TALLINN PAPERS

Jeremy K. Davis

Developing Applicable Standards of Proof for Peacetime Cyber Attribution

Tallinn Paper No. 13
2022

CCDCOE
NATO COOPERATIVE
CYBER DEFENCE
CENTRE OF EXCELLENCE

Previously in This Series

No. 1 Kenneth Geers 'Pandemonium: Nation States, National Security and the Internet' (2014)

No. 2 Liis Vihul 'The Liability of Software Manufacturers for Defective Products' (2014)

No. 3 Hannes Krause 'NATO on Its Way Towards a Comfort Zone in Cyber Defence' (2014)

No. 4 Liina Areng 'Lilliputian States in Digital Affairs and Cyber Security' (2014)

No. 5 Michael N. Schmitt and Liis Vihul 'The Nature of International Law Cyber Norms' (2014)

No. 6 Jeffrey Carr 'Responsible Attribution: A Prerequisite for Accountability' (2014)

No. 7 Michael N. Schmitt 'The Law of Cyber Targeting' (2015)

No. 8 James A. Lewis 'The Role of Offensive Cyber Operations in NATO's Collective Defence' (2015)

No. 9 Wolff Heintschel von Heinegg 'International Law and International Information Security: A Response to Krutskikh and Streltsov' (2015)

No. 10 Katrin Nyman Metcalf 'A Legal View On Outer Space and Cyberspace: Similarities and Differences' (2018)

No. 11 David Wallace 'Cyber Weapon Reviews under International Humanitarian Law: A Critical Analysis' (2018)

No. 12 Elaine Korzak 'Russia's Cyber Policy Efforts in the United Nations' (2021)

No. 13 TALLINN PAPERS YOUNG SCHOLAR EDITION: Garrett Derian-Toth, Ryan Walsh, Alexandra Sergueeva, Edward Kim, Alivia Coon, Hilda Hadan and Jared Stancombe 'Opportunities for Public and Private Attribution of Cyber Operations' (2021)

Disclaimer

The Tallinn Papers

The NATO CCD COE's Tallinn Papers are designed to inform strategic dialogue regarding cyber security within the Alliance and beyond. They address cyber security from a multidisciplinary perspective by examining a wide range of issues, including cyber threat assessment, domestic and international legal dilemmas, governance matters, assignment of roles and responsibilities for the cyber domain, the militarisation of cyberspace and technical. Focusing on the most pressing cyber security debates, the Tallinn Papers aim to support the creation of a legal and policy architecture that is responsive to the peculiar challenges of cyberspace. With their future-looking approach, they seek to raise awareness and to provoke the critical thinking that is required for well-informed decision-making on the political and strategic levels.

Submissions

The Tallinn Papers is a peer-reviewed publication of the NATO Cooperative Cyber Defence Centre of Excellence. Although submissions are primarily commissioned by invitation, proposals dealing with issues of strategic importance and acuteness will be considered on an exceptional basis. Since the Tallinn Papers are meant for a wide audience, such proposals should assume no prior specialised knowledge on the part of the readership. Authors wishing to submit a proposal may contact the Editor-in-Chief at publications@ccdcoe.org

Developing Applicable Standards of Proof for Peacetime Cyber Attribution

Jeremy K. Davis*

Introduction

Strained inter-state relationships and strategic competition are increasingly finding their expression in the cyberspace domain. The United States and Israel reportedly masterminded the 2009–2010 Stuxnet operation destroying centrifuges at the Natanz nuclear facility in Iran.[1] Russia meddled in the 2016 and 2020 US presidential elections.[2] North Korea perpetrated the 2017 WannaCry malware operation infecting hundreds of thousands of computers globally.[3] The US, in 2019, allegedly disabled Iranian computer systems being used to plan attacks on oil tankers in the Persian Gulf.[4] Russia conducted the 2020 SolarWinds malware operation that affected US government agencies and private sector companies.[5]

* Lieutenant Colonel (ret.), Judge Advocate General's Corps, US Air Force; former Associate Director for Airspace, Outer Space and Cyberspace Operations and Military Professor, Stockton Center for International Law, US Naval War College. The thoughts and opinions expressed are those of the author and not necessarily those of the US government, the US Department of Defense or the US Naval War College.

[1] David E. Sanger, *Obama Order Sped Up Wave of Cyberattacks Against Iran*, N.Y. TIMES (Jun. 1, 2012), https://www.nytimes.com/2012/06/01/world/middleeast/obamaordered-wave-of-cyberattacks-against-iran.html; Ellen Nakashima & Joby Warrick, *Stuxnet was work of US and Israeli experts, officials say*, WASH. POST (Jun. 2, 2012), https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAInEy6U_story.html.

[2] Report of the Select Committee United States Senate on Russian Active Measures Campaigns and Interference in the 2016 Election, Vol. 1, Redacted Ed., S. Rep. No. 116-XX (2019), https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume1.pdf; Office of the Director of National Intelligence, Press Release, *Statement by NCSC Director William Evanina: Election Threat Update for the American Public* (Aug. 7, 2020) https://www.dni.gov/index.php/newsroom/press-releases/item/2139-statement-by-ncsc-director-william-evanina-election-threat-update-for-the-american-public.

[3] The White House, Press Release, *Press Briefing on the Attribution of the WannaCry Malware Attack to North* Korea (Dec. 19, 2017), https://www.whitehouse.gov/briefings-statements/press-briefing-on-the-attribution-of-the-wannacry-malware-attack-to-north-korea-121917/; United Kingdom, Foreign and Commonwealth Office, Press Release, *Foreign Office Minister Condemns North Korean Actor for WannaCry Attacks* (Dec. 19, 2017), https://www.gov.uk/government/news/foreign-office-ministercondemns-north-korean-actor-for-wannacry-attacks; US Department of Homeland Security, Cybersecurity & Infrastructure Security Agency, Alert (TA17-132A), Indicators Associated With WannaCry Ransomware (May 12, 2017), https://uscert.cisa.gov/ncas/alerts/TA17-132A.

[4] Ellen Nakashima, *Trump Approved Cyber-strikes against Iranian Computer Database Used to Plan Attacks on Oil Tankers*, WASH. POST (Jun. 22, 2019), https://www.washingtonpost.com/world/national-security/with-trumps-approval-pentagon-launched-cyberstrikes-against-iran/2019/06/22/250d3740-950d-11e9-b570-6416efdc0803_story.html?noredirect=on.

[5] The White House, Press Release, *FACT SHEET: Imposing Costs for Harmful Foreign Activities by the Russian Government* (Apr. 15, 2021), https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/15/fact-sheet-imposing-costs-for-harmful-foreign-activities-by-the-russian-government/.

States broadly agree that cyberspace is not a lawless void.[6] Extant international law governs cyber activities whether one conceives of cyberspace as a warfighting domain[7] or, more broadly, as a strategic domain.[8] Calls to negotiate and conclude a new treaty governing cyber operations will likely be unsuccessful and, unfortunately, the two main forums aimed at achieving state consensus regarding how existing international law applies to state cyber activities – the United Nations Group of Governmental Experts ('GGE') and the United Nations Open-ended Working Group ('OEWG') – have so far yielded only tepid results.[9] While the pursuit of broad international understanding concerning what constitutes lawful cyber activity remains ongoing, states are (or should be) examining the legal and policy parameters governing their pre-planned and anticipated responses to both lawful and unlawful hostile cyber operations.[10]

To date, the GGE, the OEWG and states in their official statements have focused on the conformity of state cyber operations with existing norms of international law. Primary rule questions such as when a cyber operation constitutes an armed attack and how the principle of proportionality applies to cyber operations will likely be answered either by 'as is' application of well-settled international law or through evolutionary changes to international law resulting from state interpretation. States have seemingly eschewed identifying the quantum of evidence necessary to validate their cyber attributions[11] because questions of cyber attribution involve secondary rules of international law that are 'notoriously underdeveloped even outside the cybersecurity context'.[12]

This article adopts an international relations-based approach to standards of proof for cyber attribution, concentrating on the development of international norms of evidence applicable to state-on-state hostile cyber operations. This article will illuminate the lack of law on standards of proof for peacetime cyber attribution, discuss the complexities those missing standards introduce into the foreign relations calculus and propose discrete standards of proof that will provide a uniform frame of analysis by which to critique a victim state's attribution and resulting response.

---

[6] See, e.g., Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (2013), transmitted by Letter Dated 24 June 2013, U.N. Doc. A/68/98 (Jun. 24, 2013) [hereinafter 2013 GGE Report]; Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (2015), transmitted by Letter Dated 22 July 2015, U.N. Doc. A/70/174 (Jul. 22, 2015) [hereinafter 2015 GGE Report]; Report of the Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security (2021), transmitted by Letter Dated 28 May 2021, U.N. Doc. A/76/135 (Jul. 14, 2021) [hereinafter 2021 GGE Report]; Report of the OEWG on Developments in the Field of Information and Telecommunications in the Context of International Security (2021), U.N. Doc. A/AC.290/2021/CRP.2 (Mar. 10, 2021) [hereinafter 2021 OEWG Report].

[7] See, e.g., Mark Esper, Secretary of Defense, US Department of Defense, Address at the Department of Homeland Security Cybersecurity and Infrastructure Security Agency's Second Annual Cybersecurity Summit (Sept. 20, 2019).

[8] See, e.g., Michael P. Fischerkeller, *Current International Law Is Not an Adequate Regime for Cyberspace*, LAWFARE (Apr. 22, 2021), https://www.lawfareblog.com/current-international-law-not-adequate-regime-cyberspace.

[9] See Gary D. Brown, *State Cyberspace Operations: Proposing a Cyber Response Framework*, 2–3 Royal United Services Institute for Defence and Security Studies (2020). See also 2013 GGE Report, *supra* note 6; 2015 GGE Report, *supra* note 6; 2021 GGE Report, *supra* note 6; 2021 OEWG Report, *supra* note 6.

[10] See, e.g., North Atlantic Treaty Organization, Ministry of Defence, AJP-3.20 (ed. A, v.1), Allied Joint Doctrine for Cyberspace Operations, 3.3–3.7 (2020), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/899678/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf.

[11] See Marco Roscini, *Evidentiary Issues in International Disputes Related to State Responsibility for Cyber Operations*, 50 TEX. INT'L L. J. 233, 238 (2015). See also, e.g., 2015 GGE Report, *supra* note 6, 28(f); 2021 GGE Report, *supra* note 6, 71(g).

[12] Kristen Eichensehr, *The Law & Politics of Cyberattack Attribution*, 67 UCLA L. REV. 520, 524 (2020).

What is Attribution?

Any parent will attest that when something crashes or breaks or when someone gets hurt, the reflexive question is, 'who did it?' The same holds when states seek to respond to hostile cyber operations. The simplest definition of attribution is the identification of the actor responsible,[13] but those working at the intersection of law, foreign policy and cyber recognise that a colloquial understanding of attribution is overly simplistic.

Attribution is a term of art in both international law and the foreign policy arena. Identifying the state to blame for a hostile cyber operation requires diligent investigation and precision because '[a]ccurate attribution of cyberattacks is a crucial predicate to a wide range of related or responsive actions'.[14] To have a meaningful discussion about cyber attribution, it is important to understand there are three distinct but interrelated forms of attribution: technical, political and legal.

Technical attribution is '[i]dentifying the machine from which an attack was launched'.[15] Unfortunately, cyberspace facilitates anonymity rather than accountability and deterrence.[16] Although highly cyber-capable states are becoming increasingly skilled at identifying the technical point of origin of cyber operations,[17] malign actors' ability to misrepresent their precise location through spoofing or to delay detection by routing the cyber operation through innocent systems and infrastructure en route to the target makes technical attribution difficult.[18]

Regrettably, identifying the physical terminal from which a hostile cyber operation originates reveals little, if anything, about the identity and motives of the actor at the keyboard.[19] There is a world of difference, both legally and diplomatically, between an independent hacker looking to challenge themself by targeting a foreign government system, a sympathetic collective of hackers making a political statement and a state violating international law. Technical attribution is an enabler; states that can reliably and confidently identify hostile cyber operations' origins are better positioned to politically and legally attribute than those lacking that forensic capability.[20]

Political attribution of a hostile cyber operation requires a state to publicly admit it has been victimised. It also means the victim state is sufficiently confident in its assessment to make the foreign policy decision to publicly assign blame to another state. Political attribution takes a variety of forms, including official statements,[21] diplomatic demands that the offending state cease and

[13] See William Banks, *State Responsibility and Attribution of Cyber Intrusions after Tallinn 2.0*, 95(7) TEX. L. REV. 1487, 1492 (2017); David D. Clark & Susan Landau, *Untangling Attribution,* 2 HARV. NAT'L SEC. J. 323, 323–24 (2011).
[14] Eichensehr, *supra* note 12, 522. See also Nicholas Tsagourias, *Cyber Attacks, Self-Defence and the Problem of Attribution*, 17 J. CONFLICT & SEC. L. 229, 230 (2012).
[15] Eichensehr, *supra* note 12, 528.
[16] See Banks, *supra* note 13, 1492 (2017).
[17] See, e.g., James R. Clapper, Director of National Intelligence, Statement for the Record, Worldwide Threat Assessment of the US Intelligence Community, Senate Armed Services Comm., 2 (Feb. 26, 2015), https://www.dni.gov/files/documents/Unclassified_2015_ATA_SFR_-_SASC_FINAL.pdf; Leon Panetta, Secretary of Defense, US Department of Defense, Remarks on Cybersecurity to the Business Executives for National Security (Oct. 11, 2012), http://archive.defense.gov/transcripts/transcript.aspx?transcriptid=5136); Roy Schöndorf, *Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations*, 97 INT'L L. STUD. 395, 404 (2021).
[18] See, e.g., John P. Carlin, *Detect, Disrupt, Deter: A Whole-of-Government Approach to National Security Cyber Threats*, 7 HARV. NAT'L SEC. J. 391, 397 (2016).
[19] See *ibid*. See also Tsagourias, *supra* note 14, 234.
[20] See Tsagourias, *supra* note 14, 233. See also Eichensehr, *supra* note 12, 529.
[21] See, e.g., Marise Payne, Minister for Foreign Affairs, *Statement Attributing the Harmful Cyber Campaign against SolarWinds to Russia* (Apr. 16, 2021), https://www.internationalcybertech.gov.au/node/138; U.K. National Cyber

desist or even domestic criminal indictments of foreign actors.[22] Regardless of the form, when a victim state blames another state for a hostile cyber operation, it gambles that its attribution may be met with incredulity by other states and by the state being accused.

Legal attribution 'denotes a situation in which an individual or group's conduct is regarded as that of a state'.[23] The International Law Commission's Draft Articles on the Responsibility of States for Internationally Wrongful Acts (ARSIWA) are considered by most states to be a generally, albeit not entirely, accurate restatement of the customary law of state responsibility.[24] Under ARSIWA, a hostile cyber operation can most clearly be attributed to the offending state when it is perpetrated by an organ of that state.[25] When the malign actor is a non-state individual or group, the hostile cyber operation can be legally attributed to a state if, amongst other things, the person or entity executing the cyber operation 'is empowered by the law of that state to exercise elements of the government authority;'[26] if the non-state person or group 'is in fact acting on the instructions of or under the direction or control of, that state' in carrying out the cyber operation;[27] or if the state 'acknowledges and adopts the [cyber operation] in question as its own'.[28]

Whereas previously victim states would publicly attribute hostile cyber operations infrequently,[29] it is increasingly common for victim states to publicly attribute hostile cyber operations[30] and for other states to join in those attributions.[31] The growing inclination to publicly attribute benefits international order in two principal ways. First, public attribution, even absent public disclosure of the underlying evidence, signals to other states, international law commentators and the public that the victim state believes its retaliatory actions are legally justified.[32] States choosing to privately attribute risk having their responsive action mischaracterised as politically provocative or even unlawful.[33] Thus, transparency enhances the perceived legitimacy of the attribution and

Security Centre, Reckless campaign of cyber attacks by Russian military intelligence service exposed (Oct. 3, 2018), https://www.ncsc.gov.uk/news/reckless-campaign-cyber-attacks-russian-military-intelligence-service-exposed.

[22] See, e.g., US Department of Justice, Press Release, *Two Chinese Hackers Working with the Ministry of State Security Charged with Global Computer Intrusion Campaign Targeting Intellectual Property and Confidential Business Information, Including COVID-19 Research* (Jul. 21, 2020), https://www.justice.gov/opa/pr/two-chinese-hackers-working-ministry-state-security-charged-global-computer-intrusion.

[23] Draft Articles on Responsibility of States for Internationally Wrongful Acts, cmt. to art. 2, 12, Rep. of the Int'l L. Comm'n, 53d Sess., U.N. Doc. A/56/10, GAOR 56th Sess., Supp. No. 10, (2001), *reprinted in* [2001] *Yearbook of the International Law Commission* 36, U.N. Doc. A/CN.4/SER.A/2001/Add.1 (Part 2) [hereinafter Articles on State Responsibility]. *See also* Michael N. Schmitt, *Foreign Cyber Interference in Elections*, 97 INT'L L. STUD. 739, 742 (2021); Eichensehr, *supra* note 12, 529.

[24] Although numerous states acknowledge that the ARSIWA have been influential and are widely referred to and cited by international lawyers, Governments and courts (both national and international), states remain divided regarding whether a convention is appropriate. The main concern among states seems to be reopening discussion of the substance of the draft rules and thereby preempting the organic development of customary international law around those provisions of the ARSIWA that are not believed to reflect current customary international law. See, e.g., Sixth Committee, Summary Record of the 9th Meeting, 27-75, U.N. Doc. A/C.6/71/SR.9 (Nov. 7, 2016); Julian Simcock, Deputy Legal Adviser, US Mission to the UN, Remarks at a UN General Assembly Meeting of the Sixth Committee on Agenda Item 75: Responsibility of States for Internationally Wrongful Acts (Oct. 14, 2019).

[25] Articles on State Responsibility, *supra*, note 23, art. 4.

[26] *Ibid.*, art. 5.

[27] *Ibid.*, art. 8.

[28] *Ibid.*, art. 11.

[29] See Andrzej Kozlowski, *Comparative Analysis of Cyberattacks on Estonia, Georgia and Kyrgyzstan*, 3 EUROPEAN SCIENTIFIC JOURNAL 237, 242–243 (2014); John Markoff, *Before the Gun-fire, Cyberattacks,* N.Y. TIMES (Aug. 12, 2008),

[30] See Yuval Shany & Michael N. Schmitt, *An International Attribution Mechanism for Hostile Cyber Operations*, 96 INT'L L. STUD. 196, 211 (2020); Eichensehr, *supra* note 12, 529–30.

[31] Shany & Schmitt, *supra* note 30.

[32] See Eichensehr, *supra* note 12, 556. *Cf*. William Banks, *Cyber Attribution and State Responsibility*, 97 INT'L L. STUD. 1039, 1059 (2021) (noting 'a persuasive case may be made that international law requires that States attribute internationally wrongful acts in cyberspace if they expect to respond in ways that would otherwise violate international law, e.g., by using force or engaging in countermeasures'.).

[33] See Eichensehr, *supra* note 12, 556.

of any victim state response. Second, public attribution is a deterrent distinct from the consequences flowing from the victim state's response.[34] Notwithstanding their outward messaging, states generally dislike being perceived as rulebreakers by other states. Cyber attributions satisfying explicit, broadly-accepted standards of proof multiply the effective opportunities for naming and shaming responsible states, minimise their ability to effectively deny responsibility and deter offending states without having to rely upon subsequent cyber or kinetic retribution as the cudgel checking state misbehaviour in cyberspace.[35]

Unfortunately, states publicly attributing hostile cyber operations seldom divulge the underlying evidence on which the decision-makers relied.[36] State cyber attributions based on publicly undisclosed information run counter to the widely accepted notion that, where possible, states should reveal the underlying factual basis for their attribution decisions.[37] The GGE's use of the permissive auxiliary verb 'should' in its 2015 and 2021 Reports suggests state substantiation of cyber attributions is a voluntary and non-binding norm rather than an international legal obligation.[38] The GGE's recognition of a mere expectation that victim states substantiate their claims of state responsibility, the OEWG's silence on issues of proof and the International Law Commission's decision to avoid addressing matters of evidence in ARSIWA[39] suggest that the absence of cyber-specific legal norms establishing evidentiary obligations and thresholds of proof will likely persist, at least for now. Whether a customary law rule may eventually emerge remains to be seen.

The reticence of victim states and their supporters to reveal the evidence underpinning their attribution determinations almost certainly stems from fear that doing so will reveal the extent of their cyber and intelligence capabilities.[40] Some states have developed forensic capabilities that permit technical attribution which, when coupled with robust signals intelligence (SIGINT) and human intelligence (HUMINT) capabilities, permits them to attribute a hostile cyber operation with heightened confidence.[41] Although states are concerned that disclosing such evidence may provide adversaries with insight into their capabilities, states should substantiate their attribution decisions for both political and legal reasons.

Politically, the international atmosphere has come a long way since French President Charles De Gaulle took President John F. Kennedy at his word that the Soviet Union was positioning missiles in Cuba.[42] In the contemporary era, victim state credibility and the perceived legitimacy of state response actions require some factual showing undergirding cyber attribution. Where comity, rather than a legal commitment, binds the victim state and friendly states, the victim state must convince those friendly states both that its response is justified and that the friendly state should

[34] See Eichensehr, *supra* note 12, 552.
[35] See Eric F. Mejia, *Act and Actor Attribution in Cyberspace: A Proposed Analytic Framework*, 8 STRATEGIC STUD. Q. 114, 129 (Spring 2014); Clark & Landau, *supra* note 13, 324.
[36] Shany & Schmitt, *supra* note 30, 213.
[37] 2015 GGE Report, *supra* note 6, 28(f); 2021 GGE Report, *supra* note 6, 71(g). See also Shany & Schmitt, *supra* note 30, 213.
[38] See also TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE cmt. to Ch. 4, 13 at 83 (Michael N. Schmitt gen. ed., 2017) [hereinafter TALLINN MANUAL 2.0].
[39] Articles on State Responsibility, *supra* note 23, cmt. to Ch. V, 8. 'Just as the articles do not deal with questions of the jurisdiction of courts or tribunals, so they do not deal with issues of evidence or the burden of proof. In a bilateral dispute over State responsibility, the onus of establishing responsibility lies in principle on the claimant State'.
[40] Shany & Schmitt, *supra* note 30, 214.
[41] See *ibid*., 217.
[42] See JEAN LACOUTURE, LE SOUVERAIN 364-365 (Editions de Seuil, Paris, 1989).

at least expend political capital, if not commit military or other government resources, in collective response.[43] The confidence gap between the victim state and unafflicted friendly states counsels for a widely accepted standard of proof for cyber attribution underlying victim state responses along the spectrum from retorsion to forcible self-defence.[44]

The standard and the burden of proof are distinct aspects of the evidentiary requirement applicable to legal and political adjudication of issues.[45] The burden of proof identifies the party responsible for providing evidence on an issue in dispute. The standard of proof refers to how much substantive evidence is necessary to substantiate a party's claim.[46] The party making and relying on an attribution – the victim state responding to a hostile cyber operation – must establish the factual basis for it.[47] Unfortunately, 'there is at present no universal and coherent body of law that can be described as the international law of evidence'.[48] The judging entity alone, whether the International Court of Justice (ICJ) or other states, establishes its threshold of acceptable uncertainty and the standard of proof it will demand of states attributing hostile cyber operations.[49] International stability and predictability demand that the quantum of evidence necessary to substantiate cyber attributions underlying retorsions, countermeasures and self-defence responses be agreed between and therefore transparent to, all states.

Hostile Cyber Operations, International Law and Standards of Proof

State-on-state hostile cyber operations fall along a spectrum of graduated severity. The least severe are lawful acts. Access operations such as those enabling follow-on activities like espionage, misinformation and attack without damaging or destroying the targeted system, depriving users of access or interfering with normal system functioning typically fall in this category.[50] Disruption operations such as denial of service operations also generally fall within the category of lawful acts so long as they merely interrupt the information flow and the ability of the targeted system to function properly, but do not cause physical damage or injury.[51]

For various pragmatic policy reasons, a victim state may choose not to respond when it experiences a lawful (or at least not unlawful) but hostile cyber operation. For example, it may not

[43] See Delbert Tran, *The Law of Attribution: Rules for Attributing the Source of a Cyber-Attack*, 20 YALE J. L. & TECH. 376, 400 (2018).
[44] See *ibid*., 400–01. See also, e.g., Brian J. Egan, *International Law and Stability in Cyberspace*, 35 BERKLEY J. OF INT'L L. 169, 177 (2017); Ministry of Foreign Affairs of the Netherlands, 'Letter to the parliament on the international legal order in cyberspace, Appendix: International law in cyberspace' 6 (Jul. 5, 2019), https://www.government.nl/binaries/government/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace/International+Law+in+the+Cyberdomain+-+Netherlands.pdf; Schöndorf, *supra* note 17, 405.
[45] James A. Green, *Fluctuating Evidentiary Standards for Self-Defence in the International Court of Justice*, 58 Int'l & COMP. L.Q. 163, 165 (2009).
[46] See *ibid*.; Tomohiro Mikanagi & Kubo Mačák, *Attribution of cyber operations: an international law perspective on the Park Jin Hyok case*, 9 CAMBRIDGE INT'L L.J. 51, 65 (2020).
[47] See Green, *supra* note 45, 165. See also Ministry of Foreign Affairs of the Netherlands, *supra* note 44, 6.
[48] Mikanagi & Mačák, *supra* note 46, 55.
[49] See *ibid*.
[50] Gary D. Brown & Owen Tullos, *On the Spectrum of Cyberspace Operations*, SMALL WARS JOURNAL (Dec. 11, 2012), https://smallwarsjournal.com/jrnl/art/on-the-spectrum-of-cyberspace-operations.
[51] *Ibid*.

wish to acknowledge that it has been victimised or it may desire to preserve current or future economic or diplomatic relations with the offending state. Inaction as a victim state response does not require that evidence be produced and it is not subject to any standard of proof. This is because fellow states have no victim state conduct to adjudicate as politically or legally wrongful.

Rather than sit idly, a victim state may elect to protest the hostile cyber operation by, for example, issuing a demarche demanding that the offending state cease the objectionable behaviour. Protest, like inaction, is inherently lawful, is subject to no evidentiary standard and does not require the victim state to produce evidence. However, protests do require the victim state to officially acknowledge victimisation. If that acknowledgement takes the form of a public attribution statement, it risks the offending state publicly condemning the victim state for its 'baseless' accusation and demanding that it substantiate its allegation publicly. If the victim state is unwilling or unable to produce sufficient, compelling evidence to counter the offending state's sustained denials, it may suffer scepticism and reputational damage *vis-à-vis* its fellow states.

A victim state may also take acts of retorsion against the state it believes is responsible for a lawful hostile cyber operation. Retorsions are unilateral actions lawful under international law but perceived as unfriendly by and toward the target state.[52] Examples include severing or diminishing diplomatic relations, imposing economic sanctions, cyber espionage and blocking access to cyber infrastructure. Retorsion is an attractive and common victim state response because the triggering hostile cyber operation need not breach international law[53] and the retorsions may be retributive rather than motivated by a desire to deter the offending state.

It is wholly within the victim state's sovereign discretion, consistent with its foreign policy desires, to engage in acts of retorsion. Retorsion requires no legal justification because it involves no breach of an international legal obligation.[54] However, if the victim state's unfriendly actions appear sudden and unprovoked, other states may perceive them as arbitrary and not rationally based. If the victim state is unable or unwilling to produce satisfactory evidence to reassure fellow states, it may be misperceived as a rash, unprincipled actor. To enhance the political legitimacy of its retorsion and to minimise reputational damage, a victim state should be prepared to produce 'some' or a 'scintilla' of credible evidence to support its cyber attribution.

Next along the severity spectrum are cyber operations below the use of force threshold but amounting to internationally wrongful acts (IWA). An IWA is an act or omission that is 'attributable to the state under international law' and which 'constitutes a breach of an international obligation of the state'.[55] Hostile cyber operations below the use of force threshold are most likely to either violate the obligation to respect state sovereignty or to constitute a prohibited intervention.[56]

[52] See JAMES CRAWFORD, STATE RESPONSIBILITY: THE GENERAL PART 676 (2013); Articles on State Responsibility, *supra* note 23, cmt to Part III, Ch. II, 3 (describing retorsion as ''unfriendly' conduct which is not inconsistent with any international obligation of the State engaging in it even though it may be a response to an internationally wrongful act').
[53] See Michael N. Schmitt & Durward E. Johnson, *Responding to Hostile Cyber Operations: The 'In-Kind' Option*, 97 INT'L L. STUD. 96, 118 (2021) (stating that if an initial hostile cyber operation is lawful, an in-kind response by the victim State would likely be considered a retorsion).
[54] *Ibid*., 120. 'Acts of retorsion are permissible for any reason because they are, by definition, lawful'.
[55] Articles on State Responsibility, *supra* note 23, art. 2.
[56] See Durward E. Johnson & Michael N. Schmitt, *Responding to Proxy Cyber Operations under International Law*, 6(4) CYBER DEFENSE REVIEW 15 (Fall 2021).

Sovereignty applies in cyberspace.[57] States willing to express a firm view almost unanimously accept that sovereignty is a primary rule of international law.[58] The only state on record expressly adopting the contrary view is the United Kingdom.[59] A third and better view is that sovereignty is both a principle underpinning other primary rules and itself a rule that can be violated.[60]

State A's territorial sovereignty is violated if State B's cyber operation causes physical damage or destruction,[61] including significant or permanent loss of functionality[62] or significant injury or death within State A.[63] State A's functional sovereignty is violated if State B's cyber operation materially interferes with or usurps State A's performance of its inherently governmental functions – those that only a state can perform, such as conducting elections, collecting taxes and performing law enforcement – even if that cyber operation causes no concrete effects.[64] Finally, if State B interferes with the right of State A to choose its political, social, economic and cultural system, State B violates State A's sovereignty.[65]

The equality of states and their freedom to independently govern themselves means the principle of sovereignty underlies the prohibition of intervention.[66] The applicability of the prohibition of intervention to cyber operations is not controversial. In its 2013, 2015 and 2021 reports, the GGE recognised, either expressly or by implication, that the customary international law (CIL) prohibition of intervention applies to hostile cyber operations. The UN General Assembly endorsed this view in Resolution 70/237.

In the *Nicaragua* case, the ICJ set out the two elements of prohibited intervention under CIL.[67] To be a prohibited intervention, a hostile cyber operation must both affect a matter reserved to the free choice of another state (*domaine réservé*)[68] and be coercive in nature. Affairs falling within a

[57] See 2013 GGE Report, *supra* note 6, 20; 2015 GGE Report, *supra* note 6, 27; 2021 GGE Report, *supra* note 6, 71(b); North Atlantic Treaty Organisation, 'Wales Summit Declaration' (issued by the Head of State and Government participating in the meeting of the North Atlantic Council in Wales) 72 (Sep. 5, 2015).
[58] See, e.g., Austria, Pre-Draft Report of the OEWG - ICT: Comments by Austria (Mar. 31, 2020); Czech Republic, Statement by Mr. Richard Kadlčák, Special Envoy for Cyberspace, 2nd substantive session of the Open-ended Working Group on developments in the field of information and telecommunications in the context of international security (Feb. 11, 2020); French Ministry of the Armies, 'International Law Applied to Operations in Cyberspace', § 1.1.1 (Sep. 9, 2019); Finland, Ministry of Foreign Affairs, International Law and Cyberspace: Finland's National Positions 3 (Oct. 15, 2020); Iran, 'Declaration of General Staff of the Armed Forces of the Islamic Republic of Iran Regarding International Law Applicable to the Cyberspace' 4 (Jul. 2020); Ministry of Foreign Affairs of the Netherlands, *supra* note 44, 2; North Atlantic Treaty Organization, *supra* note 10, 20 n.26.
[59] See Jeremy Wright, 'Cyber and International Law in the 21st Century' (May 23, 2018). The US Department of Defense has endorsed, but not necessarily adopted, a similar view. See Paul C. Ney, Jr., General Counsel, US Department of Defense, Remarks at US Cyber Command Legal Conference (Mar. 2, 2020). See also Gary P. Corn and Robert Taylor, *Sovereignty in the Age of Cyber*, 111 AMERICAN JOURNAL OF INTERNATIONAL LAW UNBOUND 207, 208 (2017).
[60] See TALLINN MANUAL 2.0, supra note 38, r. 1, at 11.
[61] See, e.g., Germany, 'On the Application of International Law in Cyberspace: Position Paper' 4 (Mar. 2021); Ministry of Foreign Affairs of the Netherlands, *supra* note 44, 3. *Contra* French Ministry of the Armies, *supra* note 58, § 1.1.1. 'Any cyberattack against French digital systems or any effects produced on French territory by digital means by a State organ, a person or an entity exercising elements of governmental authority or by a person or persons acting on the instructions of or under the direction or control of a State constitutes a breach of sovereignty'.
[62] See TALLINN MANUAL 2.0, *supra* note 38, cmt. to r. 4, 13 at 20–21.
[63] See *ibid*., cmt. to r. 4, 11 at 20.
[64] TALLINN MANUAL 2.0, *supra* note 38, cmt. to r. 4, 16, 18, & 19 at 22–23. See also, e.g., Ministry of Foreign Affairs of the Netherlands, *supra* note 44, 3.
[65] See TALLINN MANUAL 2.0, *supra* note 38, cmt. to r. 2, 10 at 15.
[66] TALLINN MANUAL 2.0, *supra* note 38, cmt. to r. 2, 10 at 15. See also *Military and Paramilitary Activities in and against Nicaragua* (*Nicar. v. US*), Judgment, 1986 I.C.J. Rep. 14, 205 (June 27) [hereinafter *Military and Paramilitary Activities*].
[67] *Military and Paramilitary Activities*, *supra* note 66. See also Schmitt, *supra* note 23, 745.
[68] See, e.g., Katja Ziegler, *Domaine Réservé*, MAX PLANCK ENCYCLOPEDIA OF PUBLIC INTERNATIONAL LAW (updated Apr. 2013) https://opil-ouplaw-com.usnwc.idm.oclc.org/view/10.1093/law:epil/9780199231690/law-9780199231690-e1398?rskey=B9zCAn&result=1&prd=MPIL.

state's *domaine réservé* include the choice of a political system,[69] conducting national elections,[70] developing and expressing foreign policy,[71] and recognition of states.[72] States value these important sovereign prerogatives and will find cyber intrusions on these aspects of their sovereignty objectionable, particularly when undertaken in a manner to coerce rather than to influence.

In addition to inaction, protest or acts of retorsion, states suffering internationally wrongful cyber operations below the use of force threshold may respond with countermeasures. In contrast to lawful responses not requiring evidence and subject to no evidentiary standard, countermeasures are non-forcible[73] otherwise internationally wrongful acts undertaken by one state against another to induce the offending state to cease its own internationally wrongful conduct or make reparations.[74] The inherent wrongfulness of a purported countermeasure is precluded only if it is taken against the state actually responsible for the internationally wrongful cyber operation.[75] A victim state exacting a would-be countermeasure based on a misattributed unlawful cyber operation itself commits an IWA for which it is required to make reparations or for which it may suffer a countermeasure.[76]

The political and legal risk attending countermeasures predicated on cyber misattribution supports clearly establishing a 'preponderance of the evidence' standard as the appropriate quantum necessary to attribute. Under this standard, international law would validate the victim state's countermeasure if it can support its cyber attribution with sufficient evidence to establish that its identification of the perpetrator is more probably correct than incorrect.[77] Adoption of such a standard would mark an evolution of current CIL's inverted tolerance for misattribution.

Currently, international law demands that states taking countermeasures correctly attribute the IWA.[78] There is no room for claims of mistake because whether a particular countermeasure fulfils the predicate conditions to be valid is an objective inquiry. There is no subjective element of retaliating state knowledge or intent. In essence, international law imposes what is tantamount to strict liability or, interpreted most leniently, a standard of 'beyond a reasonable doubt'. Under this standard, the victim state's attribution must be supported by sufficient evidence to render its validity virtually beyond dispute.[79] In contrast, international law demands a state acting in self-defence merely be reasonable in its attribution determination, not also correct.[80] It is illogical that international law is unwilling to accept error when the consequence is a non-forcible breach of an international legal obligation, but it is willing to embrace error when the probable consequence is death and destruction.

---

[69] *Military and Paramilitary Activities*, *supra* note 66, 263.
[70] Ministry of Foreign Affairs of the Netherlands, *supra* note 44, 3.
[71] *Military and Paramilitary Activities*, *supra* note 66, 205.
[72] Ministry of Foreign Affairs of the Netherlands, *supra* note 44, 3.
[73] Articles on State Responsibility, *supra* note 23, art. 50.
[74] See CRAWFORD, *supra* note 52, 685; Articles on State Responsibility, *supra* note 23, cmt to Part III, Ch. II, 1.
[75] Articles on State Responsibility, *supra* note 23, art. 49. See Michael N. Schmitt, *Peacetime Cyber Responses and Wartime Cyber Operations under International Law: An Analytical Vade Mecum*, 8 HARV. NAT'L SEC. J. 239, 254 n.66 (2017).
[76] Articles on State Responsibility, *supra* note 23, cmt. to art. 49, 3. See also Schmitt, *supra* note 75, 254; TALLINN MANUAL 2.0, *supra* note 38, cmt. to r. 20, 16 at 116.
[77] See Mejia, *supra* note 35, 123. See also Roscini, *supra* note 11, 248 (describing the preponderance of evidence standard as demanding proof sufficient to establish a fact as 'more likely than not or reasonably probable').
[78] See Schmitt, *supra* note 75.
[79] See Green, *supra* note 45, 167.
[80] See Schmitt, *supra* note 75.

Commensurate with the less grave consequences attending misattribution in the countermeasures context, a preponderance of the evidence standard of proof there would realign the risk calculus. Given the increasing role cyber operations play in strategic competition and the levelling effect cyber has on relations between powerful and less powerful states, states with robust cyber capabilities will probably begin to press for greater clarity regarding evidentiary burdens and standards. States will almost certainly expect that the rules also enable effective deterrence. Applying a preponderance of the evidence standard to cyber attributions undergirding countermeasures effectively balances states' interest in minimising the risk that innocent states will bear the brunt of misattribution with their growing desire to deter hostile cyber operations, especially those that are internationally wrongful. States should embrace this proposed preponderance of the evidence model because by lowering international law's expectation for retaliating states, countermeasures become more available as a deterrent. At the same time, a relatively high threshold to validly taking countermeasures remains in place, thereby reducing the probability that the victim state will act against an innocent state.

Third in severity along the cyber operation spectrum are those violating the CIL prohibition on the inter-state use of force codified in Article 2(4) of the UN Charter. This proscription applies to hostile cyber operations attributable to a state.[81] A hostile cyber operation causing more than *de minimis* physical damage (including substantial functionality loss in the targeted system), destruction, death or injury amounts to the use of force. Below that threshold, there is no consensus among states regarding what operations constitute a prohibited use of force.[82] States approach the question on a case-by-case basis that treats hostile cyber operations comparable to kinetic uses of force in their scale and effects as wrongful.[83] Because victim states may not respond in kind or in any other forcible manner unless the UN Security Council authorises such a response under Chapter VII,[84] victim state responses are confined to inaction, protests, retorsions or countermeasures.[85] Of these options, only cyber misattribution preceding a countermeasure carries international legal risk. However, the risk to reputational and political capital attending misattribution in each of these contexts supports the development of clear, broadly-accepted standards of proof.

The final and most severe category of hostile cyber operations is armed attack. The ICJ characterised armed attacks as 'the most grave forms of the use of force'.[86] Thus, according to the predominant view, not all uses of force rise to the level of an armed attack, but all armed

[81] See 2013 GGE Report, *supra* note 6,19; 2015 GGE Report, *supra* note 6, 26; 2021 GGE Report, *supra* note 6, 71(d).
[82] France and the Netherlands have offered the most forward-leaning positions on the issue. France takes the position that a cyber-campaign causing severe nationwide economic disruption could qualify as a use of force and maybe rise to an armed attack. French Ministry of the Armies, *supra* note 58, § 1.2.1. The Netherlands may be willing to reach the same conclusion. Ministry of Foreign Affairs of the Netherlands, *supra* note 44, 4.
[83] TALLINN MANUAL 2.0, *supra* note 38, r. 69, at 330; Ney, *supra* note 59. See also, e.g., Harold Hongju Koh, Legal Adviser, US Department of State, *International Law in Cyberspace: Remarks as Prepared for Delivery to the US CYBERCOM Inter-Agency Legal Conference* (Sept. 18, 2012), reprinted in 54 HARV. INT'L L.J. ONLINE 1, 4 (2012); TALLINN MANUAL 2.0, *supra* note 38, cmt. To r. 69, 8, at 333; Schmitt & Johnson, *supra* note 53, 109.
[84] Schmitt & Johnson, *supra* note 53, 108.
[85] The use of force is not a permissible countermeasure. See, e.g., Ney, *supra* note 59; Wright, *supra* note 59; Government of Australia, 'Australia's International Cyber Engagement Strategy, Annex A: Supplement to Australia's Position on the Application of International Law to State Conduct in Cyberspace' (2019); French Ministry of the Armies, *supra* note 58, § 1.1.3; Ministry of Foreign Affairs of the Netherlands, *supra* note 44, 7; Finland, Ministry of Foreign Affairs, *supra* note 58, 5; Articles on State Responsibility, *supra* note 23, art. 50. But see *Oil Platforms* (*Iran v. US*), Judgment, 2003 I.C.J. Rep. 161, 324, 12–13 (Nov. 6) (separate opinion by Simma, J.) (suggesting that forcible countermeasures in response to a hostile use of force not qualifying as an armed attack might be lawful).
[86] *Military and Paramilitary Activities*, *supra* note 66, 191.

attacks are uses of force.[87] The ICJ identified the 'scale and effects' of the activity at issue as the measure by which to distinguish an armed attack from a less grave use of force.[88] The CIL right of a state suffering an armed attack to respond in self-defence is codified in Article 51 of the UN Charter.[89] Under the prevailing view, the inherent right of states to act in self-defence applies to cyber armed attacks.[90]

Self-defence is the only legally valid justification for the unilateral employment of military force in international law.[91] A clear, broadly-accepted standard of proof for cyber attribution underlying self-defence claims is necessary because states decide for themselves when it is proper to invoke their right of self-defence and 'a state exercising its inherent right of self-defence as referred to in Article 51 of the Charter is not, even potentially, in breach of Article 2, paragraph 4'.[92]

Under current international law, a victim state responding in self-defence need only reasonably determine, based on the information available to it at the time, that (a) it is suffering or is about to suffer an armed attack; and (b) the state against which it is about to use force in self-defence is the attacking state.[93] A victim state, therefore, can misattribute an actual or imminent cyber armed attack and employ military force against an innocent state with legal impunity so long as its response satisfies the vague standard of 'reasonableness'.[94]

The identity of the victim state, the existence of a cyber armed attack and the identity of the state perpetrator should all be objectively assessed, both factually and legally.[95] However, the victim state's cyber attribution relies in significant part on its own subjective assessments. In attributing a cyber armed attack, the victim state is likely to rely as much on the reporting from its own and friendly intelligence services and on the political relationship it has with the suspected bad actor as it relies on technical forensic data.[96] The attribution of a cyber armed attack to a particular state should be required to pass an established, explicit and consistent threshold before the victim state's response in self-defence is deemed justified.[97] Such a well-defined standard of proof would bring necessary clarity to the current 'reasonableness' benchmark.

Holding a victim state to a stringent 'beyond a reasonable doubt' (or similar) standard is unreasonable considering the speed with which a cyber armed attack can be executed and its potentially devastating consequences can manifest in the victim state. Although states sometimes make dubious assertions that they are acting in self-defence,[98] requiring a victim state to prove the predicate conditions for the exercise of self-defence before it acts will be impractical and states likely will not support the development of such a rule. Alternatively, a preponderance of the

[87] See *ibid*.; *Oil Platforms* (Iran v. US), Judgment, 2003 I.C.J. Rep. 161, 51 (Nov. 6); TALLINN MANUAL 2.0, *supra* note 38, cmt. to r. 71, 6, at 341. See also, e.g., YORAM DINSTEIN, WAR, AGGRESSION AND SELF-DEFENCE, 550–54 (5th ed. 2011).
[88] *Military and Paramilitary Activities*, *supra* note 66, 195.
[89] UN Charter art. 51. *See Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion, 1996 I.C.J Rep. 226, 96 (July 8).
[90] 2013 GGE Report, *supra* note 6, 19; 2015 GGE Report, *supra* note 6, 28(c); 2021 GGE Report *supra* note 6, 71(e); Schmitt & Johnson, *supra* note 53, 103–04.
[91] Green, *supra* note 45, 169.
[92] Articles on State Responsibility, *supra* note 23, cmt. to art. 21, 1.
[93] TALLINN MANUAL 2.0, *supra* note 38, cmt. to r. 71, 23, at 347.
[94] See *ibid*.
[95] Green, *supra* note 45, 170.
[96] See Banks, *supra* note 13, 1503; Tsagourias, *supra* note 14, 234.
[97] See Roscini, *supra* note 11, 239.
[98] See Green, *supra* note 45, 169.

evidence (or lower) standard does little to mitigate the risk of misattribution or to deter specious assertions of self-defence.[99] To deter spurious self-defence claims while still preserving states' freedom of action, international law should evolve through state interpretation of 'reasonableness' to require the victim state to produce, during examination following the incident, clear and convincing evidence that its exercise of self-defence was valid.[100]

The clear and convincing evidence standard requires a level of persuasion short of virtual certainty while adding precision and rigour to the view that '[r]easonable states neither respond precipitously on the basis of sketchy indications of who has attacked them nor sit back passively until they have gathered unassailable evidence'.[101] Under a clear and convincing standard, a victim state acting in self-defence must demonstrate that its cyber attribution is supported by sufficient evidence to 'convince the arbiter in question that it is substantially more likely than not that the [attribution is] true'.[102] This is not wholly new territory; past state practice suggests the clear and convincing evidence standard is a suitable interpretation of 'reasonable' where states act forcibly in self-defence.[103] Broad state practice further interpreting 'reasonable' to require clear and convincing evidence for cyber attributions underlying self-defence responses would set an acceptably high and generally attainable legal threshold justifying a victim state's use of force – including potentially deadly kinetic strikes – even against an innocent state it erroneously believed was the perpetrator of the precipitating cyber armed attack.

Conclusion

Attribution is a necessary condition precedent to the lawful taking of countermeasures and to the lawful exercise of the right of self-defence. Although not legally required, it is politically necessary for acts of retorsion to be perceived as credible and justified. Unfortunately, international law imposes no explicit standard of proof on states justifying the attributions underlying their responses to hostile cyber operations. Sovereign discretion aside, it is impractical and disordered to permit states to calculate their responses to hostile cyber operations with discretion unfettered by an explicit international standard by which to assess propriety and against which to measure accountability.

In the interest of international stability and predictability, states must begin the process of evolving international law by demanding that victim states tender credible evidence for their attributions of hostile cyber operations to which they respond. The standard of proof should not be uniform for all victim state responses. The respective standards of proof applicable during the post-event

[99] Roscini, *supra* note 11, 252.
[100] See, e.g., *Oil Platforms*, *supra* note 87, 51–61; Green, *supra* note 45, 169; Michael N. Schmitt, *Cyber Operations and the Jus Ad Bellum Revisited*, 56 VILL. L. REV. 569, 596 (2011).
[101] Schmitt, *supra* note 100, 595.
[102] Green, *supra* note 45, 167; Tran, *supra* note 43, 411.
[103] See, e.g., Letter from John D. Negroponte, Permanent Representative of the United States of America to the United Nations, to the President of the Security Council, U.N. Doc. No. S/2001/946 (Oct. 7, 2001), http://repository.un.org/bitstream/handle/11176/31401/S_2001_946-EN.pdf. 'Clear and compelling' is also the phrasing used by NATO Secretary General Lord Robertson when confirming that the September 11, 2001, attacks on the United States triggered Article V of the North Atlantic Treaty. Statement by NATO Secretary General, Lord Robertson (Oct. 2, 2001), https://www.nato.int/docu/speech/2001/s011002a.htm.

critique of the victim state's acts of retorsion, taking of countermeasures and responses in self-defence should be clear, consistently applied and a function of the nature and consequence of the responsive acts. Just as in the context of primary international legal obligations, 'forceful acts of violence that risk death and destruction are categorised differently than are acts causing mere inconvenience or economic loss',[104] the standard of proof against which a victim state's attribution determination should be judged should vary depending on the severity of the response.

A clear and convincing standard of proof should be applied to attributions of hostile cyber operations resulting in forcible responses hazarding death, injury, destruction or significant damage. Attribution of internationally wrongful cyber operations giving rise to countermeasures should be subject to a preponderance of the evidence standard. Acts of retorsion taken in response to lawful hostile cyber operations should be subject to a requirement that some evidence be produced to establish that the retorsions were considered and not impulsive and that they were justified, rather than arbitrary.

These standards of proof will function as a procedural device balancing three essential probabilities: (1) the likelihood that the victim state will hold the proper state to account for conducting the hostile cyber operation; (2) the likelihood that the wrong state will be erroneously made to suffer consequences for a hostile cyber operation it did not conduct; and (3) the likelihood that other states will accept the attribution as valid and publicly support it. A lack of international confidence in the victim state's attribution increases the likelihood that the victim state will at least be criticised and pay a diplomatic or political cost for its response actions, if not be viewed as having itself committed an IWA.

A state's confidence in the accuracy of its attribution of a hostile cyber operation should drive its willingness to impose increasingly severe consequences on the state deemed responsible. Development of these standards of proof for cyber attribution will function to establish a communal understanding of acceptable state conduct and serve as a uniform frame of analysis by which to examine the factual reporting of the victim state and against which to weigh the available evidence. Adoption and application of these standards of proof will increase victim states' confidence in their attribution determinations, enhance the perceived legitimacy of those attributions and make other states, non-governmental organisations and intergovernmental organisations more willing to accept the victim states' attributions as valid. In time, shared interpretations of international law standards of proof may lead to the crystallisation of customary norms of evidence governing state behaviour in response to hostile cyber operations.

[104] Brown & Tullos, *supra* note 50.