



University
of Exeter

ECIL

EXETER CENTRE FOR
INTERNATIONAL LAW

Exploring the Necessity and Proportionality of Self-Defense in the Cyber Context

Chris O'Meara

Forthcoming in Martin Faix and Marko Svicevic (eds), *Regulating the Use of Force
in International Law: Principles, Perspectives and Challenges*
(*Lieber Studies Series*, Oxford University Press)

Exeter Centre for International Law

Working Paper Series

2025/2



University
of Exeter

ECIL

EXETER CENTRE FOR
INTERNATIONAL LAW

The **Exeter Centre for International Law** builds on a long and distinguished tradition of international legal scholarship at Exeter Law School. The Centre's mission is to provide an intellectual environment for the study and development of international law and to stimulate discussion and collaboration in response to the most pressing challenges facing the international community. As part of this mission, the Centre publishes the present Working Paper Series.

Centre Director: Professor Annika Jones
General Editor: Professor Aurel Sari
Editor in Chief: Professor Kubo Mačák

Exeter Centre for International Law
Exeter Law School, Amory Building
Rennes Drive, Exeter, EX4 4RJ, United Kingdom

 <http://www.exeter.ac.uk/ecil>
 [@ExeterCIL](https://twitter.com/ExeterCIL)

© All rights reserved. No part of this paper may be reproduced in any form without the permission of the author.

Cite as Chris O'Meara, "Exploring the Necessity and Proportionality of Self-Defense in the Cyber Context", ECIL Working Paper 2025/2, forthcoming in Martin Faix and Marko Svcevic (eds), *Regulating the Use of Force in International Law: Principles, Perspectives and Challenges* (Lieber Studies Series, Oxford University Press).

Exploring the Necessity and Proportionality of Self-Defense in the Cyber Context

CHRIS O'MEARA*

I. INTRODUCTION

This chapter explores how international law delineates the boundaries of states using force in self-defense in the cyber context. Although cyber activities¹ are increasingly the focus of state and scholarly deliberation, the question of how states may act defensively using cyber means while remaining within prescribed limits remains relatively underexplored. A lack of determinacy on this vital issue leaves states greater leeway to use force, with potential negative consequences for other states and actors that might be affected by defensive cyber responses.

Our starting point is the UN Charter. The drafters of the UN Charter conceived of the right of self-defense as it existed in a purely kinetic age. Arising from the ashes of the Second World War, the aspirations of the United Nations founders, including the revolutionary prohibition of threats and uses of force contained in Article 2(4) of the UN Charter,² were realized against a background of bullets and bombs, not software and data. Negotiating in San Francisco in 1945 to finalize the Charter, state delegates operated in a pre-digital world, with modern information and communications technologies not yet envisaged. Consequently, Article 51 of the UN Charter,³ which recognizes a state's inherent right of self-defense, does not explicitly provide for states using defensive force either against, or by way of, military cyber operations that can inflict disruption or damage on an adversary.

Recognizing that cyber operations can be destructive in nature and are capable of rising to the level of an armed attack, this chapter considers how states may lawfully use force in self-defense using cyber means. The applicable body of law is the *jus ad bellum*, anchored in Articles 2(4) and 51 of the UN Charter and applicable customary international law, which governs when states may use force in their international relations. Although there is widespread acceptance by states and scholars that general international law, including the *jus ad bellum*, applies in principle to cyber activities,⁴ these legal rules born of the kinetic world must be

* Many thanks to Professor Kubo Mačák for his valuable comments on an earlier draft of this chapter.

¹ 'Cyber activities' involve the use of cyber infrastructure or employ cyber means to affect the operation of such infrastructure. Cyber activities include, but are not limited to, cyber operations. 'Cyber operation' means the employment of cyber capabilities to achieve objectives in or through cyberspace, where 'cyberspace' is understood as meaning the environment formed by physical and non-physical components to store, modify, and exchange data using computer networks. See *Glossary, CYBER LAW TOOLKIT*, <https://cyberlaw.ccdcoe.org/wiki/Glossary>, which is based on and develops the glossary from TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS (Michael N. Schmitt ed., 2017).

² Pursuant to art. 2(4), states are prohibited from threatening or using force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the purposes of the United Nations.

³ Art. 51 recognizes 'the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security.'

⁴ UNGA, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, ¶ 19, U.N. Doc. A/68/98 (Jun 24, 2013). See also TALLINN MANUAL 2.0, *supra* note 1, rr. 68–75; Dapo Akande, Antonio Coco and Talita de Souza Dias, *Drawing the Cyber Baseline: The Applicability of Existing International Law to the Governance of Information*

interpreted to apply in the cyber context. Indeed, in the absence of a treaty explicitly governing cyber operations, which is unlikely soon, the regulation of self-defense using cyber means rests largely on the interpretation of these existing rules.⁵

The focus of this chapter is on the limitations imposed by the *jus ad bellum* on self-defense using cyber means by way of the customary international law requirements of necessity and proportionality. These foundational rules of the *jus ad bellum* are essential to exploring and understanding the permissible boundaries of defensive cyber operations. Necessity and proportionality determine what states may and may not do to defend themselves, meaning an understanding of how these requirements apply in the cyber context is an essential element of national cybersecurity. My aim in this chapter, therefore, is to explore how these requirements apply to persons, objects, and events in the cyber context, as well as highlighting some of the epistemic limitations of their cyber-related scope and content.

II. SELF-DEFENSE IN THE CYBER CONTEXT

A state's right of self-defense under Article 51 of the UN Charter is triggered by the occurrence of an 'armed attack'. Such right undoubtedly applies in the cyber context.⁶ It is widely accepted that certain cyber operations, or so-called 'cyberattacks',⁷ are capable of rising to the level of armed attacks, thereby triggering a state's right of self-defense.⁸ That armed attacks may be entirely comprised of cyber operations (without a kinetic element) accords with the idea that international law is technologically neutral, meaning that it applies by default, and to the extent relevant, to all technologies, old and new.⁹ This conclusion reflects recognition by the International Court of Justice (ICJ) that Articles 2(4) and 51 of the UN Charter do not refer to specific weapons and, therefore, 'apply to any use of force, regardless of the weapons employed.'¹⁰ More importantly, this conclusion accords with state practice.¹¹

Characterizing cyberattacks as 'armed attacks' is part of determining how states may lawfully respond to malicious cyber activities directed against them, including by using force. Absent an armed attack, states may not use force to respond to malicious cyber activities by

and Communication Technologies, 99 INTERNATIONAL LAW STUDIES 4 (2022); Michael N. Schmitt and Anusha S. Pakkam, *Cyberspace and the Jus ad Bellum: The State of Play*, 103 INTERNATIONAL LAW STUDIES 194 (2024), at 199–200, 209. See further Section II.

⁵ Michael N. Schmitt, *The Law of Cyber Conflict: Quo Vadis 2.0?*, in THE FUTURE LAW OF ARMED CONFLICT 103, 105–7, 121 (Matthew C. Waxman and Thomas W. Oakley eds., 2022) (Vol. 7, Lieber Studies).

⁶ Schmitt and Pakkam, *supra* note 4, at 209. Regarding recent state practice on this point, see AFRICAN UNION PEACE AND SECURITY COUNCIL, COMMON AFRICAN POSITION ON THE APPLICATION OF INTERNATIONAL LAW TO THE USE OF INFORMATION AND COMMUNICATION TECHNOLOGIES IN CYBERSPACE 6–7 (2024); COUNCIL OF THE EUROPEAN UNION, DECLARATION ON A COMMON UNDERSTANDING OF INTERNATIONAL LAW IN CYBERSPACE 10 (2024). For other supportive national positions, see *Self-defence*, CYBER LAW TOOLKIT, <https://cyberlaw.ccdcoe.org/wiki/Self-defence>.

⁷ 'Cyberattacks' are a form of cyber operation designed to disrupt, deny, degrade, or destroy information on computers and computer networks, or the computer networks themselves. Russell Buchan, *Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions*, 17(2) JOURNAL OF CONFLICT & SECURITY LAW 211 (2012), at 211. Although taxonomy varies, this definition of cyberattacks is commonly cited and accords with both US and NATO policy. See Marco Roscini, CYBER OPERATIONS AND THE USE OF FORCE IN INTERNATIONAL LAW 13, 17 (2014).

⁸ TALLINN MANUAL 2.0, *supra* note 1, r. 71.

⁹ Akande *et al*, *supra* note 4, at 25, 27.

¹⁰ Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J Rep. 226, ¶ 39 (July 8).

¹¹ See the common and national positions in *Self-defence*, CYBER LAW TOOLKIT, *supra* note 1.

cyber or conventional means without breaching Article 2(4) of the UN Charter. Instead, states are limited to non-forcible measures to counter actions falling below the threshold of an armed attack.¹² The initial hurdle for states in assessing whether they have a legal right to defend themselves using force by cyber means is that the meaning of ‘armed attack’ is unsettled. Neither the UN Charter nor any other treaty provides a definition.¹³ This epistemic dilemma applies both to cyber and kinetic operations.¹⁴

In the cyber context, it is widely accepted that the governing factor is whether the scale and effects of cyber operations are analogous to kinetic uses of force in that they meet the *Nicaragua* gravity threshold and comprise the ‘most grave’ forms of a use of force to be regarded as armed attacks.¹⁵ Beyond that general premise, however, there is no consensus regarding how this assessment, based on various contextual factors, should be made. Accordingly, although state practice is evolving and might provide greater clarity in time, ‘no bright line test exists for distinguishing a cyber operation that qualifies as a cyber armed attack from one that does not.’¹⁶

For our consideration of the limits of self-defense using cyber means, whether attacks are comprised solely of kinetic or cyber activities, or a combination of the two, being able to surpass the armed attack threshold is not the only hurdle that states must overcome. Even where armed attack claims may be justified, there is no automaticity regarding the right to respond using force. The right of self-defense using cyber means, as with kinetic means, is further limited by additional requirements of international law.

III. THE LIMITS OF SELF-DEFENSE USING CYBER MEANS

To be considered lawful, all defensive actions comprising uses of force must comport with the customary international law requirements of necessity and proportionality.¹⁷ The *jus ad bellum*, including these requirements, applies equally to self-defense using cyber and conventional means.¹⁸ As such, necessity and proportionality apply to the entirety of defensive operations, alongside and in addition to the rules of international humanitarian law (IHL), to condition the exercise of that right so that force used is contained and confined purely to the defensive.¹⁹

¹² See Section IIIA.

¹³ *Military and Paramilitary Activities in and against Nicaragua (Nicar. v. U.S.)*, Judgment, 1986 I.C.J. Rep. 14, ¶ 176 (June 27).

¹⁴ On the latter, see TOM RUYTS, ‘ARMED ATTACK’ AND ARTICLE 51 OF THE UN CHARTER: EVOLUTIONS IN CUSTOMARY LAW AND PRACTICE (2010).

¹⁵ ‘Less grave’ uses of force do not constitute armed attacks. *Nicaragua*, *supra* note 13, at ¶¶ 191, 195. See further TALLINN MANUAL 2.0, *supra* note 1, r. 71; Schmitt and Pakkam, *supra* note 4, at 212–20.

¹⁶ Michael N. Schmitt and Liis Vihul, *European Approaches to the Application of International Law in Cyberspace: A Comparative Legal Analysis*, 45 (European Union Institute for Security Studies, 2024), at 47. See further TALLINN MANUAL 2.0, *supra* note 1, r. 71.

¹⁷ *Nicaragua*, *supra* note 13, at ¶ 176; *Nuclear Weapons*, *supra* note 10, at ¶ 41; *Oil Platforms (Iran v. U.S.)*, Judgment, 2003 I.C.J. Rep. 161, ¶¶ 73–77 (Nov. 6).

¹⁸ TALLINN MANUAL 2.0, *supra* note 1, r. 72; Schmitt and Pakkam, *supra* note 4, at 211.

¹⁹ Ruys, *supra* note 14, at 124; Eliav Lieblich, *On the Continuous and Concurrent Application of Ad Bellum and In Bello Proportionality*, in NECESSITY AND PROPORTIONALITY IN INTERNATIONAL PEACE AND SECURITY LAW 41 (Claus Kreß and Robert Lawless eds., 2020); CHRIS O’MEARA, NECESSITY AND PROPORTIONALITY AND THE RIGHT OF SELF-DEFENCE IN INTERNATIONAL LAW 84–93, 166–70 (2021).

Compliance with these requirements, while initially assessed subjectively from the perspective of a state that is the victim of an armed attack, is ultimately judged objectively, whether by a court or (more likely) by other states and international organizations.²⁰

Cyber-specific state practice and publicly available expressions of *opinio juris* are relatively sparse,²¹ meaning that it is often difficult to conclude definitively that any cyber-specific customary international law norm exists.²² Pending the identification of new cyber-specific rules, how necessity and proportionality apply to cyber activities therefore depends on interpreting existing norms, which continue generally to govern state conduct.²³ The unique characteristics of cyber operations mean that a direct transposition of rules that apply to traditional kinetic operations is not always appropriate, however. Our understanding of necessity and proportionality must consequently be adapted to apply to the cyber context. The following sections explore how we might approach this interpretative challenge.

A. Necessity

In response to an armed attack (whether conventional, cyber, or a combination of the two) necessity requires that defensive cyber operations that amount to uses of force must be measures of last resort. This means that alternatives to force are unavailable or unfeasible and/or, on their own, will be ineffective to halt or repel an armed attack, or (if a right of anticipatory self-defense is accepted) prevent an armed attack that is imminent.²⁴ In short, resort to force must be the only reasonable choice of means available to a state in the circumstances.²⁵ If not necessary, using force will be unlawful.

For defense using cyber means to be necessary, therefore, alternatives to force must be impractical or unlikely to be effective in countering an armed attack, or not have a reasonable chance of doing so, if used exclusively.²⁶ When considering recourse to self-defense in general terms, such alternatives typically include non-forceful measures like law enforcement,²⁷ diplomacy, retorsion, dispute resolution, and/or non-military countermeasures.²⁸ Likewise, it is

²⁰ See Oil Platforms, *supra* note 17, at ¶ 73.

²¹ Most states are yet to express their views on international law's regulation of cyber operations. However, states and international organizations are increasing engaging with this issue, including by setting out public positions and making other official statements. See *National Position*, CYBER LAW TOOLKIT, https://cyberlaw.ccdcoe.org/wiki/Category:National_position.

²² Questioning whether domain-specific state practice and *opinio juris* are required, see Akande *et al*, *supra* note 4, especially at 19–28, 35–36. On the requirements of customary international law, see *North Sea Continental Shelf (F.R.G. v. Den., F.R.G. v. Neth.)*, Judgment, 1969 I.C.J. Rep. 3, ¶ 77 (Feb. 20); International Law Commission, Draft Conclusions on Identification of Customary International Law with Commentaries, U.N. Doc. A/73/10 (2018).

²³ Akande *et al*, *supra* note 4, at 35. See also Kubo Mačák, *Unblurring the Lines: Military Cyber Operations and International Law* 6(3) JOURNAL OF CYBER POLICY 411 (2021), at 415–17.

²⁴ On anticipatory self-defense and the meaning of imminence, see notes 62–78 and accompanying text.

²⁵ O'Meara, NECESSITY AND PROPORTIONALITY, *supra* note 19, at 38–42. See further TALLINN MANUAL 2.0, *supra* note 1, r. 72, at 348–49.

²⁶ Elizabeth Wilmshurst, *The Chatham House Principles of International Law on the Use of Force in Self-Defence* 55(4) INTERNATIONAL AND COMPARATIVE LAW QUARTERLY 963 (2006), at 967. Similarly, the Tallinn Manual 2.0 stipulates that necessity requires non-forceful measures to be 'insufficient' to address the situation. TALLINN MANUAL 2.0, *supra* note 1, r.72, at 348.

²⁷ Attempts at law enforcement measures before resorting to active defensive measures might be an official policy preference for states and might be explored in cooperation with states from which cyberattacks by NSAs originate. See Roscini, *supra* note 7, at 89.

²⁸ See generally, Roscini, *supra* note 7, at 104–10.

possible that UN Security Council action results in effective measures to remove the threat.²⁹ Only where non-forceful alternatives, on their own, are insufficient to respond to an armed attack is there a necessity of using force in self-defense by way of conventional or cyber operations.³⁰

In the cyber context specifically, obvious alternatives to force include cyber operations falling below that threshold. Accordingly, where passive (as distinct from active) cyber defenses are adequate to reliably and completely thwart a cyber armed attack, neither cyber or kinetic forcible responses will be necessary.³¹ Passive cyber defenses (such as firewalls, honeypots, encryption, patches, anti-virus software, intrusion detection and prevention devices, and other tools) defend computers and networks by detecting and mitigating cyber intrusions and making systems more resilient to attack. Although they might successfully prevent hackers from accessing networks or computers, passive cyber defenses do not involve coercion or unauthorized intrusions into an assailant's computer systems, meaning they do constitute uses of force that require a self-defense justification.³² Similarly, if a vulnerability in a state's cyber defenses can be repaired or patched to deny future incursions, the bolstering of those defenses might, depending on the circumstances, be a sufficient non-forceful alternative that makes using force unnecessary.³³

Beyond passive measures, if active cyber defense operations falling below the threshold of using force can be used to thwart armed attacks effectively, necessity acts as a bar to forceful cyber and kinetic alternatives.³⁴ The danger, however, is that active cyber defenses (unlike their passive cousins) are in-kind responses to cyberattacks. Because they comprise cyber counter-operations against the source, they are themselves regarded as cyberattacks against an adversary.³⁵ Although they can be benign in nature, active cyber defenses do range to the more aggressive and accordingly risk crossing the threshold into uses of force, particularly if physical effects result from their use.³⁶

Necessity goes beyond the no choice of means obligation, requiring that targets of defensive force serve a defensive purpose.³⁷ This means that defensive force should in principle be directed against the source of the armed attack being halted, repelled, or prevented³⁸ and be

²⁹ Pursuant to Art. 51 of the UN Charter, the right of self-defense remains unimpaired until the UNSC takes 'necessary measures' to restore international peace and security. Recourse to the UN Security Council to respond to specific cyberattacks is perhaps an unrealistic alternative, however, given the unpredictability and speed of such attacks.

³⁰ Necessity does not require force to be the only response used to resolve the situation. Force may be combined with non-forceful measures.

³¹ TALLINN MANUAL 2.0, *supra* note 1, r. 72, at 349; Carlo Focarelli, *Self-Defense in Cyberspace*, in RESEARCH HANDBOOK ON INTERNATIONAL LAW AND CYBERSPACE 335 (Nicholas Tsagourias and Russell Buchan eds., 2d ed. 2021).

³² See Roscini, *supra* note 7, at 14, 69; *Glossary*, *supra* note 1. Such measures may nevertheless require justification by reference to other bodies of domestic or international law.

³³ Laurie R. Blank, *International Law and Cyber Threats from Non-State Actors*, 89 INTERNATIONAL LAW STUDIES 406 (2013) 418.

³⁴ TALLINN MANUAL 2.0, *supra* note 1, r. 72, at 349.

³⁵ Roscini, *supra* note 7, at 14; *Glossary*, *supra* note 1.

³⁶ See Matthias Schulze, *Syntax: Subjects and Objects in Active Cyber Defence*, in A LANGUAGE OF POWER? CYBER DEFENCE IN THE EUROPEAN UNION 32 (European Union Institute for Security Studies, Patryk Pawlak and François Delerue eds. 2022).

³⁷ See O'Meara, NECESSITY AND PROPORTIONALITY, *supra* note 19, at 84–93.

³⁸ Ruys, *supra* note 14, at 108–9.

limited to military targets connected with the armed attack.³⁹ As noted, these *jus ad bellum* rules apply independently and in addition to IHL targeting rules. Consequently, states must direct acts of defense using cyber means at the perpetrator of the armed attack and no other.⁴⁰ As an initial practical matter, this means that cyber defenders may only deploy cyber weapons that are capable of being so directed. Certain means of cyber self-defense may be technically capable of complying with this requirement. Others, however, may not be able to be used in a targeted fashion, given the nature of the weapon and/or because of the interconnected nature of cyberspace.⁴¹ An obvious example is computer worms that self-replicate, which risks their spread into computers and systems beyond those belonging to the perpetrator of the armed attack.⁴² If this is the case, their use will *prima facie* fail to satisfy the necessity requirement.⁴³

Beyond the means of self-defense, targeting the attacker also requires legal attribution of the armed attack to its author, whether it be a state or non-state actor (NSA). Attribution is notoriously problematic in the cyber context as both a technical and legal matter. Technological developments have made attribution easier in recent years and may be combined with intelligence and analysis of other information and relevant circumstances to make attribution possible. Yet, beyond unambiguous admission by the perpetrator or a clearly linked follow-up conventional attack revealing their identity, positive identification of the source of a cyberattack can be extremely complex and might be unreliable.⁴⁴ In part, this is because the origin of an attack and the identity of the attacker can be technically disguised or feigned by using botnets, IP spoofing that impersonates other systems or users, and other technical anonymisation techniques.

Anonymity is a feature of malicious cyber activities. Accordingly, if cyberattacks might appear to originate from computers located in a certain state, this fact does not necessarily mean that the state, or even the owners of the computers involved, were behind the cyberattacks.⁴⁵ Moreover, cyberattacks may not originate from a single source. They might be launched in or through several jurisdictions, making identifying the perpetrators, including the ‘mastermind’ behind the attack, extremely challenging.⁴⁶ The speed of cyberattacks might also act to frustrate identifying the source.

The bottom line is that if these technical and evidential issues cannot be overcome such that the author of the cyberattack can be positively identified, legal attribution will not be

³⁹ See Oil Platforms, *supra* note 17, at ¶ 51; O’Meara, NECESSITY AND PROPORTIONALITY, *supra* note 19, at 84–93, 163–6.

⁴⁰ O’Meara, NECESSITY AND PROPORTIONALITY, *supra* note 19, at 32–35.

⁴¹ See notes 86 to 88 and accompanying text.

⁴² If cyber weapons are capable of being targeted in a necessity complaint manner, they might nevertheless breach the proportionality requirement. See Section IIIB.

⁴³ In addition to potentially being prohibited by IHL targeting rules, most notably the rule of distinction.

⁴⁴ Nicholas Tsagourias, *Cyber Attacks, Self-Defence and the Problem of Attribution*, 17(2) JOURNAL OF CONFLICT & SECURITY LAW 229 (2012), at 234; Kubo Mačák, *Decoding Article 8 of the International Law Commission’s Articles on State Responsibility: Attribution of Cyber Operations by Non-State Actors*, 21(3) JOURNAL OF CONFLICT & SECURITY LAW 405 (2016), at 408, 410. See generally Nicholas Tsagourias and Michael Farrell, *Cyber Attribution: Technical and Legal Approaches and Challenges*, 31(3) EUROPEAN JOURNAL OF INTERNATIONAL LAW 941 (2020).

⁴⁵ Marco Roscini, *World Wide Warfare – Jus ad bellum and the Use of Cyber Force*, 14 MAX PLANCK YEARBOOK OF UNITED NATIONS LAW 85 (2010), at 96–97; TALLINN MANUAL 2.0, *supra* note 1, r. 15, at 91.

⁴⁶ Tsagourias, ‘*Cyber Attacks*’ *supra* note 44, at 233.

possible.⁴⁷ In such cases, necessity precludes force using cyber means as a response. It is not enough that states are subject factually to an armed attack before they may respond defensively using force. That necessity may act as a barrier to defensive responses due to the attribution requirement naturally places emphasis on alternatives to force, including passive cyber defenses.⁴⁸

The technical difficulties related to attribution are compounded by legal uncertainties pertaining to NSA cyber activities, which pose a particular challenge for states.⁴⁹ Malicious cyber operations and international terrorism have a common feature in the prominent role played by NSAs: ‘like terrorist attacks, it appears that the majority of cyber operations against states are conducted by individuals and groups.’⁵⁰ This factor makes it more difficult for states adhering to the necessity requirement when considering self-defense by cyber means, particularly when NSAs are operating in the territory of another state (the ‘host state’) and effective self-defence means targeting the NSAs in the host state. First, as with kinetic operations, there is the question of whether the relevant NSA cyber operations are legally attributable to the host state such that the NSA activities are those of the host state.⁵¹ If so, necessity allows for the targeting of both the NSAs and the host state, provided that the chosen targets of self-defense in all cases are military targets connected with the armed attack.⁵²

More controversial, however, is the legal question of whether NSA attacks absent attribution to any state can constitute armed attacks for the purposes of triggering a state’s right of self-defense.⁵³ Although this question is not unique to cyber activities, it does have additional significance in the cyber context, given the aforementioned ubiquitous role of NSAs and the particular threat that they pose to states. This is because individual hackers, hacktivist groups and terrorist groups like Al-Qaeda and ISIS, and even corporations, can carry out attacks against states using nothing more than computer programs and the internet. Given the potential damage that can be inflicted on states by private groups or solo actors, the NSA threat is a cybersecurity challenge that stretches well beyond a purely criminal law enforcement paradigm.

Accepting it is a controversial and unresolved question (with state practice being mixed), let us assume for present purposes that NSA activities are, in principle, legally capable of constituting armed attacks that trigger a state’s right of self-defense, including using cyber means.⁵⁴ The question then becomes how a victim state may respond defensively when the

⁴⁷ Regarding the required evidence and standard of proof, see Roscini, *supra* note 7, at 97–103; Tsagourias and Farrell, *supra* note 44, at 955–59.

⁴⁸ For the aforementioned reasons, however, the attribution requirement poses difficulties for any automated cyber defenses that go beyond the merely passive.

⁴⁹ See Mačák, ‘*Decoding Article 8*’, *supra* note 44, at 408, 410; Tsagourias and Farrell, *supra* note 44, at 961–65.

⁵⁰ Roscini, *supra* note 7, at 80.

⁵¹ The ICJ has determined that, subject to meeting the gravity threshold, NSA activities can be attributed legally to states, such that states may be considered to have carried out armed attacks. Nicaragua, *supra* note 13, at ¶ 195. See further Mačák, ‘*Decoding Article 8*’, *supra* note 44; Tsagourias and Farrell, *supra* note 44, at 961–65.

⁵² See O’Meara, NECESSITY AND PROPORTIONALITY, *supra* note 19, at 84–93. As noted, this *ius ad bellum* targeting requirement operates in addition to IHL targeting requirements.

⁵³ For an overview and summary of the current law, see O’Meara, NECESSITY AND PROPORTIONALITY, *supra* note 19, at 172–74.

⁵⁴ A majority of the Tallinn experts conclude that, in principle, states possess a right of self-defense in the face of NSA cyber operations at the armed attack level, absent any state involvement (TALLINN MANUAL 2.0, *supra* note 1, r. 71, at 345). State practice and other scholarship also seem increasingly to be moving in this direction,

NSA armed attack is perpetrated from foreign territory or routed through cyber infrastructure located in foreign territory. In considering their options, the mere fact that cyberattacks originate from within the territory of a host state does not automatically allow a victim state to use force against that host state, if the latter is not involved with the NSAs in a way that legally attributes the NSA cyberattacks to the host state. NSAs simply using state infrastructure to carry out a cyberattack, for example, without the relevant state's involvement or knowledge, would not suffice to make the state the author of the armed attack. Where hacker conduct cannot legally be attributed to a host state, the latter may not be considered the author of an armed attack and the object of defensive measures, therefore, but it might nevertheless be in breach of its due diligence obligation not to allow knowingly its territory to be used for acts contrary to the rights of other states.⁵⁵

A further unresolved question remains, however: where the host state is not the author of an armed attack, has not acted to effectively suppress the NSA threat, and has not consented to defensive action on its territory, are victim states nonetheless permitted to act against the NSAs on the host state territory without violating Article 2(4) of the UN Charter? A limited number of states and scholars argue in the affirmative, maintaining that where the host state is unwilling or unable to confront the NSAs and remove the threat, the victim state may lawfully act against the NSAs (but not the host state itself) on host state territory.⁵⁶ It is argued that necessity acts in such circumstances to excuse the temporary breach by the victim state of the host state's sovereignty and territorial integrity in order to target in self-defense the source of the NSA armed attack.⁵⁷ Conversely, where the host state acts effectively against the NSAs to remove the NSA threat, either unilaterally or in co-operation with the victim state, there is *prima facie* no necessity of self-defense by the victim state against the NSAs on host state territory.⁵⁸

There is a paucity of state practice (either explicit or implicit) in support of this so-called 'unwilling or unable doctrine', however, with states such as France explicitly rejecting it in the cyber context.⁵⁹ The doctrine is not clearly established in the *lex lata*, therefore, and stands as a normative proposition only, subject to acceptance (or not) by way of future state practice and *opinio juris*. As such, whether states can establish the necessity of self-defense (by cyber means

albeit that there exists no universally accepted consensus on this issue. See O'Meara, NECESSITY AND PROPORTIONALITY, *supra* note 19, at 172–74; Schmitt and Pakkam, *supra* note 4, at 223–25.

⁵⁵ Corfu Channel (U.K. v. Alb.), Judgment, 1949 I.C.J. Rep. 4, ¶ 51 (Apr. 9). The host state may thus be committing an internationally wrongful act if it does not take necessary and reasonable measures to prevent or stop an attack (e.g., by disabling the hackers' internet access or taking law enforcement measures against them). See Akande *et al.*, *supra* note 4, at 16–19, 27.

⁵⁶ See generally, Christian Henderson, THE USE OF FORCE AND INTERNATIONAL LAW 414–28 (2018). For recent scholarship in support of the doctrine's place in the *lex lata*, see Lucy V. Jordan, 'Unwilling or Unable', 103 INTERNATIONAL LAW STUDIES 151 (2024). In the cyber context, a majority of the Tallinn experts support this doctrine. TALLINN MANUAL 2.0, *supra* note 1, r. 71, at 347–48. The Tallinn commentary on the unwilling or unable doctrine occurs, however, under the general auspices of self-defense (Rule 71), rather than necessity (Rule 72). Unwillingness and/or inability on the part of the host state clearly relates to the latter requirement, however.

⁵⁷ See O'Meara, NECESSITY AND PROPORTIONALITY, *supra* note 19, at 183. See also Roscini, *supra* note 7, at 85–86.

⁵⁸ See O'Meara, NECESSITY AND PROPORTIONALITY, *supra* note 19, at 176–81.

⁵⁹ Ministry of Defense of France, *Droit International Appliqué aux Opérations dans le Cyberspace* § 1.2.3 (2019), https://www.defense.gouv.fr/sites/default/files/ministere-armees/Droit_international_applique_aux_operations_dans_le_cyberspace.pdf.

or otherwise) against armed attacks by NSAs operating in or through foreign territory remains a legally ambiguous contention.

Even for those states that do adopt the unable or unwilling doctrine, the ability to apply it in assessing the necessity of a defensive response against a target in a particular territory is subject to the aforementioned hazard of being able to positively identify the attacker, as well as the source of the attack. ‘In this respect, cyber poses perhaps unique challenges because of the ability to dissemble and present an attack as coming from one or more different States or locations, or simply because an attack passes through or can be traced back to multiple—even over a hundred—States.’⁶⁰ The legal and practical uncertainties surrounding the use of the unwilling or unable doctrine make it, therefore, an unreliable and legally risky tool for states considering the necessity of self-defense using cyber means against NSAs operating in foreign territory.

A final point for our consideration of necessity relates to a temporal issue, being the ability of states to respond defensively to future armed attacks.⁶¹ Whether states may act anticipatorily in self-defense to forestall future threats is a notoriously complex and controversial topic.⁶² The question applies to both conventional and cyber acts of self-defense, but is undoubtedly more complicated in the cyber context. Although a right of ‘preventive self-defense’ against indeterminate and unmaterialised potential future threats is almost universally rejected by states and scholars, there is widespread support among scholars for a right of ‘pre-emptive self-defense’ against ‘imminent’ armed attacks.⁶³ Nevertheless, inconclusive state practice means that this latter right still retains an uncertain place in international law.⁶⁴

For states that adopt a right of pre-emptive self-defense against imminent armed attacks, the associated technical and legal issues are likewise exacerbated in the cyber context. The most obvious technical issue is whether states are able to detect an imminent cyber armed attack in order to respond anticipatorily. Even if detection is possible, which is not always the case, cyberattacks might be launched at extraordinary speed with their consequences being immediately manifest. Moreover, cyberattacks are often ‘multi-layered’ in that ‘the malicious infiltration of the system, the execution of the payload and the production of the harmful effects may take place in different time frames.’⁶⁵ This means that when cyberattacks take place, ‘it is often not the malign act (emplacing malware) that will be noticed, but the effects of it, which may develop (much) later in time.’⁶⁶ The prospect of anticipatory defensive action in such cases essentially becomes redundant.

⁶⁰ Blank, *supra* note 33, at 417.

⁶¹ A separate temporal issue of the ‘immediacy’ of self-defense also speaks to whether it is necessary. Essentially, a state acting in self-defense (including using cyber means) must do so within a reasonable timeframe, without unduly postponing taking defensive measures. O’Meara, *NECESSITY AND PROPORTIONALITY*, *supra* note 19, at 72–76. See further TALLINN MANUAL 2.0, *supra* note 1, r. 73, at 353–54.

⁶² See generally, Chris O’Meara, *Reconceptualising the Right of Self-Defence Against ‘Imminent’ Armed Attacks* 9(2) *JOURNAL ON THE USE OF FORCE AND INTERNATIONAL LAW* 278 (2022).

⁶³ For further explanation of the terminology adopted here, see O’Meara, *‘Imminent’ Armed Attacks*, *id.*, at 282–87.

⁶⁴ *Id.* at 282–91. See also Schmitt and Pakkam, *supra* note 4, at 220–23.

⁶⁵ Tsagourias, ‘*Cyber Attacks*’, *supra* note 44, at 232.

⁶⁶ Peter B.M.J. Pijpers, Hans Boddens Hosang, and Paul A.L. Ducheine, *Dialects: Collective Cyber Defence in the EU and NATO*, in *A LANGUAGE OF POWER?*, *supra* note 36, at 75.

In considering pre-emptive self-defense using cyber means, states must also distinguish between two types of cyber operations. The first are preparatory actions, including ‘pre-positioning’,⁶⁷ which introduce vulnerabilities into systems and provide the capability to conduct future attacks, but which do not necessarily signal that an attack is imminent. The second are actions that are indicative of a realised and committed future attack and, therefore, do speak to imminence.⁶⁸ The need to distinguish is most prominent for standalone cyberattacks that are unaccompanied by conventional operations, where the latter more obviously signals a potential future threat. This distinction is perhaps easier to describe than to operationalize, however, with states needing to tread a fine line between acting too early and too late.

Further complicating this imminence calculus is the fact that the vast majority of cyber operations fall below the threshold of uses of force, which raises the further question of whether a series of connected below the threshold cyberattacks from the same source (i.e. a ‘cyber campaign’) may be aggregated together for the purposes of states assessing whether an armed attack is occurring or is likely to occur in the future. Although there is general scholarly and potential judicial support for this ‘accumulation of events’ or ‘pin prick’ theory of self-defense,⁶⁹ and examples of recent cyber-specific state practice also appear supportive,⁷⁰ this ability is by no means clearly established in the *lex lata*.

In addition to the practical issues associated with whether states can positively identify whether an armed attack is imminent (or occurring for that matter), thus justifying the necessity of self-defense, is the legal question of what is meant by ‘imminence’. Although often understood in solely temporal terms as relating to the timing of the armed attack, there is no universally agreed definition of imminence.⁷¹ Certain scholars and a limited number of states conceive of imminence as going beyond simply the timing of the armed attack and additionally comprising other non-temporal contextual factors that relate to the wider circumstances of the threat. These other factors include the nature and likelihood of the threat, its gravity, and the prospect of peaceful alternatives to counter it.⁷² On this conception, the timing factor manifests as a ‘last window of opportunity’ for a state to respond to an anticipated armed attack before it loses the opportunity to defend itself effectively.⁷³

This latter conceptualisation of ‘contextual imminence’ has limited support. It is most prominent in the context of combatting armed attacks by terrorist NSAs, which are unpredictable and may occur over a protracted period of time.⁷⁴ Similarly, however, in the cyber context there exist unique features of the threat environment. The ability of states to anticipate

⁶⁷ See Juliet Skingsley, *Cyber-Rattling: Can ‘Pre-Positioning’ in Cyberspace Amount to a Threat of the Use of Force Under Article 2(4) of the United Nations Charter?* JOURNAL ON THE USE OF FORCE AND INTERNATIONAL LAW 1 (2024).

⁶⁸ See TALLINN MANUAL 2.0, *supra* note 1, r. 73, at 352–53. If the vulnerability is discovered and can be neutralized using passive cyber defenses or active defenses below the level of a use of force, self-defense will be unnecessary. Roscini, *supra* note 7, at 79.

⁶⁹ See generally Henderson *supra* note 56, at 290–96. In the cyber context, see TALLINN MANUAL 2.0, *supra* note 1, r. 71, at 342; Schmitt and Pakkam, *supra* note 4, at 219–20.

⁷⁰ COUNCIL OF THE EUROPEAN UNION, *supra* note 6, at 6.

⁷¹ O’Meara, ‘Imminent’ Armed Attacks, *supra* note 62, at 291–95.

⁷² *Id.*, at 295–97.

⁷³ *Id.*, at 297–98.

⁷⁴ *Id.*, at 288, 304–11, 319.

when cyberattacks might be launched is limited and the consequences can manifest quickly, given the potential speed of cyberattacks.⁷⁵ Accordingly, it might also be argued that states require greater latitude to respond to future cyber threats, or otherwise risk being the victims of potentially devastating cyberattacks.⁷⁶ However, too much flexibility risks the abuse of any right of anticipatory self-defense. This is especially so if the timing of an armed attack is not considered as an independent injunction against self-defense and the last window of opportunity to act is understood as presenting itself long before the armed attack is said to occur.⁷⁷ Regardless, most states have yet to adopt a clear position on pre-emptive self-defense (whether in the cyber context or otherwise), with the African Union recently noting the uncertainties pertaining to the issue.⁷⁸ Where state practice settles on this question is yet to be seen, leaving the prospect of pre-emptive self-defense using cyber means in a grey area of legal regulation.

B. Proportionality

To be lawful under international law, any necessary acts of self-defense using cyber means must also be proportionate. In general terms, the proportionality requirement acts as a prohibition against excessive state responses in self-defense, operating to restrict how much force states use to that end.⁷⁹ Being concerned with the totality of defensive responses, proportionality requires states to balance their defense and its outcomes primarily against achieving a legitimate defensive purpose (*viz* halting, repelling, or (potentially) preventing an armed attack). Proportionality also requires that defensive operations, viewed as a whole, are not excessive in terms of the overall negative impacts they have on civilians and on the interests of other states and the international community more broadly.⁸⁰ In so doing, proportionality allows states to effectively defend themselves using cyber means or otherwise, but requires that states do no more than that. As with necessity, given the unique characteristics of cyber activities, interpreting how proportionality applies to self-defense using cyber means requires certain adaptations.

As noted, proportionality applies to the entirety of a defensive military operation, meaning that proportionality assessments should account for both the cyber and conventional elements of a defensive response. Proportionality does not mandate an in-kind response, however. There is no requirement that the means of defense match the armed attack. Force using cyber means may be deployed to counter both kinetic and cyber armed attacks.⁸¹ Indeed, a cyber response

⁷⁵ Schmitt and Pakkam, *supra* note 4, at 221.

⁷⁶ The Tallinn experts adopt the more flexible ‘last window of opportunity’ standard. TALLINN MANUAL 2.0, *supra* note 1, r. 73, at 351–52.

⁷⁷ Regarding how this fear might be mitigated, see O’Meara, ‘Imminent’ Armed Attacks, *supra* note 62, at 312–17.

⁷⁸ COMMON AFRICAN POSITION, *supra* note 6, at ¶ 42. Whether this view is cyber-specific, however, or applies generally, is unclear.

⁷⁹ O’Meara, NECESSITY AND PROPORTIONALITY, *supra* note 19, at 97–100; TALLINN MANUAL 2.0, *supra* note 1, r. 72, at 349.

⁸⁰ O’Meara, NECESSITY AND PROPORTIONALITY, *supra* note 19, at 100–25, 139–55.

⁸¹ TALLINN MANUAL 2.0, *supra* note 1, r. 72, at 349; Schmitt and Pakkam, *supra* note 4, at 211–12. The same is true for kinetic self-defense. See O’Meara, NECESSITY AND PROPORTIONALITY, *supra* note 19, at 127–30.

to a cyberattack may not be an effective defensive option where the attacker is low technology or has limited digital infrastructure to hit, meaning it is not vulnerable to cyber operations.⁸² In such instances, cyber operations are unlikely to achieve defensive outcomes, meaning kinetic force will be required. Alternatively, the victim state may not possess the requisite cyber technology to respond in kind, again requiring a conventional response. Cyber and kinetic operations may also be combined. Proportionality does not address the particular method of response, therefore, but what total amount of force (of any kind) is used to achieve an effective defense. A state may use whatever force is required, including of means and scale to halt, repel or (maybe) prevent an armed attack, *but no more than that*.⁸³

Applying these general proportionality requirements to the cyber context is a precarious and uncertain exercise. Calibrating the required response to cyber armed attacks might be particularly challenging if the precise nature and scale of the attack is unknown at the time the defensive response is considered or undertaken.⁸⁴ The challenge is compounded if states adopt the accumulation of events doctrine to determine the existence of an armed attack in the face of a cyber campaign over a protracted period of time.⁸⁵ As a strategic matter, therefore, cyber defenders are well-advised to limit initial cyber defense operations until the full threat is realised, or otherwise risk a response that is later deemed disproportionate and unlawful.

Calibrating defensive cyber responses for proportionality compliance purposes is further complicated by the interconnected nature of cyberspace. Cyberspace is predominantly used for civilian purposes and civilian and military networks may be connected. Indeed, military networks often rely on civilian cyber infrastructure (such as undersea fibre-optic cables, satellites, routers, nodes, etc) and civilian vehicles, shipping, and air traffic controls increasingly rely on navigation satellite systems that may also be used by the military. Civilian logistical supply chains and essential civilian services also use the same web and communication networks through which some military communications pass.⁸⁶ Although defensive cyber operations might be effective without causing harm to civilians or civilian infrastructure,⁸⁷ defensive (like offensive) cyber operations have significant potential to produce secondary effects beyond the initial direct effects on an attacked computer, system, or network.

The interconnected nature of cyberspace means that a defensive cyber operation against a specific military system connected with an armed attack (thereby satisfying the necessity requirement) might nevertheless produce effects that spread well beyond the originally intended target. Harm might be caused to other states, including to their public systems and infrastructure, as well as their legally protected interests.⁸⁸ Given that civilian harm is the

⁸² This is most likely with cyberattacks by NSAs, which require limited resources to carry out cyberattacks and, therefore, do not possess the available targets for self-defense that states possess. Blank, *supra* note 33, at 419.

⁸³ O'Meara, NECESSITY AND PROPORTIONALITY, *supra* note 19, at 129–30.

⁸⁴ See notes 65–66 and accompanying text.

⁸⁵ See notes 69–70 and accompanying text.

⁸⁶ These represent particular features of cyberspace, as noted by the ICRC in its assessment of possible civilian harms resulting from military operations in cyberspace. ICRC, INTERNATIONAL HUMANITARIAN LAW AND CYBER OPERATIONS DURING ARMED CONFLICTS 6–7 (2019).

⁸⁷ The ICRC has noted the potential for cyber tools to be designed and used in a targeted and 'discriminate' way, thus not necessarily posing harm to civilians. *Id.*, at 5.

⁸⁸ An example of the latter interest, and relevant to the proportionality calculus, is a state's neutrality. See O'Meara, NECESSITY AND PROPORTIONALITY, *supra* note 19, at 147–53.

clearest indicator of disproportionality,⁸⁹ however, most significant are the potential deleterious effects on civilian systems, any infrastructure operated by those systems, as well as possible physical harm to civilians and other civilian property ultimately affected by an attack.

Conventional self-defense operations can likewise produce harm beyond the immediate damage or destruction to the original target. Yet, cyber operations are physically unique, which magnifies this concern. As the International Committee of the Red Cross (ICRC) notes, ensuring that cyber operations affect only the targeted object ‘may be technically challenging and require careful planning in their design and use’.⁹⁰ Indeed, on the increased likelihood of unforeseen harm resulting from cyber operations, those carrying out cyberattacks (in defense or offensive) ‘because of automatic routing mechanisms, may not be able to control, or even accurately predict, the cyber pathway to the target’, which increases the risk of unintended consequences.⁹¹ The ICRC also warns that certain cyber tools have been deliberately designed to self-propagate, meaning that the program replicates itself and spreads, with the ability to indiscriminately affect other computer systems.⁹²

Depending on the object of the defensive response and the cyber tool used to carry it out, the potential ripple effects of cyberattacks mean that quantifying potential harm for the purposes of proportionality compliance is an unenviable task for the cyber defender and the *ex post* reviewer of self-defense using cyber means. The unique features of cyber operations and society’s reliance on cyberspace further complicates this assessment, as the indirect and secondary consequences of certain cyber operations are potentially of greater significance than the immediate and direct consequences for the proportionality calculus.⁹³ The risk of malware spreading uncontrollably and infecting both military and civilian systems means that the overall effects of the malware are potentially unforeseeable. The possibility of unquantifiable harm, most importantly to civilians, means that compliance with the proportionality requirement might be impossible in specific circumstances. In such cases, the particular cyber means of self-defense will be prohibited under the *jus ad bellum*.⁹⁴

This compliance risk means that cyber defenders must be prudent in their choice of tools for self-defense and be cognizant of the possible wider effects of their defensive cyber operations, beyond their immediate defensive needs. At a strategic level, there needs to be awareness that this *jus ad bellum* proportionality assessment operates in addition to IHL targeting requirements that attach at an operational level to individual cyberattacks, requiring a global assessment of civilian harm resulting from the defensive military operation taken as a whole. Compliance with the proportionality requirement will ultimately be assessed on a case-by-case basis in light of the relevant circumstances. However, meeting the requirement is likely to depend on whether, as a technical matter, the cyber tool used in self-defense has been specifically tailored with this overriding defensive purpose in mind.⁹⁵

⁸⁹ O’Meara, NECESSITY AND PROPORTIONALITY, *supra* note 19, at 139–46.

⁹⁰ ICRC, *supra* note 86, at 5.

⁹¹ Michael N Schmitt, *Computer Network Attack: The Normative Software*, 4 YEARBOOK OF INTERNATIONAL HUMANITARIAN LAW 53 (2001) 56.

⁹² ICRC, *supra* note 86, at 5.

⁹³ Matthew C Waxman, *Cyber Attacks and the Use of Force: Back to the Future of Article 2(4)*, 36 YALE JOURNAL OF INTERNATIONAL LAW 421 (2011) 445.

⁹⁴ IHL compliance is also unlikely in these circumstances.

⁹⁵ See Roscini, *supra* note 7, at 91.

IV. CONCLUDING THOUGHTS

The meaning of ‘armed attack’ as the initial threshold question for determining whether force is a lawful defensive response available to states using cyber means remains to be clarified by state practice. Recent engagement by states and international organizations on this question demonstrates how this is a pressing concern for states. Yet, it is not the only (or even the most important) factor in considering the limits that international law places on self-defense in the cyber context. After all, rhetorical recourse to self-defense being ‘necessary and proportionate’ is the standard ‘ritual incantation’ that states offer to justify defensive actions, meaning that these requirements best represent how states view their right of self-defense, explain their actions publicly, and review the defensive acts of other states.⁹⁶ Greater focus by states and scholars on developing how the requirements of necessity and proportionality apply to defensive cyber operations will accordingly serve to clarify the limits of self-defense, as and when states seek to justify cyber operations on that basis.

This chapter has highlighted some of the key aspects of states acting defensively using cyber means and has explored how the requirements of necessity and proportionality might apply to restrain the exercise of that right. The analysis has sought to focus attention on these constituent elements of self-defense and to raise awareness of the current limitations of our understanding of how they operate in the cyber context. Although the general boundaries of defensive cyber operations are revealed by means of interpretation by reference to conventional military operations, significant ambiguities and uncertainties remain.

The *jus ad bellum* will always be an indeterminate regime by its nature, but the lack of focus on necessity and proportionality in the cyber context restricts the potential for greater determinacy, leaving states increased leeway to use force using cyber means. This is to the detriment of maintaining international peace and security. The hope, therefore, is that additional focus by states and scholars on necessity and proportionality in the cyber context will help to promote predictability, avoid escalatory responses, protect civilians, and ultimately enhance state cyber security. Although the path to greater determinacy will undoubtedly not be smooth, ‘[t]he vector of the interpretive efforts in support of international law is clearly positive’,⁹⁷ which should provide some solace that the *jus ad bellum* has real potential to operate more effectively to govern cyber operations.

⁹⁶ O’Meara, NECESSITY AND PROPORTIONALITY, *supra* note 19, at 1–3, 8–9, 231–32.

⁹⁷ Schmitt, *Quo Vadis 2.0?*, *supra* note 5, at 121.