com/news/2023/02/25/ukraine-russian-cyberattacks-00084429

[35] From Ukraine to the Whole of Europe: Cyber Conflict Reaches a Turning Point'. Summary of Extensive Analysis from the Thales Cyber Threat Intelligence Team. *Thales.* (March 2023). Accessed: https://www.thalesgroup.com/en/worldwide/security/press_release/ukraine-whole-europecyber-conflict-reaches-turning-point

[36] ibid.

while civilian services like television stations should arguably be non-legal targets. In the third quarter of 2022, we observed cyber attacks spread beyond Ukraine and engag other European states in hybrid cyber warfare.[37] This also poses questions about distinction as not only 'at-war' states' military properties and services are being targeted, but third-party states are becoming involved in cyber attacks, which may not be able to be classified within the laws of war.

In general, the use of cyber warfare in the Russia-Ukraine war is similar to that of the Russo-Georgian war and raises similar questions. Its repeated use shows the changing nature of modern armed conflict in general. In this war, the scale of military operations has appeared inversely correlated with the strategic importance of cyber operations.[38] The author argues that, if this is the case, perhaps cyberwarfare should not be considered a 'fifth domain of war'.[39] This is interesting to note as cyberwarfare becomes more common in war and should be observed closely. Perhaps cyberwarfare may take a route apart from kinetic warfare, and international law will need to develop laws specific to cyberwarfare. Alternatively, it will largely remain correlated to traditional warfare, and the international community needs to amend certain laws or build upon the existing rules for armed conflict, including cyber.

CONCLUDING DISCUSSION

To discern the effectiveness of international law in dealing with the emergence of cyberwarfare's increasing prevalence, I have looked at questions of attributability, non-state actors, distinction, and the classification of use of force/legality of self-defence and pre-emptive self-defence.

Overall, the strength of international law as applied to cyberwarfare is lacking. The two cases where we observe the parallel activity of traditional kinetic warfare and cyber

[37] ibid.
[38] Jon Bateman, Nick Beecroft, Gavin Wilde. 'What the Russian Invasion Reveals About the Future of Cyber Warfare'. *Carnegie Endowment for International Peace*. (December 2022).
[39] ibid.

attacks, therefore theoretically making it easier to apply the law of armed conflict, have not seen extensive legal constraints regarding the cyber attacks. We also have not seen the Russian government held accountable by the ICC or ICJ. The major 'plot holes' in the international governance of armed conflict are due to the role of non-state actors, the linked principle of attributability, and the principle of distinction. For cyberwarfare to be legal under the law of armed conflict, it must be able to be termed a use of force or as part of a use of force and, ideally, be attributable to a state actor. In regard to distinction, cyber warfare is symbolic of the general changing nature of war. It engages in more psychological warfare as it targets civilian infrastructure and information services, which points towards the need to review the rules of distinction in relation to cyber.

Recommendations

In the case of the Russo-Georgian 2008 war and the ongoing Russia-Ukraine war, cyber attacks have been difficult to directly and definitively attribute to the state. In future questions of the international governance of cyberwarfare, we need to engage the law of state responsibility and determine the extent to which a state is responsible for individual or group actors operating on their territory or on behalf of their military objectives. Thus, we *could* look at laws regarding state-harboured terrorism. However, the role of non-state cyber actors is quite different as they tend to operate on behalf of state military objectives in regard to armed conflict. Rule 15 of Tallinn Manual 2.0 lays out State Responsibility yet struggles to define individual hacktivists as they are not 'state organs', nor does domestic law empower them.[40] Therefore, the purposeful engagement of civilian hackers and private hacking groups should be reviewed to be included in state responsibility for acts of war, potentially dependent on their damage outcomes. Buchan and Tsagourias argue that, in the case of cyber warfare, 'If a state is unwilling to curb the activities of non-state actors amounting to involvement in the attack, it should become the target of the self-defence action, whereas if the state is

[40] Michael Schmitt. 'Law of international responsibility.' In *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2017): 79-167. Cambridge: Cambridge University Press. doi:10.1017/9781316822524.010

unable, then self-defence action should target the non-state actor directly.'[41] This would seem an engaged and informed argument to be made on behalf of the role of non-state actors, attributability, and the laws of self-defence, which is the key area to which these two concepts apply in international law.

Further research

Cyberwarfare presents other problems for international law in that cyberattacks alone may not be able to be classified as armed conflict under international law and, therefore, would not face the same legal restrictions. This should be further considered; however, to investigate the constraints that international law of armed conflict places on cyber warfare, we have examined cases in which it has been used definitively in armed conflict. Further discussion and analysis can also be conducted on the ethics of war and international law principles of proportionality and necessity in regard to self-defence. However, as these case studies took place in a broader context of kinetic armed conflict and less literature on direct cyberattack self-defence, proportionality and necessity have been omitted here to keep this discussion within its limits.

In conclusion, cyberwarfare poses significant challenges to the international governance of armed conflict. Current international law concepts of non-state actors, attributability and distinction must be reviewed to apply them to cyber attacks, or new guidelines for cyberwarfare need to be discussed.

[41] Nicholas Tsagourias and Russell Buchan, 'Cyber-Threats and International Law' in Mary Footer et al. (eds.), *Security and International Law*, Hart Publishing, (2016): 386.

Bibliography

Bateman, Jon, Nick Beecroft, and Gavin Wilde. “What the Russian Invasion Reveals About the Future of Cyber Warfare.” *Carnegie Endowment for International Peace,* December 2022. Accessed: https://carnegieendowment.org/2022/12/19/what-russian-invasion-reveals-abo Ut-future-of-cyber-warfare-pub-88667

Dever, John, and James Dever. “Cyberwarfare: Attribution, Preemption, and National Self Defense.” *Journal of Law & Cyber Warfare* 2, no. 1 (2013): 25–63. http://www.jstor.org/stable/26441240.

Diamond, Eitan. “Applying International Humanitarian Law to Cyber Warfare.” Edited by Pnina Sharvit Baruch and Anat Kurz. *Law and National Security: Selected Issues*. Institute for National Security Studies, 2014. http://www.jstor.org/stable/resrep08957.8.

“From Ukraine to the Whole of Europe: Cyber Conflict Reaches a Turning Point.” Summary of Extensive Analysis from the Thales Cyber Threat Intelligence Team. THALES. March 29 2023. Accessed: https://www.thalesgroup.com/en/worldwide/security/press_release/ukraine-wh Ole-europe cyber-conflict-reaches-turning-point

Gazula, Mohan B. “Cyberwarfare Conflict Analysis and Case Studies.” *Cybersecurity Interdisciplinary Systems Laboratory (CISL), Sloan School of Management,* MIT (2017) https://cams.mit.edu/wp-content/uploads/2017-10.pdf

Giesen, K-G. “Towards a Theory of Just Cyberwar.” *Journal of Information Warfare* 12, no. 1 (2013): 22–31. https://www.jstor.org/stable/26486996.

Gotsiridze, Andria. “The Cyber Dimension of the 2008 Russia-Georgia War.” *Rondeli Foundation.* (2019). Accessed: https://gfsis.org.ge/blog/view/970

Mahmoudi, Said. “Non-State Actors and the Development of International Environmental Law: A Note on the Role of the CEDE.” *Yearbook of International Environmental Law*, Volume 30, Issue 1, (2019):68–78, https://doi.org/10.1093/yiel/yvaa073

Schatcher, Oscar. “The Right of States to Use Armed Force.” (1984) 82 *Michigan Law Review* 1620, 1635.

Principle of Distinction. How Does Law Protect in War? International Committee of the Red Cross. Accessed: https://casebook.icrc.org/law/principle-distinction.

Schmitt, Michael. “Cybersecurity and International Law.” In Nils Melzer and Robin Geiss (eds.) *The Oxford Handbook of the International Law of Global Security,* Oxford University Press, 2021.

Schmitt, Micheal (2017). Law of international responsibility. In *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (pp. 79-167). Cambridge: Cambridge University Press. doi:10.1017/9781316822524.010.

Shakarin, Paulo. “The 2008 Russian Cyber-Campaign Against Georgia.” Military review. 2011. Accessed: file:///Users/macbook/Downloads/SHAKARIAN-RussiaCyber-MilRev.pdf.

Tsagourias, Nicholas, and Russell Buchan. “Cyber-Threats and International Law.” In Mary Footer et al. (eds.), *Security and International Law*, Hart Publishing, 2016.

United Nations, *Charter of the United Nations*, 1945, Articles 2(4) & 51. available at: https://www.un.org/en/about-us/un-charter/full-text.

Van Epps, Geoff. “Common Ground: U.S. and NATO Engagement with Russia in the Cyber Domain.” *Connections* 12, no. 4 (2013): 15–50. http://www.jstor.org/stable/26326340.

Webster, D. “The Case of Caroline.” *Niles’ National Register*, (September 1842): 57.

White, Sarah P. “Understanding Cyber Warfare: Lessons From The Russia-Georgia War.” *Modern War Institute*. March 20 2018. Accessed: https://mwi.usma.edu/wp-content/uploads/2018/03/Understanding-Cyberwarfare.pdf.