Journal of Conflict & Security Law © Oxford University Press 2016; all rights reserved.
For permissions, please e-mail: journals.permissions@oup.com
doi:10.1093/jcsl/krw015
Advance Access published on 19 October 2016

'Proxies' and Cyberspace

Tim Maurer*

Abstract

States use proxies to project power through cyberspace, some capable of causing significant harm. In recent years, media outlets have published reports about proxies using Information and Communications Technologies (ICTs) from Northeast Asia to India, Pakistan, the Middle East, and Eastern Europe. Two of the landmark documents providing insight into how the international community thinks about rules of the road for cyberspace explicitly reference the term 'proxies'. However, neither report defines 'proxy', nor does the term easily translate into non-English languages. This article therefore reviews what this term means and how it has been used in various contexts. It focuses on the subset of proxies that are non-state actors used by a state actor, analysing the different logical distinctions and levels of detachment between a state and a non-state actor's activity. The goal is 2-fold: first, to provide a framework to think about the diverse array of existing proxy definitions; second, to conceptualise the relationships between a state and non-state proxies that can offer a guide for political decision-makers and a roadmap for future research on proxy actors and cyberspace.

States use proxies, some with greater capabilities than most states, to project power through cyberspace. 'Cyberspace significantly increases an actor's ability to engage in attacks with "plausible deniability", by acting through proxies', then Legal Advisor of the US Department of State, Harold Koh, pointed out in a speech at US Cyber Command in September 2012.[1] Media outlets

* Tim Maurer co-leads the Cyber Policy Initiative at the Carnegie Endowment for International Peace and is a visiting scholar at the University of Michigan's Gerald R Ford School of Public Policy. E-mail: tim.maurer@post.harvard.edu. He is particularly thankful for the comments and feedback provided by Duncan Hollis, Joseph Nye, Martha Finnemore, Matthew Noyes, Taylor Brooks as well as Jonathan Diamond, Manar Hassan, Tatiana Tropina and Wenyan Deng.

1 H H Koh, 'International Law in Cyberspace' (United States Cyber Command Inter-Agency Legal Conference, Fort Meade, MD, 18 September 2012) <www.state.gov/s/l/releases/remarks/197924.htm> accessed 31 January 2016. On the international legal responsibility of non-state actors that commit malicious cyber operations from the territory of failed states or ungoverned spaces, see in this volume Nicholas Tsagourias, 'International Responsibility for Malicious Cyber Activities by Non-State Actors Operating from Failed States or Ungoverned Spaces', Journal of Conflict and Security Law.

have published reports about this topic from Northeast Asia to India, Pakistan,[2] the Middle East[3] and Eastern Europe.[4] Beyond political calculations, many states have also only recently started to develop their capabilities to project power through cyberspace. Therefore, it is not surprising that they would rely on the private market of cyber capabilities to build them. Even states that already have significant capacities can augment them through private actors or outsource functions to them for efficiency gains. This raises important questions about how governments interact with these private actors, how they can be held responsible and how to govern this private market of cyber force generally.

Two of the landmark documents providing insight into how the international community thinks about rules of the road for cyberspace explicitly reference the term 'proxies'. A group of governmental experts from 15 UN Member States (UNGGE), including representatives from the USA, China, Russia, the UK, France and India, agreed in a consensus report in 2013 that 'States must not use proxies to commit internationally wrongful acts.'[5] Two years later, the follow-up UNGGE built on the previous report by specifying that 'States must not use proxies to commit internationally wrongful acts using ICTs, and should seek to ensure that their territory is not used by non-State actors to commit such acts.'[6] This new group consisted of 20 Member States including the permanent five members of the Security Council, as well as Brazil, Israel and Pakistan. The latter report is noteworthy because it made explicit its view that this obligation is part of existing, and therefore binding, international law and it applies to the use of ICTs by states.

However, neither report defines 'proxy' nor does the term easily translate into other languages as an analysis of the same documents in the official non-English versions reveals. This article reviews what the term 'proxy' means and how it has been used in various contexts. It then focuses on the specific definition of proxies that seems to be the basis of the UNGGE reports: proxies understood as non-state actors used by a state actor. Yet, the question remains when does a non-state actor become the proxy of a state? And when can a state be held responsible for a non-state actor's activity? What are reasonable expectations for the application of the broader concept of due diligence? The core of the

2 S Unnithan, 'Inside the Indo-Pak Cyber Wars' (*India Today*, 18 March 2011) <http://indiatoday.intoday.in/story/india-pakistan-cyber-war-run-by-hired-hackers/1/132147.html> accessed 2 February 2016.

3 N Hopkins and L Harding, 'Pro-Assad Syrian hackers launching cyber-attacks on western media' *The Guardian* (29 April 2013) <http://www.theguardian.com/world/2013/apr/29/assad-syrian-hackers-cyber-attacks> accessed 2 February 2016.

4 J Carr, 'Rival hackers fighting proxy war over Crimea' *CNN* (25 March 2014) <www.cnn.com/2014/03/25/opinion/crimea-cyber-war/> accessed 2 February 2016.

5 UNGA 'Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security' (24 June 2013) UN Doc A/68/98.

6 UNGA 'Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security' (22 July 2015) UN Doc A/70/174.

article is therefore an analysis of the different logical distinctions and levels of detachment between a state and a non-state actor's activity. This framework is based on the counterterrorism literature, the logic underlying various standards in international law, and proposals for state responsibility and the broader concept of due diligence in the context of cyberspace. The goal is 2-fold: first, to provide a framework to think about the diverse array of existing proxy definitions; second, to conceptualise the relationship between a state and non-state proxies offering a guide to political decision-makers and a roadmap for future research focusing on proxy actors and cyberspace.

1. Proxies Generally

Proxies have existed around the world for centuries. Thucydides writes about proxies, including mercenaries and privateers used in the Peloponnesian War. Geraint Hughes's book on proxy warfare carries the title 'My Enemy's Enemy', a phrase taken out of the Arthashastra, a treatise on statecraft from India dating back to the fourth century BC.[7] Machiavelli wrote 'Mercenaries and auxiliaries are at once useless and dangerous, and he who holds his State by means of mercenary troops can never be solidly or securely seated.'[8] In Chinese history, the 36 stratagems include one recommending 'Kill with a borrowed sword'. According to an article published by the Shanghai Daily in 2013, 'the true meaning of this stratagem is to attack your enemy by using the forces or strength of a third party, or to entice your ally into attacking your enemy instead of doing it yourself.'[9] The Oxford English Dictionary lists 'proxy war' as a US specific term for 'a war limited in scale or area, instigated by a major power which does not itself become involved.'[10]

Meanwhile, the etymology of the English term 'proxy' dates back to the Latin word procurare, 'pro' meaning 'on behalf of' and 'curare' meaning 'to attend to; to take care of'. The Merriam-Webster Dictionary offers a contemporary definition of proxy as '(1) the agency, function, or office of a deputy who acts as a substitute for another, (2a): authority or power to act for another (3) a person authorized to act for another'.[11] In short, while the term's etymology is Latin

7 Stephen Walt also references this text in his 1985 *International Security* on alliance formation illustrating the importance of the principal-agent and power relationship between the two actors to distinguish proxies from allies: S Walt, 'Alliance Formation and the Balance of Power' (1985) 9 International Security 3.

8 N Machiavelli, Chapter XIII 'Of Auxiliary, Mixed, and One's Own Soldiers' *The Prince* (first published 1532, Dover Publications 1992; University of Chicago Press 2010) 31.

9 'Thirty-Six Stratagems Ancient ruses can still be useful' *Shanghai Daily* (Shanghai, 7 July 2013) <www.shanghaidaily.com/Vibe/now-and-then/%E4%B8%89%E5%8D%81%E5%85%AD%E8%AE%A1-ThirtySix-Stratagems-Ancient-ruses-can-still-be-useful/shdaily.shtml> accessed 31 January 2016.

10 *The Compact Edition of the Oxford English Dictionary: Complete Text Reproduced Micrographically - Volume II P-Z* (OUP 1971) 2342–43.

11 'Proxy' (Merriam-Webster) <www.merriam-webster.com/dictionary/proxy> accessed 2 February 2016.

and the modern 'proxy war' primarily US-centric, the phenomenon it describes has occurred across countries over millennia-granted, varying in its manifestations regionally and over time.

The International Relations (IR) literature reflects these varied meanings of proxies with articles referring to 'proxy war',[12] 'proxy warfare',[13] 'proxy warriors'[14] or 'proxies'.[15] They all focus and hinge on the question, what constitutes a proxy actor? During the Cold War, the term proxies became increasingly associated with one of the two super powers using another state as a proxy illustrated by the related terms 'satellite' or 'client' state.[16] For example, The New York Times wrote on 9 January 1955 that 'the United States would instantly retaliate with atomic weapons against the heart of the Communist world if the Commies started another proxy or brush-fire war.'[17] Karl Deutsch described proxy wars in 1964 as 'an international conflict between two foreign powers, fought out on the soil of a third country; disguised as a conflict over an internal issue of that country; and using some of that country's manpower, resources and territory as a means for achieving preponderantly foreign goals and foreign strategies.'[18] The more recent IR literature focuses specifically on non-state actors as proxies.[19] In his 2012 'My Enemy's Enemy – Proxy Warfare in International Politics', Hughes defines a proxy as 'a non-state paramilitary group receiving direct assistance from an external power'.[20] And Daniel Byman and

12 RK Cragin, 'Semi-Proxy Wars and U.S. Counterterrorism Strategy' (2015) 38 Studies in Conflict & Terrorism 311; M A Newton, 'War by Proxy: Legal and Moral Duties of "Other Actors" Derived From Government' (2006) 23 Case Western Reserve Journal of International Law 249; Geraint Hughes 'A Proxy War in Arabia: The Dhofar Insurgency and Cross-Border Raids into South Yemen' (2015) 69 The Middle East Journal 91.

13 B Dunér, 'Proxy Intervention in Civil Wars' (1981) 18 Journal of Peace Research 353.

14 A Ahram, *Proxy Warriors: The Rise and Fall of State-Sponsored Militias* (Stanford UP 2011).

15 C M Wyatt, 'Princes, Patriots, and Proxies: Great Power, Politics and the Assertion of Afghan Sovereignty' (2014) I Fletcher Security Review 126; Dunér (n 13).

16 MT Klare, 'Subterranean Alliances: America's Global Proxy Network' (1989) 43 Journal of International Affairs 97, 104; CG Brewer, 'Peril by Proxy: Negotiating Conflicts in East Africa' (2011) 16 International Negotiation 137.

17 *The Compact Edition* (n 10).

18 KW Deutsch, 'External Involvement in Internal Wars' in H Eckstein (ed) *Internal War: Problems and Approaches* (Free Press of Glencoe 1964) 102.

19 Y Bar-Siman-Tov, 'The Strategy of War by Proxy' (1984) 19 Cooperation and Conflict 263; A Mumford, *Proxy Warfare* (Polity 2013); A Ahram, 'Origins and Persistence of State-Sponsored Militias: Path Dependent Processes in Third World Military Development' (2011) 34 Journal of Strategic Studies 531; G Hughes, *My Enemy's Enemy: Proxy Warfare in International Politics* (Sussex Academic Press 2014); D Byman and S Kreps, 'Agents of Destruction? Applying Principal-Agent Analysis to State-Sponsored Terrorism' (2010) 11 International Studies Perspectives 1.

20 G Hughes, *My Enemy's Enemy: Proxy Warfare in International Politics* (Sussex Academic Press 2014) 11.

Sarah Kreps have written about proxies applying principal-agent theory, while Kim Cragin uses the term 'semi-proxy war' to underscore the importance of non-state actors.[21]

The IR literature on proxies relates to the law of agency[22] and principal-agent theory developed in the economics and business departments in the USA in the 1970s.[23] Adopted by political scientists soon thereafter, its extensive literature shows among others the various ways an agent can exercise power over the principal. Principal-agent theory has since also been applied in counterterrorism studies on the relationship between states and terrorist groups with useful insights for proxies using ICTs.[24] For example, Byman and Krebs offer the insight that 'rationalist calculations about efficiency gains explain only part of the dynamic between principal and agent in the state-terrorist group relationship. Rarely does a strategic cost-benefit logic, for example, explains the convergence of principal-agent preferences and behavioural outcomes. Rather, a strong ideological bond often reduces divergence and thus reduces the need for other control mechanisms.'[25] This also applies to proxies in cyberspace, for example, to hacktivist groups. At the same time, ideology can also create a need for control, for example, if there is not only an ideological bond, but the proxy's ideology might be more extreme than that of the principal in which case the proxy's actions might have to be tempered.[26] Moreover, proxies in the context of cybersecurity or counterterrorism also raise questions about what some have called 'passive support' especially in the context of harboring terrorists further discussed below.

This article's builds on this history and literature by conceptualising proxies starting with the broadest definition. The first category of proxies builds on its etymological roots[27] defining a proxy as 'actor b acting for actor a'. This definition already includes the two necessary elements of all proxy definitions: (i) a relationship between at least two actors and (ii) a relationship that is unequal (an equal partnership between two actors would be better described as partners or allies).[28] Building on Andrew Mumford's scholarship, actor b can therefore be described as the *proxy*, whereas actor a is the *beneficiary*.[29] Therefore, the best way to describe the relationship between the two for this broad category is that one of the two actors is the beneficiary and the other is the proxy. Other

21 Byman and Kreps (n 19); Cragin (n 12) 312.
22 W Müller-Freienfels, 'Agency', *Encyclopedia Britannica* <www.britannica.com/topic/agency-law> accessed 2 February 2016.
23 BM Mitnick, 'Origin of the Theory of Agency: An Account by One of the Theory's Originators' (University of Pittsburgh 2013) <www.pitt.edu/~mitnick/agencytheory/agencytheoryoriginrev11806r.htm> accessed 31 January 2016.
24 D Byman and S Kreps, 'Agents of Destruction? Applying Principal-Agent Analysis to State-Sponsored Terrorism' (2010) 11 International Studies Perspectives 1.
25 ibid 12.
26 I thank Joseph Nye for this thought.
27 P Towle, 'The Strategy of War by Proxy' (1981) 126 The RUSI Journal 21.
28 Dunér (n 13) 357.
29 Mumford (n 19) 11.

Table 1. Beneficiary–proxy relationships

		Actor b: proxy			Actor c
		state	non-state		
Actor a: beneficiary	state	I	II*	→	*State*
	non-state	III	IV		*Non-state*

words used to describe this relationship are sponsor-client,[30] patron-client,[31] principal-agent, benefactor-proxy,[32] satellites,[33] auxiliary,[34] surrogates,[35] etc. It is worth emphasising that this terminology should not distract from the fact that the proxy is also deriving a benefit from this relationship and it is an empirical question who derives greater benefit. Last but not least, some articles use the term proxy implying not only a relationship between two but three or more actors with the proxy's actions being directed at a third or more parties. The broad definition of proxy therefore requires at least two, but not necessarily only two, actors.

The second and narrower category defines one of the two actors with more specificity, as outlined in Table 1. Usually actor a is assumed to be a state narrowing the definition of a proxy to 'actor b acting for actor a, state A'. This category has two subcategories further specifying the type of actor b. Subcategory (I) narrows the definition to 'actor b, state B, acting for actor a, state A' corresponding with cell I in Table 1. This includes the aforementioned literature on satellite and client states. In subcategory (II), actor b is a non-state actor, narrowing the definition to 'actor b, non-state actor I, acting for actor a, state A' corresponding with cell II in Table 1. The literature on the private

30 M Schmitt and L Vihul, 'Proxy Wars in Cyber Space: The Evolving International Law of Attribution' (2014) I Fletcher Security Review 55, 59–60.

31 I Salehyan, 'The Delegation of War to Rebel Organizations' (2010) 54 Journal of Conflict Resolution 493; SJ Majeski and DJ Sylvan, 'Institutionalizing the Ad Hoc: New Military Aid Programs' (American Political Science Association 2013 Annual Meeting, Chicago, IL, 29 August–1 September 2013) <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2300093> accessed 16 December 2015;
Ahram (n 19) 543.

32 Mumford (n 19) 56.

33 Dunér (n 13) 354.

34 Thucycides, Chapter XIII 'Seventh and Eighth Years of the War - End of Corcyraean Revolution - Peace of Gela - Capture of Nisaea' History of the Peloponnesian War (translated by R Crawley, Penguin Books 1964); Machiavelli n (8)

35 J Bernier, 'Asia's Shifting Strategic Landscape: China's Strategic Proxies' (2003) 47 Orbis 629, 634; Klare (n 16) 97–98.

market of force and outsourcing (for example, the scholarship on private security companies) can be grouped under this category.

Subcategories (I) and (II) usually underlie definitions used in the extensive literature on intervention, which includes a third actor c, to which actor b's actions are directed. Actor c is usually assumed to be another state, but can also be a non-state actor. This category includes the literature on privateers,[36] mercenaries,[37] proxy wars[38] and proxy warfare,[39] intervention as well as private sector companies to the extent that their activities relate to a third actor. This category also includes the body of work on state-sponsored terrorism and the scholarship in international law focusing on proxies that's the focus of this journal's edition.

Categories (III) and (IV) diverge from the state-centric approach of the second category and associated scholarship. It is worth pointing out that the beneficiary, actor a, need not be a state, but can be a non-state actor using a state or a non-state actor as a proxy corresponding with cells (III) and (IV) in Table 2. The literature on 'weak states' and organised crime provides examples of states having been co-opted by organised crime groups for their purposes. Moisés Naím also describes the blurring of lines between the state and organised crime groups in his 2012 'Mafia States' quoting Atanas Atanasov, a member of the Bulgarian parliament and a former counterintelligence chief, as saying that 'other countries have the mafia; in Bulgaria the mafia has the country.'[40] This third category is useful to bear in mind given that some non-state actors have

36 FR Stark, 'The Abolition of Privateering and the Declaration of Paris' in Faculty of Political Science of Columbia University (eds), *Studies in History, Economics and Public Law* (Columbia University 1897); J Thomson, *Mercenaries, Pirates, and Sovereigns: State-Building and Extraterritorial Violence in Early Modern Europe* (Princeton UP 1996); C Ford, 'Here Come the Cyber Privateers' (Hudson Institute, 2010) <www.hudson.org/research/9112-here-come-the-cyber-privateers> accessed 31 January 2016; B Hallas, 'Are Nation States Resorting to Cybersecurity Privateering?' (2012) <www.brucehallas.co.uk/are-nation-states-resorting-to-cybersecurity-privateering/> accessed 31 January 2016; JR Clark, 'Arghhh … Cyber-Pirates' (2013) <http://josephrogerclark.com/2013/05/28/arghh-cyber-pirates/> accessed 31 January 2016; JC Hirsch and S Adelsberg, 'An Elizabethan Cyberwar' *The New York Times* (31 May 2013) <www.nytimes.com/2013/06/01/opinion/an-elizabethan-cyberwar.html?_r=0> accessed 31 January 2016; Peter W. Singer and A Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (OUP 2014); TE Ricks, 'Cyber-Privateers' (Foreign Policy, 29 April 2014) <http://foreignpolicy.com/2014/04/29/cyber-privateers/> accessed 31 January 2016; F Egloff, 'Cybersecurity and the Age of Privateering: A Historical Analogy' (2015) Cyber Studies Working Papers 1 <http://www.politics.ox.ac.uk/materials/centres/cyber-studies/Working_Paper_No.1_Egloff.pdf> accessed 1 February 2016.

37 D Avant, *The Market for Force: The Consequences of Privatizing Security* (Cambridge UP 2005); P Singer, *Corporate Warriors: The Rise of the Privatized Military Industry* (Cornell UP 2007); Ž Branović and S Chojnacki, 'The Logic of Security Markets: Security Governance in Failed States' (2011) 42 Security Dialogue 553.

38 Cragin (n 12); Newton (n 12); Hughes (n 12) 91.

39 Mumford (n 19) 56.

40 M Naím, 'Mafia States: Organized Crime Takes Office' (2012) 91 Foreign Affairs 100.

cyber capabilities that are more sophisticated than those of many states. They can use a state's infrastructure for their own purposes. An example for category (IV) would be one hacker group asking another to hack a specific target or a company hiring a hacker targeting a third party.[41]

The aforementioned categories discuss proxies primarily through the lens of actor a, the beneficiary. It is important to remember that the actor treated as the affected third party, actor c, can in turn itself use a proxy either affecting actor a or yet another actor altogether. This quickly complicates the analysis and many empirical examples consist of such a complex multi-party environment. Moreover, this review of the proxy literature and categorisation does not yet capture important other elements that come into play such as (i) territory and the location of the beneficiary and proxy; (ii) time and the duration of the action the proxy carries out for the beneficiary, which could be measured not only in years, months, weeks or days but also daytime or nighttime[42] making attribution and questions of autonomous behaviour even more complicated and; (iii) the nature of the action ranging from overt to covert from direct to indirect to name but a few. These are beyond the scope of this article.

2. 'Proxies' in the 2013 and 2015 Reports of the UN Group of Governmental Experts

Neither of the UNGGE reports defines 'proxies'. Moreover, the term does not easily translate into other languages as an analysis of the same document in the official non-English versions reveals. The 2013 UNGGE report uses the term three times, including once in the UN Secretary-General's foreword that only exists in English. Paragraph 6 states 'individuals, groups, or organizations, including criminal organizations, may act as proxies for States in the conduct of malicious ICT actions' and paragraph 23 'States must not use proxies to commit internationally wrongful acts.' (What is interesting about the UN Secretary-General's foreword is that he distinguishes proxies as a category separate from non-state actors 'existing and potential threats from States, their proxies or non-State actors through the use of ICTs'.[43]) In the 2015 UNGGE report, the term 'proxies' appears only once in paragraph 28 (e) 'States must not use proxies to commit internationally wrongful acts using ICTs, and should seek to ensure that their territory is not used by non-State actors to commit such acts.'

The Chinese version of the 2013 and 2015 reports uses 代理 (dàilǐ) throughout, meaning 'representative' in a broad sense. This term has been used in the context of Cold War studies in combination with 国 (guó), meaning 'country',

41 D Kravets, 'Exclusive: I Was a Hacker for the MPAA' (Wired, 22 October 2007) <http://archive.wired.com/politics/onlinerights/news/2007/10/p2p_hacker?currentPage=all> accessed 17 March 2016.

42 J Healey, 'The Spectrum of National Responsibility for Cyber Attacks' (2011) 18 Brown Journal of World Affairs 57.

43 UNGA (n 5).

with 代理国 describing satellite states. In the UNGGE reports, 代理 is used in combination with 人 (rén) for people, adding to its meaning the notion of an 'agent'. With regard to other languages, the Arabic term in paragraph 6 of the 2013 report can be translated to the English word 'delegates', whereas the syntax of the French and Spanish sentences is such that it avoids using the specific term where the English version reads 'proxy'. Similarly, the Russian version does not include a specific word similar to proxies, but describes it by including 'act in the interests of states'. In paragraph 23, on the other hand, the French, Spanish and Russian texts do include a word for 'proxy', but the terms used are more similar to the English words 'agent' or 'intermediary', in French 'leurs agents', in Spanish 'agentes', and in Russian 'посредников', which can be translated as 'intermediary' or 'middleman'. The Arabic terminology can be translated as 'entities acting on behalf of states'. Similarly, the versions of the 2015 report in official UN languages other than English use a variety of terms. The French version no longer uses 'agents' but 'intermédiaires' and the Spanish version uses 'terceros', third parties, instead of 'agentes'. The Russian text uses a synonym for the word used in paragraph 23 of the 2013 report 'представителей'. The Arabic version can be translated as 'indirect means/ways'.

While there is little public information available about how the various states interpret this language specifically, some details are available about the US government's understanding of the term. At a workshop focusing on proxy actors in cyberspace hosted by the Association of Southeast Asian Nations (ASEAN) Regional Forum in Viet Nam in March 2012, a foreign service officer at the US Department of State, Dr Sharri Clark, defined proxy actors as 'groups and individuals who, on behalf of a state (and possibly involving a state unwittingly), take malicious cyber actions against the governments, the private sector and citizens of other states.'[44] Koh also addressed this circumstance in his speech at Ford Meade. In fact, in response to the question 'Are States responsible when cyber acts are undertaken through proxies?', Koh highlights:

> Yes. States are legally responsible for activities undertaken through 'proxy actors', who act on the State's instructions or under its direction or control. The ability to mask one's identity and geography in cyberspace and the resulting difficulties of timely, high-confidence attribution can create significant challenges for States in identifying, evaluating, and accurately responding to threats. But putting attribution problems aside for a moment, established international law does address the question of proxy actors. States are legally responsible for activities undertaken through putatively private actors, who act on the State's instructions or under its direction or control. If a State exercises a sufficient degree of control over an ostensibly private person or group of persons committing

44 'Co-Chairs' Summary Report' (ARF Workshop on Proxy Actors in Cyberspace, Hội An City, 14–15 March 2012) <www.mofa.go.jp/files/000016404.pdf> accessed 31 January 2016.

> an internationally wrongful act, the State assumes responsibility for the act, just as if official agents of the State itself had committed it. These rules are designed to ensure that States cannot hide behind putatively private actors to engage in conduct that is internationally wrongful.[45]

Interestingly, while Clark includes the possibility of a state being involved unwittingly, Koh's statement is more limited focusing on actors acting under a State's instruction, direction or sufficient degree of control.[46]

Both remarks suggest that the term proxies used in the English version and related terms in the other languages represent proxies consisting of non-state actors with a state as the beneficiary. (This corresponds with the aforementioned second category of proxies, specifically the second subcategory (II) marked with an asterisk in Table 1.) Other supporting documents, the context of the UNGGE's language, and commentary by officials involved in the process support this conclusion. It is noteworthy that the UNGGE reports add a normative dimension to their references of proxies by specifically mentioning proxies that 'commit internationally wrongful acts'. This language builds on the International Law Commission's 2011 'Draft[47] Articles on the Responsibility of States for Internationally Wrongful Acts.'[48]

Yet, Koh's conclusion regarding a state's responsibility faces two caveats: first, the high legal thresholds and, second, the attribution problem. First, Michael Schmitt and Liis Vihul, who have produced one of the most comprehensive discussions of proxies in this context with their 2014 article 'Proxy Wars in Cyberspace: The Evolving International Law of Attribution', conclude that 'the relatively high levels of support that are required before a state can be held responsible for the activities of non-state groups or individuals, as distinct from their own responsibility for being involved, creates a normative safe zone for them.'[49] In other words, the existing international law standards of 'direction or control'[50] outlined in article 8 of the 'Draft Articles on the Responsibility of

45 Koh (n 1).

46 I thank Duncan Hollis for this observation.

47 There is a discussion among international lawyers whether the articles are still 'draft' articles following the UN General Assembly's reference of them in a resolution or not, the reference in this article is based on the title of the ICJ document.

48 The UN International Law Commission 'Draft Articles on the Responsibility of States for Internationally Wrongful Acts, with commentaries' (2001) UN Doc A/56/10 do not reference the term proxy, mercenary, privateer, client, or surrogate, but, nearly 500 years after Machiavelli expressed his disdain at the use of auxiliaries [the draft articles] do refer to 'auxiliaries' twice on page 47.

49 Schmitt and Vihul (n 30) 71.

50 It is noteworthy that linguistic challenges are not limited to the term 'proxy'. For example, Art 17(7) of the *Draft Articles on the Responsibility of States for Internationally Wrongful Acts* (n 48) mentions 'The choice of the expression, common in English, "*direction and control*", raised some problems in other languages, owing in particular to the ambiguity of the term "direction" which may imply, as is the case in French, complete power, whereas it does not have this implication in English'.

States for Internationally Wrongful Acts' are so high that they are unlikely to be useful for most situations encountered by political decision-makers today.

Second, Koh mentioned the attribution problem and the technology's ability to obfuscate the origin of a malicious activity. This problem is not as insurmountable as some have claimed. It is clear that attribution is possible as successful law enforcement cases and prosecutions have shown in the past. Moreover, attribution is not binary but has varying degrees.[51] Often, the question is less *if* attribution is possible but *by when*. Moreover, the quality of the attribution depends on the skills and resources available and the complexity of the malware. At the same time, robust attribution remains challenging, which is often not available within the timeframe that decision-makers need to act, and while some countries are getting better at attribution, asymmetric attribution capabilities among countries will persist.

To help think about other potential options, it is therefore helpful to outline the full spectrum of how a state can relate to a proxy's action. For example, the literature on terrorism also discusses passive state sponsorship and distinguishes between state-sponsored, state-supported and state-sanctioned terrorism.[52] It illustrates that attribution and when to hold a state responsible is ultimately a political decision.[53] Jason Healey, a leading cybersecurity expert who has worked at the White House, echoes this assessment with his statement that 'For national security policymakers, knowing "who is to blame?" can be more important than "who did it?"'[54] This article therefore offers a comprehensive review of how the activity of a non-state actor can relate to a state. The following table and framework below try to accomplish three goals: (i) translate the insights from the counterterrorism literature to proxies and cybersecurity; (ii) expand Healey's framework; and (iii) marry the former two with the nuanced distinctions and thresholds embodied in international law.

3. Non-State Proxies and Relationship with the State

The following section describes the possible relationships between a beneficiary state and a proxy's actions combining the insights from: (i) the counterterrorism literature; (ii) a proposal for state responsibility developed for cyber-attacks and; (iii) the nuanced spectrum outlined in international law. It is important to highlight that the various tests and logical distinctions used in this section originate in various bodies of international law and institutions. International lawyers have developed different, sometimes competing standards based on

51 T Rid and B Buchanan, 'Attributing Cyber Attacks' (2015) 38 Journal of Strategic Studies 4.

52 D Byman, 'Passive Sponsors of Terrorism' (2005) 47 Survival 140.

53 For a good illustration see D Jinks' on how the response to 9/11 expanded state responsibility to include 'harboring' in D Jinks, 'State Responsibility for the Acts of Private Armed Groups' (2003) 4 Chicago Journal of International Law 83.

54 Healey (n 42).

highly fact-dependent circumstances ranging from the International Court of Justice (ICJ) to the International Criminal Tribunal for the former Yugoslavia (ICTY) and apply only under specific conditions. This article focuses on the logical distinctions made in these various standards describing different degrees of separation between a state and the non-state actor. The table therefore integrates the different bodies of law and combines them for the purpose of developing a comprehensive framework detailing the logical differentiations of a state's relationship with a non-state actor, without regard for the legal consequences of different categorisations, eg, the legal availability of countermeasures, etc.

To start, two general distinctions can be made. The first is whether the state responsibility for the proxy's malicious cyber activity is established ex ante or ex post of the incident. It is important to highlight that while the term 'cyber-attack' is often used in the literature, malicious cyber activity can take place over a prolonged period of time—months if not years—is often undetected, and is therefore better described as 'cyber operations' rather than 'attack' to represent the prolonged rather than ephemeral nature of most intrusions, at least those witnessed to date. Apart from the special case of Distributed Denial of Service attacks targeting the availability of information, intrusions to undermine the availability, confidentiality or integrity of information often take place over months and are therefore emphasised here, by using the descriptor '*ex ante* and *in progressu*'. Moreover, while an intrusion can be used to cause an effect rising to the level of use of force or armed attack, lesser disrupting and damaging effects also raise questions of state responsibility.

The second distinction is the beneficiary state's choice between the commission and omission of specific acts. With regard to the latter, Byman's counter-terrorism scholarship differentiates between active state sponsorship and passive state sponsorship. Both can occur *ex ante* and *in progressu* or *ex post*. For example, as long as a state is aware that a particular activity is going to begin, or is in progress, it has a range of choices available to it. It may willingly allow or facilitate the activity to being or to continue, or it may do nothing, particularly if it is incapable of stopping or at least warning the victim. A state also has a range of choices after an activity has started or concluded including the ability to prevent it from reoccurring, for example, by patching vulnerable infrastructure, or to provide assistance, to investigate or to punish the actor carrying out the malicious activity. It is worth noting that distinguishing a state's options is not a new discussion in international law. For example, Brierly discussed this topic in an article published in 1928, including a discussion whether failing to punish harmful activity can be considered 'implied complicity' or 'condonation' of an activity.[55] He prefers to call it the latter and this article uses 'condonation' for the non-punishment of an activity while referring to 'implied complicity' in case of non-prevention to maintain a logical distinction between the two omissions.

55 James Leslie, 'The Theory of Implied State Complicity in International Claims' (1928) 9 British Yearbook of International Law 42.

Another relevant international law concept in this context is denial of justice and 'By what artifice might a state owe a duty to the world at large to maintain an adequate system for the administration of justice?'[56]

A. Ex Ante and In Progressu

The varying degrees of separation of a non-state actor from the state can be described as follows moving from the smallest degree of separation to the largest. To start, the state itself and de jure state organs recognised as such under domestic law are a stand-alone category since they are formally part of the state, whereas non-state actors are formally not part of the state.

The first category of proxies, those with a first, and smallest level of detachment from an organisational perspective, are actors that are not part of the state but completely dependent on the state such as de facto state organs or exercise government authority.[57] (For example, Schmitt and Vihul consider the Estonian Defense League's Cyber Unit to fall into this category.[58]) This article uses this legal distinction to draw the line between the state as such and actors under what Byman calls 'active state sponsorship'.

The next category and degree of detachment constitutes non-state actors under a state's instruction such as auxiliaries, non-state actors that are instructed and authorised by the state supplementing a state's activity. This category is closely followed by non-state actors under the direction or control of the state, including those under the 'effective control' of the state meaning its specific operation is under the instruction of the state.[59]

The next three degrees of separation further remove the actors from the state. These are actors not under 'effective' but 'overall control'[60] of the state, where the state is not directly controlling a specific operation, but exercises general influence by participating in the planning and supervision, organising,

56 Paulsson (n 37) 1; I thank Duncan Hollis for this addition. Other relevant works on denial of justice include A Freeman, *The International Responsibility of States for Denial of Justice* (Longmans, Green and Company 1938) 758.

57 With regard to state-owned entities, Schmitt and Vihul write on page 61, 'Of particular note are state owned IT companies. Ownership by the state as such does not suffice for attribution. Instead, a company (assuming it is not exercising elements of governmental authority) must be acting under the instruction, direction, or control of the state before its cyber activities are attributable to that state' building on Art 8(6) of the ILC 'Articles on Responsibility of States' for Internationally Wrongful Acts (3 August 2001) UN Doc A/56/83.

58 Schmitt and Vihul (n 30) 60.

59 *Case Concerning Military and Paramilitary Activities in and Against Nicaragua* (*Nicaragua v US*) [1986] ICJ Rep 14. For a discussion of the international legal rules relating to attribution in cyberspace, see in this volume K Mačák, 'Decoding Article 8 of the International Law Commission's Articles on State Responsibility: Attribution of Cyber Operations by Non-State Actors', Journal of Conflict and Security Law.

60 *Tadic Case* (Judgment) ICTY-94-1 (26 January 2000).

coordinating or planning of the non-state actors' activities or has the power and ability to instruct the non-state actor to stop. These loser criteria apply to organised groups, whereas individuals and loose groups of individuals need to meet the higher threshold of receiving instruction from a state for the threshold of overall control to apply.

The distinction between 'overall control' and the next degree of separation is particularly important in international law. The Appeals Chamber of the International Tribunal for the Former Yugoslavia lowered the 'effective control' threshold by establishing a distinct 'overall control' criterion in the Tadić case. These two thresholds were applied to two different contexts and could also be viewed as competing views among the ICJ and the ICTY. The ICJ case focused on state responsibility whereas the ICTY focuses on individual criminal responsibility and in the Tadić case specifically the applicable rules of international humanitarian law.[61] Logically, the 'overall control' test lowers the 'effective control' threshold, although still excludes from state responsibility non-state actors receiving specific support in form of financing, provision of equipment, supply of weapons, training, intelligence support or logistics support. The Appeals Chamber argued that these forms of support do not rise to the threshold of participation in planning and supervision, elements that are required in order to establish overall control. It is at this point and below where attribution and state responsibility transition from the primarily legal to the political realm.

The last category constituting active state sponsorship ex ante or in progressu is a non-state actor receiving not specific but general support, for example, a government actively making statements sympathetic to the non-state actor, such as Ayatollah Khamenei reportedly telling a group of university students, 'You are the cyber-war agents and such a war requires Amman-like insight and Malik Ashtar-like resistance. Get yourself ready for such war wholeheartedly.'[62]

With regard to what Byman describes as 'passive' state sponsorship, the remaining ex ante and in progressu classifications are characterised by a state's omission to take certain action. This relates to the broader concept of due diligence in international law.[63] This includes when the state simply chooses not to prevent the non-state actors' activity, in spite of being aware of the specific operation and capable of stopping it directly or at least warning the victim, presumably because the state perceives that it can benefit from the activity. Such action implies a state's complicity, given its knowledge ex ante and in progressu, to the activity taking place. Furthermore, a state is 'harboring' a non-state actor when it is unaware of *specific* operations, but aware and capable of *generally* stopping activities, yet essentially willing to turn a blind eye and

61 'Draft Articles on the Responsibility of States' (n 48), Art 8(5).

62 'Iran's Supreme Leader Tells Students to Prepare for Cyber War' *Russia Today* (13 February 2014) <www.rt.com/news/iran-israel-cyber-war-899/> accessed 31 January 2016.

63 International Law Association Study Group on Due Diligence in International Law, 'First Report' (7 March 2014) <www.ila-hq.org/en/committees/study_groups.cfm/cid/1045> accessed 2 February 2016.

thereby willing to provide sanctuary, allow fundraising, recruiting activity, or the acquisition of weaponry. Similar to non-prevention, a state can engage in willful non-termination being aware of the ongoing malicious activity and capable of stopping it, yet unwilling to do so. It is lower on the scale for state responsibility compared with non-prevention because the effect or at least part of the effect has already occurred.

The exact scope of what to consider passive state sponsorship remains controversial. The following three categories are included here to be comprehensive yet it remains questionable if they can actually be considered passive state sponsorship. This includes what I call 'apologetic non-cooperation', 'apologetic cooperation' and 'mitigation and termination following negligence'. They all have in common that the state is willing to terminate the malicious activity. Yet, in the case of apologetic non-cooperation the state is willing but not capable of providing assistance. In case of apologetic cooperation, the state is willing yet incapable to terminate the activity but does provide assistance. The last scenario consists of a state that stops or at least disrupts the malicious activity but did not harden systems sufficiently beforehand to prevent the activity from occurring.

For the specific context of cyber-attacks, Healey developed a stand-alone framework for state responsibility. This article builds on his excellent foundation and expands it primarily by integrating international law and including the *ex ante*, *in progressu* and *ex post* distinctions. (Healey does not reference the 'Draft Articles on the Responsibility of States for Internationally Wrongful Acts' and international law cases.) Healey's description of 'state-executed' attacks corresponds with the involvement of de jure state organs under international law.[64] When de facto state organs are involved, Healey uses the term 'state-integrated' attacks, which, together with the following categories, fall into what Byman classifies as 'active state sponsorship' and arguably also includes auxiliaries. Healey's category of 'state-ordered' includes the international law categories of non-state actors under a state's instruction, direction or effective control. The biggest divergence between his classifications and those in international law concern non-state actors under a state's overall control and Healey's differentiation between 'state-ordered', 'state-coordinated' and 'state-shaped' as illustrated in Table 2. This article also includes a few more categories relating to cooperation and denial of justice.

B. Ex Post

After an activity has ended, there are other ways a state can be involved. This includes the active step of adopting the non-state actor's activity that has already

64 For an application of Healey's framework, see R Beijtlich's about North Korea and the Sony hack published in R Bejtlich, 'What Does "Responsibility" Mean for Attribution?' (*TaoSecurity*, 22 December 2014) <http://taosecurity.blogspot.com/2014/12/what-does-responsibility-mean-for.html> accessed 31 January 2016.

occurred as its own and taking action in support of it, for example, defending it. One step removed is a state's verbal endorsement of a non-state actor's activity without taking further action in support of it. On the passive side, a state may choose not to punish a non-state actor thereby condoning its actions.

Again, three categories are included in this article to be as comprehensive as possible, but it is an open question whether they can be considered passive state sponsorship. These include what I call 'apologetic non-punishment', 'non-cooperative investigation' and 'punishment following negligence'. When the state is willing, yet incapable, to punish the responsible non-actor, for example, due to domestic laws protecting privacy or minors,[65] it can be considered 'apologetic non-punishment'. The state might even condemn the activity publicly, but there is no punishment. Next on the spectrum is the scenario where the responsible actor is not and remains unknown and the state is unwilling to cooperate in the investigation. And last, one could think of an incident for which the state does punish the responsible non-state actor, but the state did not harden systems sufficiently to prevent such activity from occurring in the first place.

Needless to say that for all of these categories, especially the ones relating to passive state sponsorship, assessing a state's responsibility depends on intent and the broader political context. Its actions will depend on the extent to which the state is benefitting from the activity of the non-state actor.

Table 2 focuses on the logical distinctions that can be made between a state's relationship with a non-state actor' activities. Other variables relevant in the context of proxies but beyond the scope of this publication include:

1. a non-state actor constitution can be an ongoing enterprise or an ad hoc grouping;
2. a non-state actor's relationship with the state can be ongoing or ad hoc, an example of the latter would be a criminal group that is usually only profit-driven becoming politicised during a conflict and working with the state, such as the mafia and US military in World War II;
3. the state's relationship with a non-state actor and the standards to apply will differ during peace time and times of an armed conflict;
4. the relationship between a state and the proxy can be overt or covert or, to use the language of the law of agency, the principal can be a disclosed or undisclosed principal;[66]
5. the relationship may be legal, illegal or taking place in a legal grey zone;[67]
6. an actor might be a state employee during working hours from 9 AM to 5 PM but carry out actions autonomously from 5 PM to 9 AM;[68]

65 I thank Matthew Noyes for this point.
66 Mumford (n 19).
67 Ahram (n 31).
68 Healey (n 42) 59.

7. intent is another variable, be it profit- or politically driven or mixed motive;
8. the nationality of the state actors and non-state actors involved has jurisdictional implications;
9. especially relevant in the context of cybersecurity, the geographic location of a proxy actor cannot always be assumed to be on the beneficiary state's territory or that of the affected third party. The proxy actor might be operating from another fourth or be spread across multiple other states to carry out its activities.

Last but not least, this discussion needs to take into account differences between states' systems, capabilities, and cultural contexts. As Deborah Avant points out in her seminal 'The Market for Force', 'all of this refers to the world of advanced, industrialized countries where the state, government, and public revolve around some notion of collective good. In parts of the developing world, state institutions and international recognition of them function mainly as mechanisms for rulers to achieve personal (private) gain.'[69] The distinction between state and non-state, as well as public and private, therefore differs across countries and political systems.

4. Conclusion

The research for this article points to a number of key takeaways. First, the term 'proxies' has been used in very different categories within and across academic disciplines, making it necessary to define or clarify which category is meant when the term is being used. This is particularly important in an international context since the term itself does not easily translate into other languages. Second, analysing the specific nature of a relationship between a state and a non-state proxy requires attribution especially for a potentially affected third party to decide what actions to take in response. Such attribution may occur across a spectrum ranging from active to passive state sponsorship and depends on the level of support, a state's knowledge, and a state's capability to potentially stop the activity of a non-state proxy. However, attribution takes time and attribution challenges continue to exist including asymmetric attribution capabilities across states. Therefore, and with regard to the high existing legal thresholds, the discussion would benefit from a stronger focus on other regimes to govern security that can complement the attribution-based regime around deterrence and compellence.

Some scholars[70] have started to shift attention to study a state's responsibility for malicious activity emanating from its territory independent of whether it can

69 Avant (n 37) 24.

70 M Schmitt, 'In Defense of Due Diligence in Cyberspace' (2015) 125 Yale Law Journal Forum 68; D Hollis, 'An e-SOS for Cyberspace' (2011) 52 Harvard International Law Journal 374; Healey (n 42) 67.

be attributed to or is actively sponsored by the state. This idea of 'due diligence' dates back to the 17th century and Hugo Grotius and US Supreme Court justice Moore observed in 1927 that '[i]t is well settled that a State is bound to use due diligence to prevent the commission within its dominions of criminal acts against another nation or its people.'[71] The 2015 UNGGE report incorporates elements of this concept in its sections on existing international law, voluntary and non-binding norms as well as the section on confidence-building measures. As Table 2 shows, specific issues that need attention include the various scenarios that may constitute passive state sponsorship. Moreover, the report is silent on a state's responsibility to take preventive measures and it does not clarify if 'emanating from their territory' and these provisions apply to transit states, only to states that are the original source of the malicious activity or both.

Additional questions relevant for future research include those focusing on the types of malicious activity, expectations for international cooperation, and expectations for unilateral action. For example, what do states consider to constitute 'malicious activity'? When are states required to mitigate and stop malicious activity transiting through or emanating from their territory and how? When are states required to provide assistance before and during an incident and how? As Hollis points out, 'In terms of severity, notably, most losses from cyber threats involve risks of only economic loss. Traditionally, the law of the sea handles such losses under different rules [than the SOS], known as salvage. Salvors provide assistance in recovering property lost at sea, but are paid to do so.'[72] When are states required to assist with an investigation after an incident and how? What happens if states fail to meet these expectations because it is unwilling or incapable? And to what extent can states be required to harden their infrastructure? An open question is whether a state 'bears some passive responsibility for the attack, both for being unable to stop it and for having insecure systems in the first place',[73] as Healey argues. If a state is unable to stop an attack because it has limited resources, does that mean there is also a passive responsibility for states with more resources for helping states to be able to stop attacks? And what thresholds apply? Conceptualising proxies is only a first step to this broader research agenda that will necessarily need to include non-Western perspectives and scholarship.

71 Case of the SS Lotus (*France v Turkey*) [1927] PCIJ Rep Series A No 10. On the topic of due diligence in cyberspace see in this volume Russell Buchan, 'Cyberspace, Non-State Actors and the Obligation to Prevent Transboundary Harm', Journal of Conflict and Security Law.

72 Hollis (n 70) 413.

73 Healey (n 42) 59.

Table 2. Degrees of detachment and relationship between the state and non-state proxies' activities affecting a third party

Time	Counterterrorism—form of sponsorship		Degrees of detachment[74]	Description of relationship informedby international law	Cyber-attack(Healey)[75]
			State	Exclusively government actors	State-executed(special case: state-rogue-conducted)
			de iure state organ*	State organs recognized as such in domestic law	
	Below are the non-state actors ordered by their degree of detachment from the state starting from low levels to high levels of detachment				
ex ante and *in progressu*	Active statesponsorship** (commission)[76]	State-sponsored	*de facto* state organ*	Private actors are *de facto* state organs completely dependent on state (can include unauthorized action e.g. rogue unit)	State-integrated
			Non-state actor exercising'governmental authority'*	Non-state actor exercising elements of government authority* (can include unauthorized action e.g. rogue unit)	
			Non-state actors under a state's instruction – 'auxiliary'*	Non-actors authorized or acting on instruction of a state usually to supplement a state's activity	State-ordered
			Non-state actor under a state's 'direction or control'*, specifically 'effective control'[77]	State involved in control of specific operation providing guidance through planning, direction, and support with non-state actor as subordinate and dependent on state	
			Non-state actor under a state's 'overall control'***[78] (organized groups)	State exercises generalinfluence, namely by-participating in planning and supervision- being involved in organizing, coordinating or planning- power to or ability to instruct to stop	State-coordinated/State-shaped
			Non-state actorunder a state's 'overall control'*** (individuals and loose group of individuals)	State issues specificinstruction	State-ordered
		State-supported	Non-state actor receivingspecific support from state***	State involved in financing,providing equipment, supplying weaponry, training, intelligence support, and/or logistics support	State-coordinated/State-shaped
			Non-state actor receivinggeneral support from state	State provides general encouragement or support	-

(continued)

Table 2. Continued

Time	Counterterrorism—form of sponsorship		Degrees of detachment[74]	Description of relationship informedby international law	Cyber-attack(Healey)[75]
ex ante and *in progressu*	Passive state sponsorship** (omission)	State-sanctioned	Non-prevention ('implied complicity')[79]	State does not prevent activity: state is aware of specific operation and capable of stopping planned activity directly or by warning yet unwilling	State-ignored
			'Harboring'[80]	State harbors non-state actor: state is unaware of specific operation but aware and capable of generally denying activities yet willing to provide sanctuary, allow fundraising activity, allow recruiting activity, and/or allow acquisition of weaponry**	
			Willful non-termination	State is capable but unwilling to terminate ongoing non-state actor's activity	
	?	?	Apologetic non-cooperation	State is willing yet incapable to terminate malicious activity but does not provide assistance	State-prohibited-but-inadequate
			Apologetic cooperation	State is willing yet incapable to terminate malicious activity but does provide assistance	
			Mitigation and termination following negligence	State is willing and (partially) capable of disrupting or terminating malicious activity but did not harden systems sufficiently to prevent malicious activity in the first place	State-prohibited
ex post	Active state sponsorship (commission)	State-sponsored	Non-state actor's behavior 'adopted' by state	State acknowledges and adopts non-state actor's conduct as its own including taking steps to support or defend beyond mere acknowledgment[81]	State-encouraged
		State-supported	Non-state actor receives verbal endorsement by state	State endorses non-state actor's activity by expressing verbal support for non-state action*	

(continued)

Table 2. Continued

Time	Counterterrorism—form of sponsorship		Degrees of detachment[74]	Description of relationship informedby international law	Cyber-attack(Healey)[75]
ex post	Passive state sponsorship (omission)	State-sanctioned	'Condonation'[82]	State is capable yet unwilling to punish non-state actor	-
	?	?	Apologetic non-punishment	State is willing yet incapable to punish non-state actor, for example, due to domestic laws protecting privacy or minors	-
			Non-cooperative investigation	State does not cooperate in investigation and non-state actor remains unknown	-
			Punishment following negligence	State punishes non-state actor but did not harden systems sufficiently to prevent malicious activity in the first place	-

[74] References with '*' build on the following literature: UN International Law Commission (n 61); Schmitt and Vihul (n 30).
[75] Healey (n 42).
[76] References with '**' build on Daniel Byman, 'Passive Sponsors of Terrorism' (2005) 47 Survival 117.
Byman illustrates this type of relationship describing the US relationship regarding the Irish Republican Army (IRA) Saudi Arabia's approach toward Al Qaeda and Pakistan's approach toward Al Qaeda.
[77] Military and Paramilitary Activities in and against Nicaragua (*Nicaragua v US*) [1986] ICJ Rep 14.
[78] References with '***' are based on *Tadic Case* (Judgment) ICTY-94-1 (26 January 2000).
[79] Brierly (n 55).
[80] Jinks (n 53).
[81] For a discussion and recommendation on how to distinguish and use 'adoption' versus 'endorsement' or 'approval', see: UN International Law Commission (n 61) Art 6.
[82] Brierly (n 55) 48–49.