Applying Jus Ad Bellum in Cyberspace

https://www.e-ir.info/2016/09/01/applying-jus-ad-bellum-in-cyberspace/

SOPHIE BARNETT, SEP 1 2016

Despite their potential for disruption to international peace and security, there is no specific international legal structure for analysing cyber attacks. Consequently, scholars apply the framework of *jus ad bellum* – "international dispositions regarding the justification for entering an armed conflict"[1] – to cyber attacks, but the discussion is subject to varying interpretations. Specifically, Articles 2(4) and 51 of the United Nations ("UN") Charter of Rights and Freedoms ("Charter") governing the prohibition on the use of force and right to self-defence are at the heart of the debate. This paper examines the application of these provisions to cyber attacks in three sections. First, it identifies the unique characteristics of cyber attacks. Second, it explores existing literature on the legality of cyber attacks and adopts Michael Schmitt's criteria that cyber attacks constitute uses of force and armed attacks when they sufficiently resemble the consequences of their traditional counterparts. Third, it identifies four areas challenging the applicability of these laws to cyber attacks, namely: state responsibility, anticipatory self-defence, the principles of necessity and proportionality, and espionage. This paper argues that while Articles 2(4) and 51 can be interpreted to include cyber attacks, the unique characteristics of cyberspace strain their application.

Nature of Cyber Attacks

Cyber attacks are attempts by computer hackers to damage or destroy a computer network or system.[2] By virtue of their highly sophisticated programming, cyber attacks differ from traditional attacks in four ways. First, they are often indirect, making it difficult to establish the origin and immediate consequences of the attack.[3] Second, the intangible nature of both targets and weapons challenges the characterisation of the attack as a use of force.[4] Third, the locus of the attack –targeted data residing on an information server – challenges traditional notions of border violations.[5] Fourth, cyber attacks do not necessarily result in irreversible physical destruction and instead may simply neutralise, shut down, or intangibly "break" a system.[6]

These factors may explain the development of cyber attacks as a desirable alternative to traditional military aggression for state and non-state actors. Furthermore, due to the interconnectedness of civilian and military computer systems and the ease with which anyone with a networked internet system can launch them, cyber attacks know no borders and have the potential to seriously disrupt or cause harm to public or private infrastructure alike. They constantly threaten government, corporate, and private systems worldwide and challenge international security, public safety, and economic stability.[7] Due to the anonymity and unpredictability of cyber attacks, prevention is difficult. Yet despite the potential severity of impact comparable to traditional uses of force, cyber attacks are not explicitly governed under international law and present a grey area under *jus ad bellum.*

Interpreting *Jus Ad Bellum*

While drafted with traditional armed conflict in mind, the language of Articles 2(4) and 51 can be broadly interpreted to include cyber attacks. In referencing the Charter, examples, and case law, this section establishes how cyber attacks can be included under these provisions.

The Prohibition on the Use of Force

The prohibition on the use of force is a fundamental principle of international law.[8] Article 2(4) of the Charter holds

that "all members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state."[9] As a customary rule of international law,[10] this prohibition extends to all states, regardless of UN membership. Furthermore, conventional use of *jus ad bellum* refers to acts of states. Consequently, while they may raise other legal concerns, cyber attacks mobilized by non-state actors are irrelevant to *jus ad bellum*.

Although not defined in international law, the "use of force" under Article 2(4) clearly includes armed force[11] –relevant to *jus ad bellum* – and excludes political or economic coercion.[12] The major difference between armed force and political or economic coercion is the former's physically destructive capabilities. Given that traditional force is instrument-based and causes physical destruction, fatality, or injury, it is conceivable that a cyber attack causing such damage will be considered a use of force under Article 2(4).[13] The 2010 Stuxnet virus may be the clearest example of a cyber attack qualifying as a use of force.[14] The virus, which targeted Iran's Natanz nuclear facility, caused Iran to replace 1,000 of the 9,000 IR-1 centrifuges at the facility.[15]

Where the attack causes no physical damage, the classification of an operation as a use of force is the subject of debate between expansionist and restrictive approaches. The expansionist approach holds that the destructive outcome does not have to cause physical destruction of property.[16] Hence, a cyber operation that interfered with the functioning of a computer system such that it was considered to be "broken" would constitute armed force. In this light, the Denial of Service attacks against Georgian websites in 2008 during the Russo-Georgian War – designed to shut down computer networks by overwhelming them with useless traffic[17] – would qualify. Although the attacks caused no physical damage, they caused massive disruption.

The restrictive approach would suggest that the Denial of Service attacks more closely resemble political or economic coercion in the respect that physical destruction is lacking and thus are outside the ambit of Article 2(4). Proponents of the approach interpret Article 2(4) literally and contend that anything other than traditional armed force must be excluded[18] and tolerated as "peaceful alternatives to a full blown war."[19] Hence, cyber attacks do not constitute a use of force, notwithstanding their detrimental impact and substantial threat to international security.[20]

Schmitt, an international legal scholar on "use of force" issues, reconciles these approaches in holding that cyber attacks must fit into a traditional, consequence-based frame of reference to qualify as armed force. Every operation falls somewhere on a continuum between armed force and political or economic coercion.[21] Schmitt's criteria for placement along the continuum include the severity of the damage, immediacy of consequential harm, the directness of connection between the armed force and its consequences, the crossing of an international border, the ability to evaluate or discern the act's physical consequences, and the legality of the act under domestic and international law (that violence is presumptively illegal, whereas political or economic coercion is not).[22] While the criteria of immediacy and a violated border are less relevant to cyber attacks, the remaining criteria are useful for identifying breaches of Article 2(4).[23] Schmitt's criteria have created a satisfactory balance and also generally been accepted in recent years.[24] His approach provides the most fruitful basis for analysing *jus ad bellum* in the context of cyber attacks, allowing a fuller consideration of Article 2(4) and its application.

The Right to Self-Defence

An exception to Article 2(4) occurs if an armed attack is launched against a state, thus triggering that state's right to exercise the use of force in self-defence. Article 51 of the Charter – also a customary rule of international law[25] – recognises the "inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations."[26] As "armed attack" is not defined in the Charter, it will be up to the courts to explore the term's breadth and whether it includes cyber attacks.

In *Nicaragua v. USA*, the International Court of Justice ("ICJ") distinguished armed attacks from armed force by holding that the former must achieve a minimum level of severity to constitute a grave use of force,[27] thereby transcending the equivalent of a "mere frontier incident."[28] This implies that not all uses of force will constitute an armed attack, creating situations where a state may be the target of a use of force but unable to respond in self-defence.[29] In the context of cyber attacks, the issue will be whether an attack has caused damage of the magnitude

envisioned by the ICJ. Furthermore, it is yet to be determined whether inflicting damage through sophisticated programming constitutes an "armed attack." However, as a means of causing destruction, courts are likely to recognise cyber weaponry as arms within the meaning of "armed attack."

It may also be the case that cyber attacks come as a series of events that only cumulatively meet the threshold for an armed attack.[30] For example, it is generally agreed that if Stuxnet had occurred as a series of attacks rather than a single use of force, it would likely have qualified as an armed attack.[31] However, in*Nicaragua v. USA*, *DRC v. Uganda*, and *Oil Platforms*, the ICJ demonstrated a willingness to consider an accumulation of events as constituting an armed attack.[32] Thus, a liberal interpretation of "armed attack" potentially encompasses a state-sponsored cyber attack, thus triggering the application of Article 51. However, further interpretive difficulties remain and are discussed below.

Further Problems in Applying *Jus Ad Bellum*

While Articles 2(4) and 51 can be interpreted to include cyber attacks, these laws are tailored to address traditional attacks and consequently fail to address the unique characteristics of cyber attacks. Specifically, applying these laws raises issues concerning state responsibility, anticipatory self-defence, the principles of necessity and proportionality, and espionage.

State Responsibility

While Article 51 does not explicitly hold that the attacker must be a state actor, the ICJ has held that it is triggered exclusively by acts of states.[33] However, attributing cyber attacks to states is one of the biggest challenges in successfully claiming self-defence. In *Oil Platforms*, the ICJ held that a state invoking the right to self-defence must prove not only that an armed attack occurred, but that it was an act of state.[34] Article 11 of the International Law Commission's Articles on State Responsibility for Internationally Wrongful Acts – indicative of customary international law – contends that a state may "adopt" the conduct of a non-state actor.[35] This adoption is generally established using the effective control test applied by the ICJ in *Nicaragua v. USA*, which establishes a standard of complete dependence between a state and armed group that is "so much one of dependence on the one side and control on the other"[36] that the group may legitimately be considered as a state organ. While technically applicable to cyber attacks, this link is relatively difficult to prove.

For example, while the 2008 cyber attacks against Georgia evidenced coordination between hackers and Russian state organs, there is no clear proof of Russia's responsibility.[37] Similarly, the devastating 2007 cyber attacks against Estonia that may have emanated from Russia following Estonia's movement of a Soviet World War II memorial could not be attributed to Russia. Thus, even if they had constituted an armed attack, Estonia could not have successfully invoked self-defence.[38]

The increased use of botnets – networks of compromised computers jointly controlled without the owners' knowledge – also make it difficult to distinguish between attacks originating from a specific address and those utilising a compromised computer.[39] In the Estonian attack, Russia claimed that the few computers successfully traced to its institutions had been compromised.[40] The fact that a cyber attack "originates from a governmental cyber infrastructure is not sufficient evidence for attributing the operation to that state."[41] Instead, it merely indicates that the state is somehow associated with that operation.

Establishing a sufficient link is also difficult where the attacks are launched by loosely connected individuals alongside traditional state action. For example, Russia's action in South Ossetia during the 2008 Russo-Georgian War was supported by patriotic civilians who "participated" in the conflict by launching cyber attacks against Georgia without Russian authorisation.[42] While not meeting the threshold nor constituting an armed group – an important aspect of attribution – this event highlights the problem in determining state responsibility where a state is unaware of cyber attacks occurring within their territory. As Heather Dinniss – author of *Cyber Warfare and Laws of War* – has opined, a state must knowingly allow its territory to be used for such action if attribution is to be established.[43]

Timely attribution is also fundamental to a successful claim of self-defence.[44] This follows from the principle of necessity, discussed below. Due to the anonymity and sophistication of cyber attacks, it often takes a relatively longer time to identify the perpetrator compared to traditional attacks. In *Oil Platforms*, the ICJ held that a victim state must refrain from mobilising a forcible response until hard evidence linking the armed attack to a state is established.[45] An immediate and forceful response based on unfounded suspicions may undoubtedly increase hostilities. However, the necessity of waiting for hard evidence also risks the ultimate response being viewed as a planned armed reprisal, which is prohibited under international law, instead of self-defence.[46] Furthermore, while the appropriate time for response is inherently contextual, the longer the delay, the greater the risk of the situation becoming more a matter of international politics rather than adjudication under established international legal principles.

Thus at present, international law has the capacity to classify a cyber attack as an armed attack if the attack is attributed to a state. However, it has not yet adequately developed rules for determining when the attack may be attributed to a state.

Anticipatory Self-Defence

When a state's right to self-defence is triggered, the response is subject to strict criteria before qualifying as a legitimate use of force. Certainly, the act must be anticipatory rather than pre-emptive. Pre-emptive self-defence is considered contrary to international law as the right to self-defence is only triggered if an armed attack has already occurred.[47] Article 51 explicitly uses the phrase "if an armed attack occurs,"[48] thereby rejecting claims of self-defence that precede the actual use of force.[49] This was recognised following the 2003 American-led invasion of Iraq, when the Bush administration claimed its invasion was a necessary response to Iraq's alleged weapons of mass destruction program.[50] The UN rejected this claim, holding that it does "not favour the … reinterpretation of Article 51."[51]

The problem lies in applying the criteria for anticipatory self-defence to a cyber attack. Anticipatory self-defence implies that if an armed attack is imminent, the victim state may intercept the attack, rather than await the launch.[52] For cyber attacks, an intrusion into a network may be discovered prior to the network's destruction, in which case the victim state could enter or destroy the computer system launching the attack.[53] For example, malware often features a type of "backdoor payload"[54] that allows the attacker to control a computer and subsequently others connected to it. However, identifying an intrusion as the first step of an armed attack will depend on the information available, and analysis may lead to inconclusive results. Furthermore, it is unclear how the condition that the cyber attack is imminent will be interpreted. Thus, the issue remains whether a state could legitimately attack or enter foreign computers to prevent a cyber attack.

Principles of Necessity and Proportionality

In *Nicaragua v. USA*, the ICJ upheld the consensus of the 1837 *Caroline* Incident, which established that an act of self-defence must be necessary and proportional to the armed attack.[55] Necessity implies that acting in self-defence must be essential for the protection of the state and its interests. Specifically, the use of force must be crucial to repel the attack and alternate remedies must have previously been exhausted.[56] Necessity also highlights the principle that acts of self-defence must occur within a timely manner. As noted, this may prove challenging for cyber acts of self-defence, where establishing the origin of the attack is difficult and time-consuming. This problem is not addressed under existing law.

Proportionality requires balancing the response against its objective of ending the attack.[57] The action cannot be retaliatory or punitive and does not have to employ the same method of weaponry used by the attacking state.[58] Therefore, proportionality may permit the use of traditional force against a cyber attack. Dinniss gives the example of a victim state physically bombing the attacking computer, assuming the cyber attack launched from that computer was serious enough to justify the bombing.[59]

Espionage

As discussed, a cyber operation without a physically destructive outcome does not constitute a use of force. However, these operations may still be permitted in armed conflict as constituting espionage, which is legal under international law.[60] Although it is generally agreed that espionage is distinct from the use of force, cyber espionage challenges this distinction.[61] For example, undetected cyber intelligence gathering – while not a use of force – may be the first step in the planning of a future attack.[62] In such a situation, the victim state would only be able to retaliate through counter-espionage or other means rather than through force, perpetuating the conflict.[63] Accordingly, cyber espionage carries the potential for significant harm falling outside of Article 2(4), thus demonstrating another failure of existing law to apply to cyber aggression.[64]

Conclusion

Although no cyber attack to date has been considered to constitute an armed attack, with technological evolution it is conceivable that cyber attacks will reach this threshold in the future. However, the existing law governing*jus ad bellum* does not satisfactorily address the unique characteristics of cyber attacks and is subject to a great degree of interpretation. Consequently, states can potentially manipulate the interpretations of *jus ad bellum* and its application to cyber attacks to serve national interests. Thus, if international law is to govern cyber attacks adequately within the meaning of *jus ad bellum*, it must be subject to further jurisprudential development.

Endnotes

[1] Titiriga Remus, "Cyber-attacks and International law of armed conflicts; a "jus ad bellum" perspective,"*Journal of International Commercial Law and Technology* 8, no. 3 (2013): 179. http://www.jiclt.com/index.php/jiclt/article/view/185/183.

[2] Michael N. Schmitt, "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework," *Columbia Journal of Transnational Law* 37, no. 3 (1999): 888.

[3] Heather Harrison Dinniss, *Cyber Warfare and the Laws of War* (Cambridge: Cambridge University Press, 2012), 65, http://dx.doi.org.myaccess.library.utoronto.ca/10.1017/CBO9780511894527.

[4] Ibid., 67.

[5] Ibid., 70.

[6] Ibid., 72.

[7] Michael N. Schmitt, "Cyber Operations and the Jus Ad Bellum Revisited," *Villanova Law Review* 56, no. 3 (2011): 571.

[8] John H. Currie, et al., *International Law: Doctrine, Practice, and Theory* (Toronto: Irwin Law, 2014), 843.

[9] U.N. Charter art. 2, 4.

[10] Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America), 1986 I.C.J. Rep 14 at 213.

[11] Whether it is armed force is considered below in the discussion of Article 51.

[12] Dinniss, *Cyber Warfare*, 41.

[13] Cordula Droege, "Get off my cloud: cyber warfare, international humanitarian law, and the protection of civilians," *International Review of the Red Cross* 94, no. 886 (2012): 546, doi:10.1017/S1816383113000246.

[14] Dinniss, *Cyber Warfare*, 57.

[15] Akita Shubert, "Cyber warfare: A different way to attack Iran's reactors," *CNN.com*, last modified November 8, 2011, http://www.cnn.com/2011/11/08/tech/iran-stuxnet/.

[16] Remus, Cyber-attacks, 182.

[17] Dinniss, *Cyber Warfare*, 101.

[18] Remus, Cyber-attacks, 181.

[19] Ibid.

[20] Ibid., 182.

[21] Michael N. Schmitt, "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework," *Columbia Journal of Transnational Law* 37, no. 3 (1999): 915.

[22] Ibid., 914.

[23] Dinniss, Cyber Warfare, 64.

[24] Remus, Cyber-attacks, 183.

[25] Nicaragua v. United States at 200.

[26] U.N. Charter art. 51.

[27] Nicaragua v. United States at 191.

[28] Ibid. at 195.

[29] Remus, Cyber-attacks, 188.

[30] Dinniss, *Cyber Warfare,* 96.

[31] Ibid.*,* 57.

[32] Nicaragua v. United States at 231. See also Oil Platforms (Islamic Republic of Iran v. United States of America), 2003 I.C.J. Rep 16 at 64. Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda), 2005 I.C.J. Rep 168 at 146-301.

[33] Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion, 2004 I.C.J. Rep 126 at 139-142. See also Nicaragua v. United States at 195.

[34] Oil Platforms at 57.

[35] G.A. Res. 56/85, annex, Responsibility of States for Internationally Wrongful Acts at 11 (Jan. 28, 2002).

[36] Nicaragua v. United States of America at 115.

[37] Dinniss, *Cyber Warfare*, 101.

[38] Schmitt, Jus Ad Bellum Revisited ,578.

[39] Dinniss, *Cyber Warfare,* 66.

[40] Ibid.

[41] Michael N. Schmitt, ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge: Cambridge University Press, 2013), 34, http://dx.doi.org.myaccess.library.utoronto.ca/10.1017/CBO9781139169288.

[42] Eric Kodar, "Applying the Law of Armed Conflict to Cyber Attacks: From the Martens Clause to Additional Protocol I," *ENDC Proceedings* 15 (2012): 126, http://www.ksk.edu.ee/wp-content/uploads/2012/12/KVUOA_Toimetised_15_5_Kodar.pdf.

[43] Dinniss, *Cyber Warfare,* 98.

[44] Ibid.

[45] Oil Platforms at 61.

[46] Dinniss, *Cyber Warfare,* 102.

[47] Currie et al, *International Law*, 901.

[48] U.N. Charter art. 51.

[49] Remus, Cyber-attacks, 186.

[50] Currie et al, *International Law*, 903.

[51] U.N Secretary-General, *A more secure world: Our shared responsibility,* U.N. Doc. A/59/565 at 192 (Dec. 2, 2004).

[52] Currie et al, *International Law*, 901.

[53] Remus, Cyber-attacks, 186.

[54] Dinniss, *Cyber Warfare*, 89.

[55] Nicaragua v. United States at 194.

[56] Dinniss, *Cyber Warfare,* 102.

[57]Ibid., 104.

[58] James Lewis, "A Note on the Laws of War in Cyberspace," *Center for Strategic and International Studies*, last modified April 25, 2010, https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/100425_Laws%20of%20War%20Applicable%20to%20Cyber%20Conflict.pdf.

[59] Dinniss, *Cyber Warfare,* 104.

[60] Anna Wortham, "Should Cyber Exploitation Ever Constitute a Demonstration of Hostile Intent That May Violate UN Charter Provisions Prohibiting the Threat or Use of Force?" *Federal Communications Law Journal* 64, no. 3

(2012): 652, http://www.repository.law.indiana.edu/fclj/vol64/iss3/8.

[61] Ibid.

[62] Remus, Cyber-attacks, 188.

[63] Ibid.

[64] Ibid.

References

Akita Shubert. “Cyber warfare: A different way to attack Iran’s reactors.” *CNN.com*. Last modified November 8, 2011. http://www.cnn.com/2011/11/08/tech/iran-stuxnet/.

Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda), 2005 I.C.J. Rep 168.

Currie, John H., et al. *International Law: Doctrine, Practice, and Theory.* Toronto: Irwin Law, 2014.

Deibert, Ronald J. *Black Code: Surveillance, Privacy, and the Dark Side of the Internet.* Toronto: McClelland & Stewart, 2013.

Dinniss, Heather Harrison. *Cyber Warfare and the Laws of War.* Cambridge: Cambridge University Press, 2012. http://dx.doi.org.myaccess.library.utoronto.ca/10.1017/CBO9780511894527.

Droege, Cordula. “Get off my cloud: cyber warfare, international humanitarian law, and the protection of civilians.” *International Review of the Red Cross* 94, no. 886 (2012): 533-578, doi:10.1017/S1816383113000246.

G.A. Res. 56/85, annex, Responsibility of States for Internationally Wrongful Acts (Jan. 28, 2002).

James Lewis. “A Note on the Laws of War in Cyberspace.” *Center for Strategic and International Studies*. Last modified April 25, 2010. https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/100425_Laws%20of%20War%20Applicable%20to%20Cyber%20Conflict.pdf.

Kessler, Oliver, and Wouter Werner. “Expertise, Uncertainty, and International Law: A Study of the Tallinn Manual on Cyberwarfare.” *Leiden Journal of International Law* 26 (2013): 793-810. doi:10.1017/S0922156513000411.

Kodar, Eric. “Applying the Law of Armed Conflict to Cyber Attacks: From the Martens Clause to Additional Protocol I.” *ENDC Proceedings* 15 (2012): 107-132. http://www.ksk.edu.ee/wp-content/uploads/2012/12/KVUOA_Toimetised_15_5_Kodar.pdf.

Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion, 2004 I.C.J. Rep 126.

Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America), 1986 I.C.J. Rep 14.

Oil Platforms (Islamic Republic of Iran v. United States of America), 2003 I.C.J. Rep 16.

Remus, Titiriga. “Cyber-attacks and International law of armed conflicts; a “jus ad bellum” perspective.”*Journal of International Commercial Law and Technology* 8, no. 3 (2013): 173-189. http://www.jiclt.com/index.php/jiclt/article/view/185/183.

Schmitt, Michael N, ed. *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press, 2013. http://dx.doi.org.myaccess.library.utoronto.ca/10.1017/CBO9781139169288.

Schmitt, Michael N. "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework." *Columbia Journal of Transnational Law* 37, no. 3 (1999): 885-937.

Schmitt, Michael N. "Cyber Operations and the Jus Ad Bellum Revisited," *Villanova Law Review* 56, no. 3 (2011): 569-606.

Schmitt, Michael N. "Wired Warfare: Computer network attack and jus in bello," *International Review of the Red Cross* 84, no. 846 (2002): 365-399. http://dx.doi.org.myaccess.library.utoronto.ca/10.1017/S1560775500097741.

Schmitt, Michael N. "Rewired warfare: rethinking the law of cyber attack." *International Review of the Red Cross* 96, no. 893 (2014): 189-206. doi:10.1017/S1816383114000381.

U.N. Charter article. 2, 4.

U.N. Charter article. 51.

U.N Secretary-General, *A more secure world: Our shared responsibility,* U.N. Doc. A/59/565 (Dec. 2, 2004).

Wortham, Anna. "Should Cyber Exploitation Ever Constitute a Demonstration of Hostile Intent That May Violate UN Charter Provisions Prohibiting the Threat or Use of Force?" *Federal Communications Law Journal* 64, no. 3 (2012): 643-660. http://www.repository.law.indiana.edu/fclj/vol64/is

Written by: Sophie Barnett
Written at: University of Toronto
Written for: Gerard Kennedy and Brian Kolenda
Date written: June 2016

About the author:

Sophie Barnett is a second year, pursuing an Honours Bachelor of Arts degree in International Relations at the University of Toronto. Her primary research interests focus on cybersecurity and human rights, and how the two interact.