ARTICLE

Outsourcing of Governmental Functions in Contemporary Conflict: Rethinking the Issue of Attribution

JENNIFER MADDOCKS*

* Major Jennifer Maddocks, British Army, is a PhD candidate at the University of Exeter and at the time this article was written, she was a faculty member at the Stockton Center for the Study of International Law at the U.S. Naval War College. The views expressed are those of the author and do not necessarily represent those of the U.K. Ministry of Defence, the British Army, the U.K. government, the U.S. government, the U.S. Department of the Navy or the U.S. Naval War College.

I. INTRODUCTION

It is common today for private entities to carry out activities that, in years past, were considered governmental in nature. Privatization and outsourcing have increased markedly across all sectors of government, ranging from the railways and prisons to military-related activities in combat zones. The trend is equally apparent in the cyber domain where private actors not only play a significant role in upholding cybersecurity but also engage in hostile operations on states' behalf.[1] This blurring of the boundaries between public and private sector activity has raised questions regarding accountability for the wrongful behavior of the private entities concerned. The abuses committed by contractors working for private military and security companies (PMSC) at Abu Ghraib in Iraq are a case in point.[2] While the individual contractors were personally liable under criminal law for their misconduct, the question of state responsibility remains.

A hiring state's responsibility in such circumstances depends upon two factors: first, whether the private entity's conduct is attributable to the state and second, whether the conduct in question amounts to a breach of the state's international obligations.[3] When both conditions are satisfied, the relevant act or omission amounts to an internationally wrongful act, entailing the international responsibility of the state.[4] The focus of this article is upon the first of these elements: the issue of attribution. The International Law Commission's (ILC) Draft Articles on Responsibility of States for Internationally Wrongful Acts (ARSIWA)[5] set out a number of

---

1. For example, in December 2017, a number of governments publicly attributed the "WannaCry" ransomware attack to Lazarus Group, a hacking entity that works on behalf of the North Korean government. *See* Dustin Volz, *U.S. Blames North Korea for "WannaCry" Cyber Attack*, REUTERS (Dec. 18, 2017), http://www.reuters.com/article/us-usa-cyber-northkorea/u-s-blames-north-korea-for-wannacry-cyber-attack-idUSKBN1ED00Q.

2. *See* Rachel Weiner, *A Suit over Abu Ghraib Getting to "What Actually Happened,"* WASH. POST (Sept. 22, 2017), http://www.washingtonpost.com/local/public-safety/abu-ghraib-contractor-treatment-deplorable-but-not-torture/2017/09/22/4efc16f4-9e3b-11e7-9083-fbfddf6804c2_story.html?utm_term=.b7417c8be7bf (noting that interrogators working for one contractor were "accused of directing beatings, starvation, sexual violations, sleep deprivation and other abuse of prisoners in the detention facility").

3. Int'l L. Comm'n, *Draft Articles on Responsibility of States for Internationally Wrongful Acts, (with commentaries)*, *in* Rep. on the Work of Its Fifty-Third Session, U.N. Doc. A/56/10, at 43 (2001), http://www.un.org/documents/ga/docs/56/a5610.pdf [hereinafter ARSIWA]. Article 2 provides that "[t]here is an internationally wrongful act of a State when conduct consisting of an action or omission: (a) [i]s attributable to the State under international law; and (b) [c]onstitutes a breach of an international obligation of the State." *Id.*

4. *Id.* ("Every internationally wrongful act of a State entails the international responsibility of that State.").

5. *Id.* ARSIWA is not a treaty and therefore is not binding under international law. The International Law Commission drafted ARSIWA during a process that took more than fifty years. Once completed, the U.N. General Assembly commended ARSIWA to governments. *See* G.A. Res.

grounds upon which a private actor's conduct may be attributable to a state.[6] Article 5 ARSIWA, relating to attribution based upon an actor's performance of government functions, provides that:

> The conduct of a person or entity which is not an organ of the State under article 4 but which is empowered by the law of that State to exercise elements of the governmental authority shall be considered an act of the State under international law, provided the person or entity is acting in that capacity in the particular instance.[7]

The commentary to Article 5 clarifies that it is intended to encompass the activities of private entities exercising elements of governmental authority in place of state organs, as well as those of formerly state-owned corporations that retain certain public or regulatory functions following privatization.[8] This basis of attribution is intended to prevent a state from avoiding responsibility by privatizing or outsourcing functions that were traditionally carried out by the state's own organs.[9] Thus, if, for example, a state delegates the management of a detention facility to a private company and that company's employees then commit acts in breach of the state's international human rights law obligations, Article 5 ARSIWA operates to attribute the employees' conduct to the state.

To date, the practical application of the attribution standard encompassed within Article 5 ARSIWA remains unclear. This is largely due to uncertainty as to the types of activity that fall within the sphere of governmental authority, as well as ambiguity regarding the nature of the

---

56/83, at 2 (Jan. 28, 2002). By 2012, international courts, tribunals, and other legal bodies had cited ARSIWA and the accompanying commentary 154 times. *See* U.N. Secretariat, Materials on the Responsibility of States for Internationally Wrongful Acts, U.N. Doc. ST/LEG/SER B/25, at viii (2012), http://legal.un.org/legislativeseries/documents/Book25/Book25.pdf. Further, a number of courts and tribunals have described ARSIWA as reflective of customary international law. *See, e.g.*, Noble Ventures, Inc. v. Romania, No. ARB/01/11, Award, Int'l Ctr. for Settlement of Inv. Disputes [ICSID], ¶ 69 (Oct. 12, 2005), http://www.italaw.com/sites/default/files/case-documents/ita0565.pdf ("While those Draft Articles are not binding, they are widely regarded as a codification of customary international law.").

6. *See infra* Part II.B.

7. ARSIWA, *supra* note 3, at 44. Conduct falling within the scope of Article 5 is distinct from that carried out by entities amounting to organs of state, such as government ministries or agencies. Organs of state are addressed in ARSIWA. *See id.*

8. *Id.* at 92.

9. *Id.* at 83 ("But international law does not permit a State to escape its international responsibilities by a mere process of internal subdivision."). *See also Summary Records of the 2553rd Meeting*, [1998] 1 Y.B. Int'l L. Comm'n 228, ¶ 1, U.N. Doc. A/CN.4/SER.A/1998, http://legal.un.org/ilc/publications/yearbooks/english/ilc_1998_v1.pdf (statement of Special Rapporteur James Crawford).

> Generally speaking, the main concern of Governments was to ensure that attribution could be made on a sufficiently broad basis to prevent a State from escaping its responsibility by means of formal definitions of its organs or agents and to prevent the recent tendency for privatization of the public sector from leading to any reduction of the scope of the rules of attribution.

delegation that is required for an entity to be "empowered by the law" of the state. This article seeks to address such issues, focusing principally on security-related activities carried out by private entities operating either in zones of conflict, or in the cyber domain. Both are areas in which government outsourcing has increased in recent years.

This article first assesses the relevance of Article 5 ARSIWA in contemporary conflict. It considers the outsourcing of public functions to PMSCs and cyber operators, as well as the general features of the attribution standard. It then explores in detail the three criteria upon which attribution under Article 5 is based: delegation of governmental authority, empowerment by the internal law of the state, and action pursuant to a governmental mandate. The article seeks to develop an analytical framework within which to assess the scope of the attribution standard, concluding that it may, in practice, provide a broader basis of attribution than that indicated by the strict wording of Article 5.

II. ARTICLE 5 AND CONTEMPORARY CONFLICT

A. Outsourcing in the Contemporary Security Environment

Since the early 1990s, states' reliance on contractors during combat operations has increased significantly.[10] The United States and United Kingdom have been at the forefront of this development, with PMSCs involved in every major U.S. military operation since the 1991 Gulf War.[11] There are a number of reasons for this change. These include the reduction in the size of states' military forces following the end of the Cold War; the protracted nature of the deployments to Bosnia, Iraq, and Afghanistan; and the lack of the requisite skills among military personnel to operate sophisticated equipment.[12] In 2009, for example, U.S. Central Command contracted the services of over 20,000 civilians in support of combat

10. *See, e.g.*, MATTHEW UTTLEY, HERITAGE FOUND., PRIVATE CONTRACTORS ON DEPLOYED MILITARY OPERATIONS: INTER-AGENCY OPPORTUNITIES AND CHALLENGES 2 (2006), http://www.heritage.org/defense/report/private-contractors-deployed-military-operations-inter-agency-opportunities-and (noting that the ratio of civilian contractors to total deployed military personnel increased from 1 in 60 in Iraq in 1991 to 1 in 10 in Bosnia, 1 in 2 in Kosovo, and 1.5 to 1 in Iraq in 2006); Rod Nordland, *Risks of Afghan War Shift from Soldiers to Contractors*, N.Y. TIMES (Feb. 11, 2012), http://www.nytimes.com/2012/02/12/world/asia/afghan-war-risks-are-shifting-to-contractors.html (noting that more civilian contractors working for U.S. companies lost their lives in Afghanistan in 2011 than American soldiers).

11. U.S. GOV'T ACCOUNTABILITY OFF., GAO-03-695, MILITARY OPERATIONS: CONTRACTORS PROVIDE VITAL SERVICES TO DEPLOYED FORCES BUT ARE NOT ADEQUATELY ADDRESSED IN DOD PLANS 1 (2003).

12. *Id.*; *see also* UTTLEY, *supra* note 10, at 2.

operations in Iraq and Afghanistan,[13] while in 2010, expenditure on contractor support amounted to an estimated sixty per cent of the U.K.'s overseas operational defense spending.[14] In light of such figures, it is necessary to determine the circumstances in which contractors' conduct is potentially attributable to the hiring state.

The issue of attribution turns, in part, upon the nature of the activities undertaken by the PMSC.[15] During armed conflict states have entrusted contractors with a wide variety of responsibilities, ranging from support functions to offensive combat.[16] These may be loosely divided into four categories.[17] First, contractors frequently provide services in support of personnel working in deployed locations. In the relatively stable environment of the Balkans, for instance, contractors provided a range of base operations support services, including food and waste management and recreational services.[18]

Second, contractors commonly provide equipment and logistical support services, such as maintaining and servicing weapons systems, vehicles, and other essential items, or controlling ammunition. These functions are prevalent both in conflict zones and in more benign environments. In 2017, for example, about a third of the civilians contracted to support U.S. operations in Iraq and Afghanistan carried out logistics and maintenance tasks, while the remainder were involved in activities such as construction and base support.[19]

The third category of service undertaken by PMSCs is the provision of security. Particularly in more volatile environments, contractors often engage in security tasks that previously fell within the exclusive purview of the armed forces. Such functions include the physical protection of individuals and convoys traveling through unsecured areas, as well as the protection of fixed assets such as military facilities or government buildings.[20]

---

13. *See* U.S. DEP'T OF DEF., CONTRACTOR SUPPORT OF U.S. OPERATIONS IN THE USCENTCOM AOR, IRAQ, AND AFGHANISTAN (2009), http://psm.du.edu/media/documents/reports_and_stats/us_data/dod_quarterly_census/dod_quarterly_census_nov_2009.pdf.

14. HENRIK HEIDENKAMP, ROYAL UNITED SERVS. INST., SUSTAINING THE UK'S DEFENCE EFFORT: CONTRACTOR SUPPORT TO OPERATIONS MARKET DYNAMICS 2 (2012), http://rusi.org/sites/default/files/201504_whr_contractor_support_to_operations_0.pdf.

15. *See infra* Part III.

16. *See, e.g.*, IAN RALBY & HANNAH TONKIN, CHATHAM HOUSE, REGULATION OF PRIVATE MILITARY SECURITY COMPANIES IN ARMED CONFLICT (2011), http://www.chathamhouse.org/sites/files/chathamhouse/public/Research/International%20Law/071011ralby%26tonkin.pdf.

17. *See* HEIDENKAMP, *supra* note 14, at 4.

18. U.S. GOV'T ACCOUNTABILITY OFF., *supra* note 11, at 7.

19. U.S. DEP'T OF DEF., CONTRACTOR SUPPORT OF U.S. OPERATIONS IN THE USCENTCOM AREA OF RESPONSIBILITY 2 (2017), http://www.acq.osd.mil/log/PS/.CENTCOM_reports.html/5A_July2017_Final.pdf.

20. RALBY & TONKIN, *supra* note 16, at 4.

Finally, the fourth category of function performed by PMSCs encompasses roles with a direct operational effect. The clearest example is contractors' involvement in offensive combat, as occurred in Angola and Sierra Leone in the 1990s.[21] Although PMSCs no longer openly offer such services, news reports reveal contractors' recent involvement in the hostilities in Syria and Yemen, as well as in intelligence-led drone operations and raids against individuals suspected of insurgent activity in Iraq and Afghanistan.[22] In addition, the United States engages contractors to undertake operational roles such as interrogation, operation of military equipment, and intelligence analysis.[23]

The character of the functions performed by PMSCs is crucial when assessing whether they amount to an exercise of governmental authority within the meaning of Article 5 ARSIWA. This is not a straightforward determination.[24] The same considerations apply when examining the activities of private actors operating in the cyber domain. But from a factual and evidential perspective, the issue of attribution in the latter context is yet more complex. For a start, there is the difficulty of technical attribution, tracing the cyber activity back to its source.[25] Moreover, even if a state or

---

21. *Id.* at 3 (noting that Executive Outcomes and Sandline International "provided offensive combat services to the governments of Angola and Sierra Leone . . . [that] were crucial in quelling hostilities and compelling the rebels in each country to negotiate settlements").

22. *See, e.g.*, Metin Gurcan, *Private Military Companies: Moscow's Other Army in Syria*, AL-MONITOR (Dec. 1, 2017), http://www.orient-news.net/en/news_show/142945/0/Private-military-companies-Moscows-other-army-in-Syria; Emily B. Hager & Mark Mazzetti, *Emirates Secretly Sends Colombian Mercenaries to Yemen Fight*, N.Y. TIMES (Nov. 25, 2015), http://www.nytimes.com/2015/11/26/world/middleeast/emirates-secretly-sends-colombian-mercenaries-to-fight-in-yemen.html; Mark Mazzetti, *C.I.A. Sought Blackwater's Help to Kill Jihadists*, N.Y. TIMES (Aug. 19, 2009), http://www.nytimes.com/2009/08/20/us/20intel.html; James Risen & Mark Mazzetti, *Blackwater Guards Tied to Secret C.I.A. Raids*, N.Y. TIMES (Dec. 10, 2009), http://www.nytimes.com/2009/12/11/us/politics/11blackwater.html; James Risen & Mark Mazzetti, *C.I.A. Said to Use Outsiders to Put Bombs on Drones*, N.Y. TIMES (Aug. 20, 2009), http://www.nytimes.com/2009/08/21/us/21intel.html; Maria Tsvetkova & Anton Zverev, *Ghost Soldiers: The Russians Secretly Dying for the Kremlin in Syria*, REUTERS (Nov. 3, 2016), http://www.reuters.com/article/us-mideast-crisis-syria-russia-insight/ghost-soldiers-the-russians-secretly-dying-for-the-kremlin-in-syria-idUSKBN12Y0M6.html.

23. HEIDENKAMP, *supra* note 14, at 4; Mazzetti, *supra* note 22; Risen & Mazzetti, *Blackwater Guards Tied to Secret C.I.A. Raids*, *supra* note 22; Risen & Mazzetti, *C.I.A. Said to Use Outsiders to Put Bombs on Drones*, *supra* note 22. For further discussion regarding the involvement of U.S. contractors in intelligence collection and analysis, see Simon Chesterman, *"We Can't Spy…If We Can't Buy!": The Privatization of Intelligence and the Limits of Outsourcing "Inherently Governmental Functions,"* 19 EUR. J. INT'L L. 1055 (2008).

24. *See infra* Part III.

25. Technical or factual attribution relates to the degree of certainty that may be reached as to the identity of the person or persons responsible for a particular cyber operation. *See, e.g.*, OFF. OF THE GEN. COUNSEL, U.S. DEP'T OF DEF., LAW OF WAR MANUAL § 16.3.3.4 (rev. ed. 2016) ("Attribution may pose a difficult factual question in responding to hostile or malicious cyber operations because adversaries may be able to hide or disguise their activities or identities in cyberspace more easily than in the case of other types of operations."); Jeremy Wright QC, MP, Attorney General for Eng. & Wales, Speech on Cyber and International Law in the 21st Century, (May 23, 2018) http://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century ("There

cybersecurity company can name the actor it considers responsible for a particular cyber operation, concerns about revealing sources and methods frequently preclude a clear articulation of the evidence or intelligence upon which this assessment is based.[26] For an injured party, therefore, it is particularly problematic to prove that relevant cyber activity is attributable to a state.

Acting through cyberspace appeals to malicious actors for exactly these reasons. They are frequently able to take advantage of the ambiguities in cyberspace to conceal their involvement in an incident. Cyber operations are particularly attractive to less developed nations as a relatively inexpensive tool against an enemy with traditional battlefield superiority. North Korea, for instance, reportedly grooms cyber specialists as a cost-effective means to counter adversaries such as South Korea and the United States, with which it cannot compete militarily.[27] But powerful nations cultivate cyber expertise too. China's People's Liberation Army reportedly funds "a vast complex of part-time cyber-devotees to supplement and complement the official structure of cyber interception and invasion."[28] In contrast with the

---

are obviously practical difficulties involved in making any attributions of responsibilities when the action concerned is capable of crossing traditional territorial boundaries and sophisticated techniques are used to hide the identity and source of the operation. Those difficulties are compounded by the ready accessibility of cyber technologies and the resultant blurring of lines between the actions of governments and those of individuals."). Factual attribution is subject to a reasonableness standard. *See* TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS, 81-82 (Michael N. Schmitt ed. 2017) [hereinafter TALLINN MANUAL 2.0].

26. States will often wish to keep the extent of their cyber capabilities secret and therefore will not wish to reveal the sources and methods they used to determine the identity of the person or group responsible for a cyber operation. For a general discussion regarding the problems associated with technical or factual attribution, see TIM MAURER, CYBER MERCENARIES: THE STATE, HACKERS, AND POWER, 22-25 (2018).

27. *See, e.g.*, Sangwon Yoon, *North Korea Recruits Hackers at School*, AL JAZEERA (June 20, 2011), http://www.aljazeera.com/indepth/features/2011/06/201162081543573839.html; Oh Seok-min, *N. Korea Boosts Cyber Operations Capabilities*, YONHAP NEWS AGENCY (May 10, 2015), http://english.yonhapnews.co.kr/news/2015/05/08/97/0200000000AEN20150508006900315F.html ("A total of 6,800 hackers – some 1,700 experts and 5,100 supportive members – have been assigned to hacking and other cyber provocations . . . ."); Timothy W. Martin, *How North Korea's Hackers Became Dangerously Good*, WALL ST. J. (Apr. 19, 2018), http://www.wsj.com/articles/how-north-koreas-hackers-became-dangerously-good-1524150416; Jenny Jun, Scott LaFoy & Ethan Sohn, *North Korea's Cyber Operations: Strategy and Responses*, CENTER FOR STRATEGIC AND INT'L STUDIES 24-51 (Dec. 2015), http://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/151216_Cha_NorthKoreasCyberOperations_Web.pdf; DEF. COMMITTEE, RASH OR RATIONAL? NORTH KOREA AND THE THREAT IT POSES, 2017-19, HC 327, at 18-24 (UK), http://publications.parliament.uk/pa/cm201719/cmselect/cmdfence/327/327.pdf. North Korea also seeks other benefits from its cyber operations, such as hacking into cryptocurrency exchanges to obtain funds to offset the effects of sanctions. *See, e.g.*, David E. Sanger, David D. Kirkpatrick & Nicole Perlroth, *The World Once Laughed at North Korean Cyberpower. No More*, N.Y. TIMES (Oct. 15, 2017), http://www.nytimes.com/2017/10/15/world/asia/north-korea-hacking-cyber-sony.html.

28. George H. Wittman, *China's Cyber Militia*, AM. SPECTATOR (Oct. 21, 2011), http://spectator.org/36718_chinas-cyber-militia/. The article refers to an official Chinese People's Liberation Army publication, according to which there are thousands of such units around the country. *See also* MAURER, *supra* note 26, at 107-19, discussing the evolving relationship between the Chinese

well-defined contractual arrangements that are common when states outsource functions to PMSCs, state relationships with such individuals frequently are informal and ill-understood. Meanwhile, in the words of the Director of the U.S. Federal Bureau of Investigation, "We're seeing an increase in nation-state sponsored computer intrusions. And we're also seeing a 'blended threat' – nation-states using criminal hackers to carry out their dirty work."[29]

The outsourcing of cyber activity to non-state actors also appeals to states wishing to defend their networks against cyberattack. Hiring private cybersecurity experts allows states to fill capability gaps, offering a prompt means of response to cyber incidents, often at minimal cost.[30] Such services appeal not only to developing nations lacking the capability to deal with cyber threats,[31] but also to sophisticated states with considerable cyber expertise. The United States, for example, relies significantly on the private sector to secure computer networks and critical infrastructure from hostile cyber intrusions.[32] Given the public character of such activities, the question arises as to whether private conduct of this nature is attributable to the state.[33]

---

state and its cyber proxies; BRYAN KREKEL, U.S.-CHINA ECON. & SEC. REVIEW COMM'N, CAPABILITY OF THE PEOPLE'S REPUBLIC OF CHINA TO CONDUCT CYBER WARFARE AND COMPUTER NETWORK EXPLOITATION 33-50 (2009), http://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-030.pdf; MIKK RAUD, NATO COOP. CYBER DEF. CTR. OF EXCELLENCE, CHINA AND CYBER: ATTITUDES, STRATEGIES, ORGANISATION 26-27 (2016), http://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_CHINA_092016_FINAL.pdf; FIREEYE, INC., RED LINE DRAWN: CHINA RECALCULATES ITS USE OF CYBER ESPIONAGE 15 (2016), http://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-china-espionage.pdf.

29. Matthew Kahn, *FBI Director Christopher Wray's Remarks on Encryption to the International Conference on Cyber Security*, LAWFARE (Jan. 9 2018), http://www.lawfareblog.com/fbi-director-christopher-wrays-remarks-encryption-international-conference-cyber-security.

30. Very few states have the requisite cyber expertise to respond promptly and adequately to threats. Private cybersecurity experts offer a means by which states can augment their cyber capabilities on a flexible basis, more quickly and often at a lower cost than if they were to build their own cyber capability in-house. *See* MAURER, *supra* note 26, at 38-39.

31. *See, e.g.*, Sheera Frenkel, *Hackers Find "Ideal Testing Ground" for Attacks: Developing Countries*, N.Y. TIMES (July 2, 2017), http://www.nytimes.com/2017/07/02/technology/hackers-find-ideal-testing-ground-for-attacks-developing-countries. html.

32. *See, e.g.*, President Barack Obama, Remarks by the President at the Cybersecurity and Consumer Protection Summit (Feb. 13, 2015), http://obamawhitehouse.archives.gov/the-press-office/2015/02/13/remarks-president-cybersecurity-and-consumer-protection-summit.

> So much of our computer networks and critical infrastructure are in the private sector, which means government cannot do this alone. But the fact is that the private sector can't do it alone either, because it's government that often has the latest information on new threats. There's only one way to defend America from these cyber threats, and that is through government and industry working together, sharing appropriate information as true partners.

See also Kristen E. Eichensehr, *Public-Private Cybersecurity*, 95 TEX. L. REV. 467, 501 (2017).

33. *See infra* Part III.

To further complicate the issue of cyber accountability, states do not universally accept that the laws of state responsibility apply to cyber operations.[34] The most recent meeting of the United Nations Group of Governmental Experts[35] foundered after failing to reach consensus on the application of basic principles of international law in this context.[36] Nonetheless, the majority of states, as well as the International Group of Experts involved in drafting the Tallinn Manual 2.0, consider the rules articulated in ARSIWA to apply with equal force in the cyber domain.[37] This article therefore proceeds on the basis that Article 5 ARSIWA applies to determine the issue of attribution, irrespective of the domain in which the non-state actor operates.

B. Attribution Pursuant to Article 5

ARSIWA sets out a number of grounds upon which a private entity's activities may be attributable to a state for the purpose of determining that state's international responsibility. These include Article 5 as well as Article 4, relating to entities that *de facto* amount to an organ of state, and Article 8, relating to private conduct performed on the state's instructions or under its direction or control. More than one attribution standard may potentially apply to any given conduct and it may not initially be clear which is most

34. *See, e.g.*, Michael Schmitt & Liis Vihul, *International Cyber Law Politicized: The UN GGE's Failure to Advance Cyber Norms*, JUST SEC. (June 30, 2017), http://www.justsecurity.org/42768/international-cyber-law-politicized-gges-failure-advance-cyber-norms/.

35. The U.N. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (GGE) first met in 2004. Initially experts from fifteen countries made up the GGE, increasing to twenty-five countries by 2016. The five permanent U.N. Security Council member states have been involved in the GGE from the outset. *See id.*

36. *Id.* At issue were the right to respond to internationally wrongful acts, the right to self-defense, and the application of international humanitarian law in the cyber domain. The rules of attribution in the law of state responsibility were not addressed specifically.

37. TALLINN MANUAL 2.0, *supra* note 25, rs. 14-30, at 79-153. The TALLINN MANUAL 2.0 was published in 2017 following completion of a four-year project, involving a group of nineteen renowned international law experts, aimed at clarifying the international law applicable to cyber operations. Delegations from over fifty states were given the opportunity to comment on TALLINN MANUAL 2.0 prior to its publication in what was known as The Hague Process. *See also* Brian Egan, Speech on International Law and Stability in Cyberspace (Nov. 10, 2016), http://www.justsecurity.org/wp-content/uploads/2016/11/Brian-J.-Egan-International-Law-and-Stability-in-Cyberspace-Berkeley-Nov-2016.pdf ("There are three pillars to the U.S. strategic framework . . . . The first is global affirmation of the applicability of existing international law to State activity in cyberspace in both peacetime and during armed conflict."); Wright, *supra* note 25 ("It is the UK's view that when states and individuals engage in hostile cyber operations, they are governed by law just like activities in any other domain."); Stef Blok, Neth. Minister of Foreign Affairs, Speech by Minister Blok on the Occasion of the First Anniversary Tallinn Manual 2.0 (June 20, 2018), http://www.government.nl/documents/speeches/2018/06/20/speech-by-minister-blok-on-first-anniversary-tallinn-manual-2.0 ("We [the Netherlands] take the position that there's no need to develop a new system of international law for [cyberspace]. On the contrary, making clear that existing laws apply equally in cyberspace is our best guarantee of a future with an open, free and stable internet.").

appropriate. Before examining the scope of Article 5 ARSIWA, therefore, it is first necessary to differentiate it from the other attribution standards.

The wording of Article 5 ARSIWA makes clear that it does not encompass the activities of state organs.[38] These comprise all government entities that make up the organization of the state, including the military, intelligence, and other state agencies.[39] When assessing potential attribution, a first consideration is thus whether the entity concerned is a state organ under the terms of the state's domestic law. If the entity is a *de jure* state organ, then, in accordance with Article 4 ARSIWA, the state is responsible for its conduct when acting in its public capacity.[40] A clear example is the conduct of soldiers within a state's armed forces, or the official actions of civil servants or police officers.

Article 4 applies equally to the conduct of *de facto* state organs. This term refers to those entities that are not organs of state under domestic law, but are nonetheless analogous to state organs in terms of their complete dependence on the state and lack of autonomy.[41] Accordingly, if a private entity exercising governmental functions relies entirely upon the state in order to perform those functions and is subject to complete state control, its conduct may be attributable to the state on the basis of Article 4 rather than Article 5 ARSIWA. Consider, for example, the position of a police force that is not characterized by domestic law as a state organ. Provided that a relationship of complete dependence and control nevertheless exists between the force and the state, the police officers' actions are likely attributable to the state as a *de facto* state organ.[42]

Control is also a relevant factor when considering attribution under Article 8 ARSIWA. This attribution standard applies when a private entity

---

38. ARSIWA, *supra* note 3, art. 5.

39. *Id.* art. 4 commentary, ¶ 1.

40. *Id.* art. 4. Article 4 addresses the conduct of organs of a state, providing:

> 1. The conduct of any State organ shall be considered an act of that State under international law, whether the organ exercises legislative, executive, judicial or any other functions, whatever position it holds in the organization of the State, and whatever its character as an organ of the central Government or of a territorial unit of the State.
>
> 2. An organ includes any person or entity which has that status in accordance with the internal law of the State.

See also id. art. 7. Article 7 addresses *ultra vires* conduct of state organs, providing, "The conduct of an organ of State . . . shall be considered an act of the State under international law if the organ . . . acts in that capacity, even if it exceeds its authority or contravenes instructions."

41. Application of Convention on Prevention and Punishment of Crime of Genocide (Bosn. & Herz. v. Serb. & Montenegro), Judgment, 2007 I.C.J. 43, ¶¶ 392-93 (Feb. 26).

42. ARSIWA, *supra* note 3, art. 4 commentary, ¶ 11.

> In [some legal systems] the police have a special status, independent of the executive; this cannot mean that for international law purposes they are not organs of the State. Accordingly, a state cannot avoid responsibility for the conduct of a body which does in truth act as one of its organs merely by denying it that status under its own law.

acts on the state's instructions, or under its direction or control.[43] In order to prove attribution on this basis, there must be evidence that the state instructed the private entity to carry out a particular act, or that it exercised "effective control" over the operation during which the act was committed.[44] This is a high evidentiary threshold, requiring evidence that the state "directed or enforced" the relevant violation of international law.[45] To date, no court or tribunal has found evidence of "effective control" sufficient to trigger state responsibility. Nevertheless, the standard could conceivably be met if a hiring state were to exercise significant control over an individual PMSC operation, including planning the operation, specifying the training requirements for the personnel involved, identifying the weapons and equipment to be used, and supervising the contractors' performance on the ground.[46]

In contrast with the requirements of Article 8 ARSIWA, the presence or absence of state control over an entity's activities is irrelevant to the determination of attribution pursuant to Article 5.[47] The ARSIWA commentary makes clear that, under Article 5, "an entity is covered even if its exercise of authority involves an independent discretion or power to act; there is no need to show that the conduct was in fact carried out under the control of the State."[48] Thus, attribution may arise under Article 5 whether the state exercises a high degree of control, partial control, or no control whatsoever over an entity's conduct. This means that, provided the requirements of Article 5 are met, a PMSC's conduct could be attributable to a state even if that state exerts no authority or influence over the way in which the relevant operation is performed. From an evidential perspective, therefore, attribution on the basis of Article 5 ARSIWA may be easier to prove than that based upon Article 8.

ARSIWA sets out two further grounds on which a private entity's conduct may be attributable to the state, in addition to those envisaged in Articles 4, 5 and 8. Article 9 relates to the exceptional situation in which a private entity "exercises elements of governmental authority in the absence or default of the official authorities," such as may occur in times of

43. *Id.* art. 8 ("The conduct of a person or group of persons shall be considered an act of a State under international law if the person or group of persons is in fact acting on the instructions of, or under the direction or control of, that State in carrying out the conduct").

44. The International Court of Justice formulated the "effective control" standard in the case concerning Military and Paramilitary Activities in and Against Nicaragua. Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, ¶ 115 (June 27).

45. *Id.*

46. *See* HANNAH TONKIN, STATE CONTROL OVER PRIVATE MILITARY AND SECURITY COMPANIES IN ARMED CONFLICT 120 (2011).

47. ARSIWA, *supra* note 3, art. 5 commentary, ¶ 7.

48. *Id.*

revolution or conflict.[49] For instance, if a group of private citizens work together to secure their local area following the withdrawal of state police forces due to conflict, their actions may be attributable to the state.[50]

Alternatively, attribution may arise after the fact under the terms of Article 11 ARSIWA.[51] This attribution standard applies if a state "acknowledges and adopts" the acts of a private entity following their commission.[52] Article 11 requires more than mere toleration or endorsement of the entity's activities; rather, it applies if the state espouses the conduct as its own.[53] For example, demonstrators' seizure of the U.S. Embassy in Tehran in 1979 was attributable to Iran due to the Iranian state's subsequent and deliberate maintenance of the occupation as a means of coercing the United States.[54]

The distinction between the various grounds for attributing a private entity's activities to the state is not always clear. For example, in the *Nicaragua* case, the majority of the International Court of Justice seemed to conclude that the actions of a group of non-state actors should be attributed to the state on the basis of state instructions.[55] In contrast, former ILC Special Rapporteur Judge Ago concluded in his separate opinion that the appropriate basis of attribution was the group's empowerment by the United States to exercise elements of governmental authority.[56] Other

---

49. *Id.* art. 9 ("The conduct of a person or group of persons shall be considered an act of a State under international law if the person or group of persons is in fact exercising elements of the governmental authority in the absence or default of the official authorities and in circumstances such as to call for the exercise of those elements of authority.").

50. The Iran-United States Claims Tribunal attributed the conduct of non-state actors to Iran on the basis of the attribution standard reflected in Article 9 ARSIWA in the Yeager case. *See* Yeager v. Iran, 17 Iran-U.S. Cl. Trib. Rep. 92, ¶ 43 (1987). The Tribunal concluded that in the context of the 1979 Islamic Revolution, the revolutionary "Komitehs" or "Guards" "were acting in fact on behalf of the new government, or at least exercised elements of governmental authority in the absence of official authorities, in operations of which the new Government must have had knowledge and to which it did not specifically object." *Id.*

51. ARSIWA, *supra* note 3, art. 11 ("Conduct which is not attributable to a State under the preceding articles shall nevertheless be considered an act of that State under international law if and to the extent that the State acknowledges and adopts the conduct in question as its own.").

52. *Id.*

53. *Id.* art. 11 commentary, ¶ 6.

54. United States Diplomatic and Consular Staff in Tehran (U.S. v. Iran), Judgment, 1980 I.C.J. 3, ¶¶ 58, 73, 74, 87 (May 24).

55. Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. Rep. 14, ¶¶ 75, 85 (June 27). The private individuals concerned are referred to in the judgment as Unilaterally Controlled Latino Assets, or UCLAs. In concluding that the UCLAs' actions should be attributed to the United States, the ICJ majority referred to the fact that the UCLAs were "paid by, and acting on the direct instructions of, United States military or intelligence personnel." This suggests that the UCLAs' conduct was attributable to the United States on the basis of the attribution standard now reflected in Article 8 ARSIWA. The ICJ majority further concluded that "agents of the United States participated in the planning, direction, support and execution of the operations" conducted by the UCLAs. *Id.*

56. Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. Rep. 14, 181, ¶15 (June 27) (separate opinion by Ago, J.). Judge Ago's choice of wording indicates

courts and commentators, meanwhile, consider that these non-state actors were *de facto* state organs,[57] or fell within the notion of "effective control."[58] Differences such as this arise, in part, due to a lack of clarity regarding the scope of the various attribution standards.

The ARSIWA commentary sets out the most authoritative guidance as to the parameters of each basis of attribution. In relation to Article 5, the commentary makes clear that acts committed by any type of entity may be attributable to the state.[59] Provided they are not classified as organs of state under domestic law, their legal status is irrelevant. The entities to which the article applies may be totally or partially state-owned or state-funded, or they may be entirely private in nature, such as private companies specializing in cybersecurity or operating as PMSCs.[60] They may equally be private individuals or groups, such as individual contractors, loosely associated groups of hackers, or criminal organizations engaged in cyber-crime.[61]

While the character of the private entity is unimportant, the commentary to Article 5 sets out three conditions that must be satisfied in order for attribution to arise.[62] First, the private actor's conduct must amount to an exercise of governmental authority. Second, the private actor must be empowered by the domestic law of the state to exercise such authority. And third, the private actor must in fact be acting in the exercise of governmental authority, as opposed to in a purely private capacity, at the relevant time.[63] These three factors alone determine the potential attribution

---

that in his view, the UCLAs' conduct was attributable to the United States on the basis of the attribution standard now reflected in Article 5 ARSIWA.

57. Prosecutor v. Tadić, Case No. IT-94-1-A, Appeals Chamber Judgment, ¶ 114 (Int'l Crim. Trib. for the Former Yugoslavia July 15, 1999). In the Appeals Chamber's view, the UCLAs fell into the category of "private individuals acting as *de facto* State organs," suggesting that their conduct was attributable to the United States on the basis of the attribution standard now reflected in Article 4 ARSIWA. *See also* Antonio Cassese, *The Nicaragua and Tadić Tests Revisited in Light of the ICJ Judgment on Genocide in Bosnia,* 18 EUR. J. INT'L L. 649, 652 (2007).

58. LINDSEY CAMERON & VINCENT CHETAIL, PRIVATIZING WAR 213 (2013). The notion of "effective control" is relevant to the attribution standard reflected in Article 8 ARSIWA.

59. ARSIWA, *supra* note 3, art. 5 commentary, ¶¶ 2-3.

> The generic term "entity" reflects the wide variety of bodies which, though not organs, may be empowered by the law of a State to exercise elements of governmental authority. They may include public corporations, semi-public entities, public agencies of various kinds and even, in special cases, private companies . . . . The fact that an entity can be classified as public or private according to the criteria of a given legal system, the existence of a greater or lesser State participation in its capital, or, more generally, in the ownership of its assets . . . these are not decisive criteria for the purpose of attribution of the entity's conduct to the State.

60. *Id.*

61. Although private individuals and groups are not specifically referred to within the commentary to Article 5 ARSIWA, there is nothing within the commentary to indicate that they should be excluded from the Article's scope.

62. ARSIWA, *supra* note 3, art. 5 commentary, ¶ 2.

63. *Id.*

of private conduct to the state pursuant to Article 5, but their practical meanings remain unclear.[64]

ARSIWA does not define "governmental authority" and the guidance within the commentary is of limited assistance in this respect.[65] To exacerbate the issue, as one Tribunal considering the scope of Article 5 noted, "There is no common understanding in international law of what constitutes a governmental or public act."[66] The meaning of "empowerment by the law" is equally ambiguous. And determining when a private individual is acting in his or her public capacity is not always straightforward. It is therefore difficult in practice to determine the circumstances in which the conduct of a private entity may be attributable to the state in accordance with Article 5. Parts III, IV and V of this article address the three criteria in turn and, in each case, seek to add some granularity as to their practical meanings.

III. ELEMENTS OF GOVERNMENTAL AUTHORITY

When assessing whether the actions of a private entity are potentially attributable to the state in the circumstances envisaged by Article 5 ARSIWA, a first consideration is whether the functions performed amount to an exercise of governmental authority. This notion is described in the commentary to Article 5 as encompassing "functions of a public character

---

64. When providing comments to the International Law Commission in relation to the draft wording of Article 5, a number of states raised concerns regarding the ambiguity surrounding the concepts of "governmental authority" and "empowered by the law." *See* Comments and Observations Received from Governments, U.N. Doc. A/CN.4/515 and Add.1-3, 48-49 (Mar. 19, Apr. 3, May 1, June 28, 2001), http://legal.un.org/ilc/documentation/english/a_cn4_515.pdf; *see also* James Crawford (Special Rapporteur), *First Rep. on State Responsibility*, [1998] 2 Y.B. Int'l L. Comm'n, 38, ¶ 185, U.N. Doc. A/CN.4/SER.A/1998/Add.1 (Part 1), http://legal.un.org/ilc/documentation/english/a_cn4_490.pdf [hereinafter *First Rep. on State Responsibility*].

65. The International Law Commission did not intend to define the scope of governmental authority. *See First Rep. on State Responsibility*, *supra* note 64, at 39, ¶ 190.

> It is another thing to identify precisely the scope of 'governmental authority' for this purpose, and it is very doubtful whether article 7 [the predecessor to article 5] itself should attempt to do so . . . . It will be a matter for the claimant to demonstrate that the injury does relate to the exercise of such powers . . . .

See also Summary Records of the 2553rd Meeting, supra note 9, at 229, ¶ 6.

> The comments of Governments revealed no opposition to the rule of attribution stated in the paragraph, but one government had requested the Commission to define the notion of public power. The Commission could of course clarify the notion by means of examples and commentary, but it should not try to define it. Public power was not defined only in terms of content but also in terms of its treatment in internal law. Furthermore, it was not for international law to prescribe a priori what conduct should be regarded as public.

66. Noble Ventures, Inc. v. Romania, ICSID No. ARB/01/11, Award, ¶ 82 (Oct. 12, 2005); *See also First Rep. on State Responsibility*, *supra* note 64, at 33-34 ("[I]nternational law does not determine the particular structures of government within States. Many activities carried out by Governments could be entrusted to the private sector, and the line between public and private varies continually over time within and between different countries.").

normally exercised by State organs."[67] The emphasis is therefore upon those functions performed in the public interest that are conventionally carried out by government bodies or agencies, as opposed to private entities.

It is, however, far from easy to identify the precise activities that a state traditionally performs. In the words of the ARSIWA commentary, "Beyond a certain limit, what is regarded as 'governmental' depends on the particular society, its history and traditions."[68] Such ambiguity engenders uncertainty as to the scope of Article 5 and potentially leads to a lack of parity between states. As Special Rapporteur Ago noted, "If the same public function were performed in one State by organs of the State proper and in another by para-State institutions, it would indeed be absurd if the international responsibility of the State were engaged in one case and not in the other."[69] For example, it would make little sense to attribute armed security activities to one state on the basis that the activity is performed by military personnel, but not to another where the function is commonly outsourced.[70]

Further difficulties arise due to the prevalence of outsourcing in recent years. As public functions are increasingly privatized or outsourced, activities that were historically performed by the state may cease to serve as relevant indicators of what is truly "governmental" in nature.[71] If states continue to outsource functions to private entities, the range of activities that are considered governmental may steadily diminish, leading to further ambiguity regarding the scope of Article 5 and a reduction in states' responsibility.[72]

A better approach is to identify factors that apply to all states, irrespective of their individual outsourcing practices, and apply them to an evaluation of the functions that states empower non-state actors to

---

67. ARSIWA, *supra* note 3, art. 5 commentary, ¶ 2. An earlier version of the commentary provided for attribution when "entities are empowered, if only exceptionally and to a limited extent, to exercise specific functions which are akin to those normally exercised by the organs of the State." *See Draft Articles on State Responsibility with Commentaries Thereto Adopted by the International Law Commission on First Reading*, 31, art. 7 commentary, ¶ 18 (Jan. 1997), http://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_1996.pdf.

68. ARSIWA, *supra* note 3, art. 5 commentary, ¶ 6.

69. *Summary Records of the 1251st Meeting*, [1974] 1 Y.B. Int'l L. Comm'n 5, 8, ¶ 17, U.N. Doc. A/CN.4/SER.A/1974, http://legal.un.org/ilc/publications/yearbooks/english/ilc_1974_v1.pdf.

70. *But see* Comments and Observations Received from Governments, *supra* note 64, at 49. Here, the United Kingdom queried the status of a body established by a state to regulate a particular activity, such as administering a national lottery, that may not exist in other states.

71. *See* JAMES CRAWFORD, STATE RESPONSIBILITY: THE GENERAL PART 129 (2013); TONKIN, *supra* note 46, at 101. For example, in 1971, U.N. Special Rapporteur Robert Ago included "public transport" and "postal communications" within the examples he gave of private persons entrusted by the state with the performance of public tasks. Such tasks, today, are unlikely to be considered governmental in nature. *See* Roberto Ago (Special Rapporteur, the Internationally Wrongful Act of the State, Source of International Responsibility), *Third Rep. on State Responsibility*, 263, ¶ 190, U.N. Doc. A/CN.4/246 and Add.1-3 (1971), http://legal.un.org/ilc/documentation/english/a_cn4_246.pdf [hereinafter *Third Rep. on State Responsibility*].

72. Christine Chinkin, *A Critique of the Public/Private Dimension,* 10 EUR. J. INT'L L. 387, 390 (1999).

perform. This provides greater certainty as to the meaning of governmental activity and bypasses the difficulties arising through states' varying attitudes toward privatization. A number of criteria may assist in this analysis. These include a consideration of functions that are "quintessentially governmental" and an assessment of the overall context in which the relevant activities are performed. First, however, the ARSIWA commentary provides some initial guidance as to the types of criteria that should be taken into account.

A. Guidance within the ARSIWA Commentary

The ARSIWA commentary identifies four factors that are of particular importance when determining whether a function performed by a non-state actor falls within the sphere of governmental authority. These are: (1) the content of the powers, (2) the way the powers are conferred on an entity, (3) the purposes for which the powers are to be exercised, and (4) the extent to which the entity is accountable to the government in the exercise of the powers.[73]

The content of the powers delegated to a private entity is key to determining the public or private status of the act or function in question. This analysis focuses on the activities that the state empowers the entity to perform and in particular, whether those activities are normally reserved to the state or can be freely carried out by private individuals.[74] For instance, the exercise of powers involving the use of force or the right to constrain or control the activities of private individuals strongly indicates that the function concerned is governmental in nature.

On closer examination, however, the latter three criteria within the commentary are of limited assistance. The manner in which the powers are conferred relates to the "empowered by the law" requirement considered within Part IV below. A state may enact legislation authorizing the delegation of a particular function to a PMSC, for example, thereby indicating the importance of its decision and perhaps a likelihood that the delegated task is governmental. But that may equally be the case if a lesser means of empowerment is used, such as a contract. Thus, the manner in which the powers are conferred has no bearing on the status of the delegated activity.

The purpose of the powers is of greater relevance, but is rarely determinative of the issue. For instance, the fact that delegated powers are to be exercised in the public interest may indicate a governmental nexus. However, this criterion encompasses a broader range of functions, such as

---

73. ARSIWA, *supra* note 3, art. 5 commentary, ¶ 6.

74. *See infra* Part III for further discussion regarding the "private person" test. *See also* CRAWFORD, *supra* note 71, at 129-30.

education or the postal service, than those which necessarily amount to an exercise of governmental authority.[75]

The final factor referred to in the commentary relates to accountability, in terms of government supervision over the delegated activity.[76] This criterion captures the premise that states may wish to exercise greater control over private entities performing governmental functions than those that are not. But the fact that a private entity is not accountable to the government does not automatically mean that it is not performing governmental functions. Under the terms of Article 5, there is no requirement for state control over the activities in question in order for attribution to arise.[77] Indeed, if accountability were given too much weight when assessing the potential for state responsibility under Article 5, this could undermine the entire attribution standard.[78] As United Nations lawyer Hannah Tonkin stated in her analysis of state control over PMSCs, "[I]t is precisely in those cases where the government authorizes a PMSC to carry out a particular function, and yet fails to hold that PMSC accountable for its actions, that the rationale for the attribution of PMSC misconduct to the state is the strongest."[79] It is therefore necessary to look to other factors, in addition to those highlighted within the commentary, to determine whether a particular activity falls within the scope of governmental authority.[80]

B. Quintessentially Governmental Functions

A first such consideration is whether the task is "quintessentially" governmental. This classification encompasses functions typically performed by the state that are central to the nature and purpose of government.[81] Thus, the levying of taxes, the conduct of foreign affairs, and

75. CAMERON & CHETAIL, *supra* note 58, at 174. For further discussion regarding those functions that amount to an exercise of governmental authority, see the text accompanying notes 81-120 relating to quintessentially governmental functions and the "private person" test.

76. CRAWFORD, *supra* note 71, at 131.

77. ARSIWA, *supra* note 3, art. 5 commentary, ¶ 7.

78. *See* Chia Lehnardt, *Private Military Companies and State Responsibility*, *in* FROM MERCENARIES TO MARKET: THE RISE AND REGULATION OF PRIVATE MILITARY COMPANIES 139, 145 (Simon Chesterman & Chia Lehnardt eds., 2007); *see also* CAMERON & CHETAIL, *supra* note 58, at 174; TONKIN, *supra* note 46, at 103.

79. TONKIN, *supra* note 46, at 103.

80. The ARSIWA commentary itself indicates that the four factors are of "particular importance" but not the only criteria to be taken into account. *See* ARSIWA, *supra* note 3, art. 5 commentary, ¶ 6.

81. There is no definition in international law of those functions that are quintessentially or inherently governmental. However, guidance as to the meaning of the term may be found in the domestic law and policy of states, most notably the United States. *See, e.g.*, U.S. OFFICE OF FEDERAL PROCUREMENT POLICY, POLICY LETTER 11-01: PERFORMANCE OF INHERENTLY GOVERNMENTAL AND CRITICAL FUNCTIONS, FED. REG. 176, 56227 (Sept. 12, 2011), http://www.gpo.gov/fdsys/pkg/FR-2011-09-12/pdf/2011-23165.pdf. According to the Policy Letter, an inherently governmental activity is one that is "so intimately related to the public interest as to require performance by Federal Government employees." The Policy Letter lists five categories of

the enactment of laws are all inherently governmental, but the full range of tasks falling within this category is increasingly ambiguous. As one scholar noted, "When private companies are now rendering logistical support for military operations, running prisons and conducting interrogations, providing armed escort for personnel and convoys, doing general policing work, and carrying out surveillance, it is becoming more and more difficult, without offending either logic or common sense, to insist on maintaining that a particular activity is 'quintessentially sovereign' or 'typically private.'"[82] The assessment is especially problematic in the cyber domain, due to the novelty of cyber operations and the proliferation of non-state actors.

Nonetheless, if the focus remains on the functions themselves, certain activities qualify as inherently governmental irrespective of the domain in which they are undertaken. The ARSIWA commentary sets out a number of activities falling within the scope of Article 5 that may be considered quintessentially governmental. These include "powers of detention and discipline pursuant to a judicial sentence or to prison regulations . . . powers in relation to immigration control or quarantine . . . identification of property for seizure,"[83] and the activities of the police.[84] The contractors hired by the U.S. government to police post-conflict Bosnia were thus engaged in an inherently governmental function.[85]

Offensive combat also falls within this category, as a corollary of the state monopoly on the legitimate use of force.[86] Accordingly, the PMSCs that participated in the conflicts in Sierra Leone and Angola were engaged

---

function that are inherently governmental, including actions that determine, protect and advance the state's interests by military or diplomatic action and those that significantly affect the life, liberty, or property of private persons. Appendix A to the letter sets out an illustrative list of twenty-four functions that are considered to be inherently governmental. These include combat, security operations performed in environments where there is "significant potential for the security operations to evolve into combat" and the direction and control of intelligence and counter-intelligence operations. *See id.* For a discussion regarding the U.S. law and policy relating to inherently governmental functions, *see* James R. Lisher II, *Outsourcing Cyberwarfare: Drawing the Line for Inherently Governmental Functions in Cyberspace*, J. CONT. MGMT. 7, 8-10 (Summer 2014); Lindsay Windsor, *James Bond, Inc.: Private Contractors and Covert Action*, 101 GEO. L.J., 1427, 1431-40 (2013).

82. ZIAODONG YANG, STATE IMMUNITY IN INTERNATIONAL LAW 59-60 (2012).

83. ARSIWA, *supra* note 3, art. 5 commentary, ¶ 2.

84. *Id.* chapeau to pt. I, ch. II, ¶ 6.

85. TONKIN, *supra* note 46, at 100-01.

86. *See, e.g.*, Human Rights Council, Rep. of the Working Group on the Use of Mercenaries as a Means of Violating Human Rights and Impeding the Exercise of the Right of Peoples to Self-Determination, at 13, U.N. Doc. A/HRC/15/25, 13 (July 2, 2010), http://www2.ohchr.org/english/issues/mercenaries/docs/A.HRC.15.25.pdf.

> The Working Group describes inherently State functions . . . consistent with the principle of State monopoly on the legitimate use of force, [as including] the direct participation in hostilities, waging war and/or combat operations, taking prisoners, law-making, espionage, intelligence, knowledge transfer with military, security and policing application, use of, and other activities related to, weapons of mass destruction and police powers, especially the powers of arrest or detention including the interrogation of detainees.

in governmental activity.[87] But states rarely outsource such tasks to PMSCs. The Coalition Provisional Administration in Iraq, for example, took care to avoid even the appearance of contractors engaging in offensive activities, emphasizing that they were providing services that were defensive in nature.[88]

While PMSCs more commonly act in defensive roles, the line between offensive and defensive activities is often blurred. For example, a contractor tasked with protecting dignitaries may respond offensively to a perceived threat. In any event, purely defensive functions may qualify as inherently governmental. For instance, an armed contractor protecting a military objective against enemy attack in the context of an ongoing conflict is directly participating in hostilities.[89] While controversy remains as to the precise activities that amount to a direct participation in hostilities, [90] any contractor conduct that meets this threshold is so closely associated with the hiring state's military operations that it is inherently governmental in nature. The same is true of all PMSC activities with a direct operational effect, such as providing convoy security for a military operation, gathering or analyzing intelligence, interrogating detainees, or operating military equipment.[91] In addition, the running of prisoner of war camps or places

87. RALBY & TONKIN, *supra* note 16, at 3. *See also* Michael Ashworth, *Africa's New Enforcers*, INDEPENDENT (Sept. 15, 1996), www.independent.co.uk/news/africas-new-enforcers-1363564.html.

88. Lehnardt, *supra* note 78, at 147 (citing JENNIFER ELSEA & NINA M. SERAFINO, CONG. RESEARCH SERV., RL32419, PRIVATE SECURITY CONTRACTORS IN IRAQ: BACKGROUND, LEGAL STATUS, AND OTHER ISSUES 3 (2004)).

89. NILS MELZER, INT'L COMM. OF THE RED CROSS, INTERPRETIVE GUIDANCE ON THE NOTION OF DIRECT PARTICIPATION IN HOSTILITIES UNDER INTERNATIONAL HUMANITARIAN LAW 38 (2009). *But see* Allison Stanger, *Transparency as a Core Public Value and Mechanism of Compliance*, 31 CRIM. JUST. ETHICS 287, 295 (2012). Stanger distinguishes between those contractors who provide static security, for example guarding a particular location, and those who provide moving security, for example guarding personnel or convoys, opining that only the latter function is inherently governmental. If a guarding function does not amount to a direct participation in hostilities, *see infra* for discussion as to whether the function may nevertheless be governmental in light of the overall context in which it is performed.

90. Many governments, legal academics, and other commentators have raised concerns regarding the ICRC's conclusions. For example, the Spring 2010 issue of the New York University School of Law Journal of International Law and Politics featured a forum dedicated to discussing this issue. *See* Kenneth Watkin, *Opportunity Lost: Organized Armed Groups and the ICRC "Direct Participation in Hostilities" Interpretive Guidance*, 42 N.Y.U. J. INT'L L. & POL. 641 (2010); Michael N. Schmitt, *Deconstructing Direct Participation in Hostilities: The Constitutive Elements*, 42 N.Y.U. J. INT'L L. & POL. 697 (2010); Bill Boothby, *"And for Such Time As": The Time Dimension to Direct Participation in Hostilities*, 42 N.Y.U. J. INT'L L. & POL. 741 (2010); W. Hays Parks, *Part IX of the ICRC "Direct Participation in Hostilities" Study: No Mandate, No Expertise, and Legally Incorrect*, 42 N.Y.U. J. INT'L L. & POL. 769 (2010); *see also* Nils Melzer, *Keeping the Balance between Military Necessity and Humanity: A Response to Four Critiques of the ICRC's Interpretive Guidance on the Notion of Direct Participation in Hostilities*, 42 N.Y.U. J. INT'L L. & POL. 831 (2010) (responding to the four articles critiquing the ICRC's assessment).

Further discussion regarding the precise PMSC activities that amount to a direct participation in hostilities is beyond the scope of this article.

91. *See, e.g.*, Lehnardt, *supra* note 78, at 146; TONKIN, *supra* note 46, at 101; CAMERON & CHETAIL, *supra* note 58, at 200-01.

of civilian internment in international armed conflict is quintessentially governmental, as treaty obligations prohibit states from outsourcing such tasks.[92]

Equivalent functions performed in the cyber domain also qualify as inherently governmental.[93] Therefore, if in the context of an armed conflict, a state empowers a private entity to undertake certain cyber activities in support of the state's military operations, the entity's conduct in this respect amounts to an exercise of governmental authority. The 2008 cyber operations targeting government, media, and communications websites in Georgia and intentionally timed to coincide with the Russian military invasion in South Ossetia, fall within this category.[94] Equally, an offensive cyber operation that results in physical damage to, or a loss in functionality of, the target cyber infrastructure is governmental in nature.[95] The same is true in respect of other cyber operations that implicate governmental functions, such as the collection of intelligence regarding terrorist threats through cyber means.[96]

The assessment is more complex when considering the activities of non-state entities involved in cybersecurity. Private companies in recent years have played a dominant role in securing private computer networks against hostile cyber operations emanating from both state and non-state actors. Such activity includes operations aimed at eliminating the botnets responsible for a range of malicious cyber activity.[97] While the companies

---

92. Geneva Convention (III) Relative to the Treatment of Prisoners of War art. 39, Aug. 12, 1949, 6 U.S.T. 3316, 75 U.N.T.S. 135; Geneva Convention (IV) Relative to the Protection of Civilian Persons in Time of War art. 99, Aug. 12, 1949, 6 U.S.T. 3516, 75 U.N.T.S. 287. The state also has certain obligations under The Hague Regulations and Geneva Convention IV when it is an occupying power. These obligations again cannot be outsourced and are inherently governmental in nature.

93. For the purposes of Article 5 ARSIWA, if persons or entities are empowered to exercise elements of governmental authority, their conduct in performing those functions is potentially attributable to the state regardless of the domain within which the functions are performed. *See* ARSIWA, *supra* note 3, art. 5.

94. *See, e.g.*, John Markoff, *Before the Gunfire, Cyberattacks*, N.Y. TIMES (Aug. 12, 2008), http://www.nytimes.com/2008/08/13/technology/13cyber.html.

95. The 2010 *Stuxnet* operation targeting Iran's nuclear control systems is a classic example of a cyber operation that caused physical damage. *See* David E. Sanger, *Obama Order Sped Up Wave of Cyberattacks Against Iran*, N.Y. TIMES (June 1, 2012), http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html. Cyber operations causing physical damage or a loss in functionality are most likely to amount to a violation of a state's sovereignty, an unlawful use of force, or an armed attack and therefore implicate a state's foreign policy. *See* TALLINN MANUAL 2.0, *supra* note 25, at 20-21, 330-37, 340-42; Wright, *supra* note 25; Egan, *supra* note 37, at 11-14, 20.

96. *See also* Michael N. Schmitt & Liis Vihul, *Proxy Wars in Cyberspace: The Evolving International Law of Attribution*, 1 FLETCHER SECURITY REV. 54 (2014), http://ccdcoe.org/sites/default/files/multimedia/pdf/c28a64_2fdf4e7945e9455cb8f8548c9d328ebe.pdf. Schmitt and Vihul give the example of a private entity that issues certificates for national identification documents with the aim of assuring the security and authenticity of legally binding digital signatures as inherently governmental conduct. *Id.* at 61.

97. Eichensehr, *supra* note 32, at 479-82. Such operations are known as "botnet takedowns." A botnet is "[a] network of compromised computers, so-called 'bots,' remotely controlled by an intruder,

involved have a self-interest in pursuing such operations, public benefits often ensue, including the protection of critical cyber infrastructure and the reduction of transnational cybercrime. The functions performed thus ostensibly fall within the scope of law enforcement activity. Furthermore, private companies in the United States have engaged in "private intelligence-gathering at a sophisticated level" for the purpose of publicly attributing hacks to foreign states, when the U.S. government has been unwilling to do so.[98]

Activities of this nature implicate state foreign policy and have the potential to breach the state's obligations under international law. For example, such conduct may violate another state's sovereignty.[99] Despite this, the state's involvement in such operations is often minimal. Private companies have publicly attributed malicious cyber activity to foreign states at their own initiative, with little, if any, state involvement.[100] Moreover, although some "botnet takedown" operations have been conducted collaboratively between state law enforcement agencies and private companies, others involve private companies acting alone.[101] The activities of Microsoft provide a clear example. The company itself mounted six "botnet takedowns" prior to collaborating in further such operations with the U.S. government.[102]

In such circumstances, given the absence of any decision by the state to delegate elements of its governmental authority, it seems counterintuitive for a private company's activities to be potentially attributable to the state. Courts have yet to rule on the issue of attribution in such situations. In

---

'the botherder,' used to conduct coordinated cyber operations . . . ." *See* TALLINN MANUAL 2.0, *supra* note 25, at 563.

98. Eichensehr, *supra* note 32, at 489-94. Eichensehr gives a number of examples, including the 2015 hack of the U.S. Office of Personnel Management in relation to which the cybersecurity firm CrowdStrike alleged that the hackers were linked to the Chinese government. The U.S. government declined to identify those responsible but reportedly did provide CrowdStrike with technical information regarding the hack.

99. TALLINN MANUAL 2.0, *supra* note 25, at 17-27 (discussing Rule 4). *But see* Wright *supra* note 25, articulating the U.K. position that there is no cyber specific rule prohibiting a "violation of territorial sovereignty" in relation to interference in the computer networks of another state without its consent. The majority of states have not yet expressed a clear position as to the status of sovereignty as a binding rule, or merely a principle from which other obligations derive.

100. Eichensehr, *supra* note 32, at 493-94.

101. *Id.* at 479-82.

102. *Id.* at 481; *see also* Tim Cranton, *Cracking Down on Botnets*, MICROSOFT (Feb. 24, 2010), http://blogs.microsoft.com/blog/2010/02/24/cracking-down-on-botnets/; Kevin Poulsen, *Putin's Hackers Now under Attack—From Microsoft*, THE DAILY BEAST (July 20, 2017), http://www.thedailybeast.com/microsoft-pushes-to-take-over-russian-spies-network. Other states have collaborated with private actors in similar operations. *See, e.g.*, Jeremy Kirk, *Dutch Team Up with Armenia for Bredolab Botnet Take Down*, COMPUTERWORLD (Oct. 26, 2010), http://www.computerworld.com/article/2513676/government-it/dutch-team-up-with-armenia-for-bredolab-botnet-take-down.html.

practice, the key consideration may be whether the private company was empowered by the state to perform the relevant functions.[103]

But the fact remains that this type of activity often implicates foreign affairs, police power and national defense – functions that are inherently governmental in nature.[104] Thus, if the attribution standard encompassed within Article 5 ARSIWA is to retain its relevance, private companies' extensive involvement in cybersecurity should not serve to limit the breadth of tasks that are considered public in nature. Instead, if a company's activities in the cyber domain extend beyond simply protecting the security of its own networks or products to involve public functions such as law enforcement, intelligence gathering, or the conduct of foreign affairs, these activities should properly be considered an exercise of governmental authority.

When assessing the functions performed by private entities, such as cybersecurity companies, it is important to disaggregate the various tasks the entity carries out and consider the issue of attribution separately in each case. Thus, when assessing the potential attribution of Microsoft's conduct to the state, the many private functions the company performs should be considered separately from the activities it undertakes in the public interest, such as its "botnet takedown" operations. Likewise, if a PMSC performs a range of tasks within a detention facility located in a combat zone, its conduct related to the interrogation of detainees should be considered separately from its other functions, such as catering or cleaning. While the former is quintessentially governmental in nature, the latter tasks are not. But the fact that activities like catering do not fall within this category does not automatically exclude them from amounting to an exercise of governmental authority for the purposes of Article 5 ARSIWA. Instead, further enquiry is required to determine the status of those functions that do not relate intrinsically to the nature and purposes of government, but nevertheless have a governmental nexus due to the context in which they are performed.

C. The "Private Person" Test

The disaggregation of a private entity's activities serves to separate any governmental functions from those that are private or commercial in nature, and therefore fall outside the scope of governmental authority.[105] A key characteristic of private and commercial conduct is that it can be carried out

103. *See infra* Part IV.

104. Eichensehr, *supra* note 32, at 475.

105. ARSIWA, *supra* note 3, art. 5 commentary, ¶ 5 ("If it is to be regarded as an act of the State for the purposes of international responsibility, the conduct of an entity must accordingly concern governmental activity and not other private or commercial activity in which the entity may engage.").

by private entities without authorization from the state. Conversely, functions within the sphere of governmental authority imply the exercise of powers that "the state ordinarily reserves . . . for itself," meaning that if such powers are to be exercised by a private entity, explicit government permission is first required.[106]

By way of example, the ARSIWA commentary refers to a railway company that exercises some police powers, as well as carrying out other activities such as ticket sales.[107] While the former may amount to an exercise of governmental authority, the latter do not. In the context of PMSCs, a contractor's activities relating to the supply of military equipment to the state is private and commercial in nature and thus analogous in this respect to the sale of tickets. In the cyber domain, setting up a computer network for use by a state's military is similarly private and commercial.[108] Such conduct, therefore, does not fall within the scope of governmental authority.

This "private person" test is often used in the law of state immunity to distinguish between those activities that involve sovereign authority and are therefore immune from the jurisdiction of other states and those that do not.[109] The test also assists in determining whether a particular activity falls within the scope of governmental authority for the purposes of Article 5 ARSIWA.[110] The key determination is whether the function concerned is one that a private entity could lawfully perform pursuant to a relationship with a private client rather than a state.[111] For example, private individuals cannot lawfully provide military advice to local militias involved in armed conflict or engage in official government communications without express

106. CRAWFORD, *supra* note 71, at 130; s*ee also* CAMERON & CHETAIL, *supra* note 58, at 198; TONKIN, *supra* note 46, at 101-02.

107. ARSIWA, *supra* note 3, art. 5 commentary, ¶ 5.

108. The sale of software by a private entity to a state is also commercial in nature. *See, e.g.*, Joseph Cox, *The FBI Spent $775k on Hacking Team's Spy Tools Since 2011*, WIRED (July 6, 2015), http://www.wired.com/2015/07/fbi-spent-775k-hacking-teams-spy-tools-since-2011/.

109. For the purposes of state immunity, it is the nature of the act that is the most significant, rather than the motive or purpose for which it is carried out. *See* YANG, *supra* note 82, at 85-108. If a state exercises sovereign, public or governmental powers (*acta iure imperii*) then it enjoys immunity, but if it exercises private or non-governmental powers that could be exercised by a private citizen (*acta iure gestionis*), then it does not. Examples of the former include the administration of justice, the take-off and landing of military aircraft and the conduct of foreign and military affairs, while the principal activities falling within the latter are commercial in nature. *See* TONKIN, *supra* note 46, at 104; CAMERON & CHETAIL, *supra* note 58, at 182. In this context, the repair of installations at a naval base and the establishment of security measures at an embassy were also held to be sovereign activities. *See* YANG, *supra* note 82, at 82-83.

110. CRAWFORD, *supra* note 71, at 130. In Crawford's view, the distinction should be applied to attribution under Article 5 to achieve consistency between the two areas of international law. However, this view is not universally shared. For example, the United Kingdom commented that "The principles developed for the purpose of deciding whether bodies are entitled to State immunity are not necessarily applicable for the purpose of deciding whether the State is responsible for the acts and omissions of those bodies." *See* Comments and Observations Received from Governments, *supra* note 64, at 49.

111. TONKIN, *supra* note 46, at 101.

state approval.[112] In contrast, private individuals may post information about terrorist organizations on a website or provide training on interrogation techniques without such permission.[113] Such conclusions indicate that the former activities are public in nature, whereas the latter are not. Equally, while a contractor may lawfully collect information from open sources for a private client, it cannot use intrusive methods to gather intelligence, in potential violation of privacy laws, without state authorization.[114] The latter, if performed pursuant to an empowerment by the state, is therefore likely to amount to an exercise of governmental authority.

In the cyber domain, many states prohibit private entities that have fallen victim to a malicious cyber intrusion from engaging in "active defense" measures affecting the data or computer networks owned by others.[115] Commonly known as "hacking back," such activity may range in effect from mere information gathering to the deletion of stolen data or the emplacement of malicious code on the perpetrator's network. As this may have cross-border effects and implicate foreign affairs, cybersecurity companies cannot lawfully perform such functions at the instigation of a private client, without express government authorization.[116] However, in view of states' limited capacities to deal with cybersecurity threats, some commentators advocate for the compilation of a government-approved list of firms that are permitted to take action to identify attackers and to "hack back" on victims' behalf.[117] If such a system were implemented, the activities of the private entities concerned would likely amount to an exercise of governmental authority, with potential attribution to the state of their conduct when acting in the designated capacity.[118] In these circumstances, any activities violating the sovereignty of nations affected by

112. *Id.* at 102; TALLINN MANUAL 2.0, *supra* note 25, ¶ 17 (discussing Rule 4).

113. TALLINN MANUAL 2.0, *supra* note 25, ¶ 17 (discussing Rule 4).

114. TONKIN, *supra* note 46, at 102.

115. For example, in the United States, such measures are contrary to the Computer Fraud and Abuse Act, while in the United Kingdom these measures contravene the Computer Misuse Act 1990. More than fifty states have ratified the Budapest Convention on Cybercrime, Nov. 23, 2001, which aims to harmonize states' domestic criminal laws relating to cybercrime and establish a common minimum standard of offences. Conduct in the cyber domain is prohibited by the Convention if it is performed "without right." States are not restricted in the way in which they implement this concept in their domestic law, but it may refer to conduct taken without the state's authority. *See* Council of Europe, Explanatory Report to the Convention on Cybercrime (Nov. 23, 2001) ¶¶ 38, 47, http://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090 00016800cce5b.

116. *Id.*

117. Jeremy Rabkin & Ariel Rabkin, *Hacking Back Without Cracking Up*, LAWFARE (July 1, 2016), http://www.lawfareblog.com/hacking-back-without-cracking-0; *The Attribution Revolution: Raising the Costs for Hackers and Their Customers: Hearing Before the Subcomm. on Crime and Terrorism of the S. Comm. on the Judiciary*, 113th Cong. 7 (2013) (statement of Stuart A. Baker, Partner, Steptoe & Johnson LLP), http://www.judiciary.senate.gov/imo/media/doc/5-8-13BakerTestimony.pdf.

118. Attribution would only arise if the entity were properly empowered by the state to undertake the relevant "hack back" activity. *See infra* Part IV.

the "hack back" activity would amount to an internationally wrongful act, triggering state responsibility.[119]

While finding that state permission is required for a private actor to perform a given task strongly indicates its governmental nature, the converse is not always true. Actions which do not by their nature require state permission, but which were requested by, or conducted in the service of the state, may still be attributable. For example, if a contractor gathers and analyses open source intelligence on behalf of the state, this nexus to governmental activity should be taken into account when assessing whether the task falls within the scope of governmental authority. Similarly, although PMSC contractors could lawfully serve as armed guards for a mining company operating within a hostile environment without state authorization, this does not mean that equivalent services performed for the benefit of the state are not governmental in nature.[120] It is therefore necessary to look to the broader context in which an activity is performed for further guidance as to its status.

D. The Overall Context

English courts considering the distinction between sovereign and private powers for the purposes of state immunity have looked beyond the "private person" test to the wider environment in which the relevant functions are carried out.[121] The courts concluded that, when viewed in context, the provision of educational and medical services for military personnel located at U.S. air bases in the United Kingdom was sovereign in nature.[122] One English judge stated, "I do not think that there is a single test or 'bright line' by which cases on either side can be distinguished. Rather, there are a number of factors which may characterize the act as nearer to or

---

119. *See supra* note 99.

120. CRAWFORD, *supra* note 71, at 130; TONKIN, *supra* note 46, at 101-02.

121. YANG, *supra* note 82, at 105-07 and n.248.

> [T]he court must consider *the whole context* in which the claim against the state is made, with a view to deciding whether the relevant act(s) upon which the claim is based, should, in that context, be considered as fairly within an area of activity, trading or commercial, or otherwise of a private law character, in which the state has chosen to engage, or whether the relevant act(s) should be considered as having been done outside that area, and within the sphere of governmental or sovereign activity.

(emphasis in original) (noting that Lord Wilberforce initially made this statement in I Congresso del Partido [1983] 1 AC 244, 267). A consideration of wider contextual issues is not unique to the United Kingdom, as Australian, New Zealand, Irish, Israeli, and Malaysian courts have also used this approach.

122. Holland v. Lampen-Wolfe [2000] 1 WLR 1573 at 1577; Littrell v. United States (No. 2) [1995] 1 WLR 82 at 91, 94-95. "The court has to look at all the circumstances in relation to the nature of the activity and its context and decide whether those factors together—no one factor being in itself determinative—characterize the activity as sovereign or non-sovereign." Littrell v. United States (No. 2) [1995] 1 WLR 82 at 91 (per Rose L.J.).

further from the central military activity."[123] He went on to articulate the most important factors to consider when making this determination, including the location where the relevant activities are conducted, whom they involve, and the nature of the act.[124]

Assessing activities in context may prove particularly important in determining the status of PMSC activities that are not inherently governmental, such as the provision of armed guarding services or logistical support. Functions performed by a PMSC in a combat zone are more likely to amount to governmental activity than those carried out in a more benign environment, but the location itself is not determinative. For example, the activities of armed security guards protecting a private oil field within an area of combat are not governmental in nature.[125] Further factors, therefore, need to be taken into account, including the identity of the personnel for whose benefit the function is being performed. In the guarding context, if the assets or personnel of a private company are protected, then the activity is unlikely to be governmental in nature. Alternatively, if the intent is to protect military assets or civilian dignitaries, then the activity is for the benefit of the state and is more likely to fall within the sphere of governmental authority. Finally, it may be relevant to consider the nature of any equipment provided to PMSC personnel for use in the performance of their duties, such as firearms. While not conclusive on their own, when considered together, these factors may indicate whether the PMSC is performing public functions amounting to elements of governmental authority.

A grey area nevertheless remains, in particular regarding those PMSC functions with the weakest nexus to military action such as catering, reconstruction, and the delivery of goods. An assessment as to whether such activities are governmental in nature is especially difficult in contemporary conflicts in which non-state armed groups often fail to discriminate between military and non-military targets.[126] Thus, in recent combat environments, even functions with a weak military nexus have drawn contractors into hostilities, as illustrated by the deaths of four Blackwater employees in Fallujah, Iraq, while collecting non-military equipment.[127]

This development tends to expand the range of circumstances in which a contractor's activities within a combat zone may amount to an exercise of governmental authority. The decisions of the English courts relating to the

123. Littrell v. United States (No. 2) [1995] 1 WLR 82 at 95 (per Hoffman L.J.).

124. *Id.*

125. TONKIN, *supra* note 46, at 101-02, 108.

126. Lehnardt, *supra* note 78, at 148.

127. *See, e.g.*, David Barstow, *The Struggle for Iraq: The Contractors; Security Firm Says Its Workers Were Lured into Iraqi Ambush*, N.Y. TIMES (Apr. 9, 2004), http://www.nytimes.com/2004/04/09/world/struggle-for-iraq-contractors-security-firm-says-its-workers-were-lured-into.html.

provision of medical and educational services on a military base also support a more inclusive interpretation regarding the scope of governmental functions.[128] Although each such determination would require a case-by-case fact intensive inquiry, many services provided by a PMSC in a conflict zone for the benefit of state armed forces or government officials may therefore fall within the scope of governmental authority.[129]

In the cyber domain, the context in which an activity is performed is equally relevant when considering whether it falls within the scope of governmental authority. While cyber operations may be carried out remotely, rendering the location potentially immaterial, other contextual factors may assist in this determination. Any tools or information a government provides in connection with a cyber operation, such as malware or intelligence, may point toward its governmental nature.[130] Furthermore, the nexus between the cyber operation and government activity is of particular importance. For example, although the maintenance of computer networks is not an inherently governmental function, if a private contractor is tasked with maintaining and defending the computer network that supports a state's integrated air defense system, the close nexus between this function and the state's military activity is likely to lead to the conclusion that it falls within the scope of governmental activity.

E. Powers Conferred on Ordinary Citizens

As these examples illustrate, conduct that is closely linked to military activity generally amounts to an exercise of governmental authority. Similarly, powers that involve the use of force are normally governmental in nature. The ARSIWA commentary, however, includes one important caveat in this respect, stating that Article 5 "does not extend to cover . . . situations where internal law authorizes or justifies certain conduct by way of self-help or self-defense; i.e. where it confers powers upon or authorizes conduct by citizens or residents generally."[131] The use of force by private individuals acting purely to defend themselves, or to exercise a power of citizen's arrest in accordance with domestic law, therefore falls outside the scope of Article 5. Nonetheless, if the state delegates a function to a private entity and

128. Littrell v. United States (No. 2) [1995] 1 WLR 82 at 91, 94-95; Holland v. Lampen-Wolfe [2000] 1 WLR 1573 at 1577.

129. TONKIN, *supra* note 46, at 107-08; *but see* CAMERON & CHETAIL, *supra* note 58, at 202 (concluding that activities such as logistics, catering, reconstruction, and delivery of goods are not governmental, even though they are necessary to support armed forces in the field).

130. *See, e.g.*, Sam Jones, *Cyber Crime: States Use Hackers to Do Digital Dirty Work*, FIN. TIMES (Sept. 4, 2015), http://www.ft.com/content/78c46db4-52da-11e5-b029-b9d50a74fd14.

131. ARSIWA, *supra* note 3, art. 5 commentary, ¶ 7.

authorizes the entity to exercise particular powers in the performance of that function, the entity's conduct is likely to fall within the scope of Article 5.[132] Clarity may be gained in such circumstances by assessing whether the powers exercised by the private entity are greater than those at the disposal of ordinary citizens under the state's domestic law. That may be the case if the delegated activity involves, for example, a power to constrain, supervise, regulate, or control the activities of private individuals, if necessary through the use of force.[133]

Consider, in this respect, the decision taken by various states in 2011 to authorize their merchant vessels to carry weapons for the purpose of countering the threat from Somali-based pirates.[134] At that time, a number of governments "reversed longstanding legal bans or serious restrictions on the direct arming of merchant ships," thereby allowing armed crew members or guards to forcefully prevent an illegal boarding.[135] While the use of force by such individuals is governed by national laws of self-defense, the authorization to carry and potentially use firearms for this purpose is provided by the state.[136] The question therefore arises as to the accountability of the state in respect of an unlawful use of force by one or more of the armed guards on board the vessel. Applying the "private person" test, a private individual cannot use weapons to protect a state-flagged vessel without government authorization. Thus, even though the armed guards in these circumstances act in accordance with national laws of self-defense, their powers are greater than those of ordinary citizens. As such, their conduct amounts to an exercise of governmental authority and potentially engages the responsibility of the state.

F. Conclusions as to the Scope of Governmental Authority

In summary, therefore, governmental authority in the context of Article 5 ARSIWA encompasses those traditional powers that undergird the state's

---

132. Alexis P. Kontos, *"Private" Security Guards: Privatized Force and State Responsibility Under International Human Rights Law*, 4 NON-STATE ACTORS & INT'L L. 199, 221 (2004); CAMERON & CHETAIL, *supra* note 58, at 170-71.

133. CAMERON & CHETAIL, *supra* note 58, at 198.

134. *See, e.g.*, William Marmon, *Merchant Ships Starting to Carry Armed Guards Against Somali Pirates*, EUR. INST. (Nov. 2011), http://www.europeaninstitute.org/index.php/ei-blog/137-november-2011/1471-merchant-ships-start-to-carry-armed-guards-against-somali-pirates-1122.

135. *Id.*

136. *See, e.g.*, DEP'T FOR TRANSPORT, INTERIM GUIDANCE TO UK FLAGGED SHIPPING ON THE USE OF ARMED GUARDS TO DEFEND AGAINST THE THREAT OF PIRACY IN EXCEPTIONAL CIRCUMSTANCES: VERSION 1.3 (updated Dec. 2015) (UK), http://www.gov.uk/government/uploads/system/uploads/attachment_data/file/480863/use-of-armed-guards-to-defend-against-piracy.pdf.

existence as a public authority.[137] But it is far from easy, in practice, to identify where exactly the boundaries lie. When assessing whether a particular function falls within the scope of governmental authority, the first requirement is to identify the specific powers involved and to disaggregate them if appropriate. The following questions may assist in evaluating whether an activity performed by a private entity amounts to an exercise of governmental authority:

(1) Is the function quintessentially governmental, involving, for example, law enforcement or offensive combat?
(2) Does the exercise of the function by a private entity require government authorization, in the sense that it cannot lawfully be performed pursuant to a relationship between two private entities?
(3) In what context will the function be performed? Relevant factors include:
    (a) The location where the activity is carried out;
    (b) Its nexus to military or other governmental activity;
    (c) The identity of the personnel for whose benefit the activity is performed; and
    (d) The nature of any tools, equipment, or information that the state provides to the entity for use in connection with the performance of the function.
(4) Does the activity involve greater powers than those at the disposal of ordinary citizens? For example, does it involve a power to constrain, supervise, regulate, or control the activities of private individuals, if necessary through the use of force?
(5) Is the activity carried out in the public interest?

While a positive answer to the first or second questions may conclusively indicate that the relevant activity falls within the scope of governmental authority, a negative response to these questions is merely indicative toward the contrary conclusion. Further enquiry into the matter is then required, including consideration of the issues raised in questions three through five. Once all the questions are addressed, it may be clear that the conduct in question either is, or is not, an exercise of governmental authority. But ambiguity may remain in relation to some borderline activities. If courts or tribunals are called upon to determine the issue of attribution in such marginal cases, the outcome is likely to depend upon the weight the court gives to the various factors outlined above. In addition, the court will need

137. Nwamaka R. Okany, *State Delegation of Functions to Private and Autonomous Entities: A Basis for Attribution Under the Rules of State Responsibility*, *in* STATE RESPONSIBILITY AND THE INDIVIDUAL 327, 335 (Kalliopi Koufa ed., 2006).

to make an assessment as to whether the entity was properly empowered by the state to carry out the activities concerned.

IV. EMPOWERED BY THE LAW

A. The Nature of the Empowerment Requirement

Article 5 ARSIWA includes a specific requirement that the person or entity exercising governmental powers be "empowered by the law of that State" to do so.[138] ARSIWA thus incorporates an express condition referring to a state's domestic law, without which responsibility will not arise. In the view of one ILC member, the inclusion of this requirement was justified because "the entities in question were not part of the formal structure of the State, and only internal law could authorize them to exercise elements of the governmental authority."[139] Nonetheless, the ILC's deliberations and the ARSIWA commentary do not specify what form the relevant legal authorization must take.

Specific legislation authorizing a private entity to exercise elements of governmental authority clearly amounts to empowerment by the law within the meaning of Article 5, but the question remains whether any other basis will suffice. The ARSIWA commentary gives the example of private security firms "contracted to act as prison guards," thereby indicating that Article 5 also encompasses a delegation of governmental authority via contract.[140] Given the prevalence of contractual arrangements between governments and PMSCs, this is an important clarification. Nevertheless, a contract is not *per se* the law of the state; it is, instead, an instrument authorized by law that has effect within the national legal order.[141] A more general legal authority is therefore required, empowering a government agency to delegate certain powers to a private company via contract. In the view of James Crawford, the ILC's final Special Rapporteur for state responsibility, "If such functions are lawfully conferred by public contract, then the empowering law would qualify for the purposes of an Article 5 delegation."[142]

The nature of the requisite authorization may vary according to the domestic legal traditions of the country concerned. By way of example, while the United Kingdom government may enter into contracts with private persons without statutory authority, as an exercise of its executive

138. ARSIWA, *supra* note 3, art. 5; *see also id.* at 92, ¶ 7 ("The formulation of article 5 clearly limits it to entities which are empowered by internal law to exercise governmental authority.").

139. *Summary Records of the 2553rd Meeting, supra* note 9, at 236, ¶ 23 (comments of Mr. Herdocia Sacasa).

140. ARSIWA, *supra* note 3, art. 5 commentary, ¶ 2.

141. CAMERON & CHETAIL, *supra* note 58, at 169.

142. CRAWFORD, *supra* note 71, at 131.

powers,[143] other states require specific legislation in order for such contractual arrangements to be lawful.[144] Empowerment by the law may thus arise in varying guises. Crawford recognizes that statutory and executive orders suffice in order to bring a delegation within the scope of Article 5.[145] The same reasoning applies to other domestic legal instruments such as regulations, byelaws, or administrative acts, and to any delegations made thereunder, including contracts, charters, operating licenses, and concessions.[146] Any form of instrument relating to a delegation that complies with the requirements of the relevant state's domestic law is thus sufficient to meet the "empowered by the law" requirement within Article 5 ARSIWA.

Ambiguity remains, however, regarding the level of detail that must be included within the relevant legal authorization. In particular, it is unclear whether a contract that specifies a broad delegated function will suffice, or whether the instrument must detail the precise activities that the PMSC or other private entity is authorized to carry out in performance of that function. The commentary to Article 5 ARSIWA suggests that the delegated public powers must be specified within the authorization.[147] But in Crawford's view, there is no requirement "that the empowering law should define the roles and responsibilities of the entity exhaustively."[148] This latter conclusion is persuasive, as otherwise few delegations of authority would likely be detailed enough to fall within the scope of Article 5. It follows that a contract delegating guarding functions to a PMSC, for example, should specify the categories of personnel or facilities to be protected, the equipment that contractors may use for this purpose, and whether they are entitled to use force, but need not include details such as day-to-day patrolling requirements or the rules of engagement under which the contractors must operate.

143. The powers of the U.K. central government derive from the executive power of the sovereign. For a discussion of these prerogative powers, see, for example, Gail Bartlett & Michael Everett, *The Royal Prerogative*, HOUSE OF COMMONS LIBRARY BRIEFING PAPER NUMBER 03861, at 11-12 (2017) http://researchbriefings.parliament.uk/ResearchBriefing/ Summary/SN03861.

144. For example, France has enacted legislation relating to the outsourcing of public functions. For a discussion regarding the outsourcing of military and security services in France, see V. Capdevielle, *The Regulatory Context of Private Military and Security Services in France,* PRIV-WAR REPORT – FRANCE, NATIONAL REPORTS SERIES 11/09 (2009), http://psm.du.edu/media/documents/reports_and_stats/think_tanks/privwar_national-report_capdevielle.pdf.

145. CRAWFORD, *supra* note 71, at 130.

146. CAMERON & CHETAIL, *supra* note 58, at 168; Okany, *supra* note 137, at 336.

147. ARSIWA, *supra* note 3, art. 5 commentary, ¶ 7 ("The internal law in question must specifically authorize the conduct as involving the exercise of public authority; it is not enough that it permits activity as part of the general regulation of the affairs of the community.").

148. CRAWFORD, *supra* note 71, at 132.

While functions are commonly delegated to PMSCs by way of contract, the same is not true in the cyber domain.[149] As previously discussed,[150] it is now common for cybersecurity companies to perform seemingly public functions without any formal delegation of powers by the state. Instead, companies simply notify the state of their activities, or in the case of "botnet takedowns," they apply to the courts to receive judicial authorization.[151] Regarding the latter, the question arises as to whether permission given by a state's domestic courts for a private company to engage in ostensibly public activities amounts to empowerment in accordance with the state's internal law. On the ordinary meaning of the words, given that the judiciary is an organ of state, such authorization appears to fulfill the requirements of Article 5 ARSIWA. However, due to the novelty of such operations, a degree of ambiguity remains. This scenario was not contemplated by the ILC when considering the scope of Article 5.[152] Moreover, judicial endorsement differs in certain respects from a delegation of state powers – when U.S. law enforcement agencies engage in similar operations, for example, they too require approval from the courts.[153] Thus, while judicial authorization logically appears to be a means through which legal empowerment may materialize, it remains somewhat unclear whether this suffices for the purposes of Article 5 ARSIWA.

In the event that judicial approval does amount to legal empowerment, an authorization given to a cybersecurity company is likely to relate only to the actions of the particular company which submitted the application.[154]

---

149. Although it is not as common for states to delegate tasks to private entities operating in the cyber domain via contract, examples nevertheless exist, particularly in the United States. *See, e.g.*, Aaron Boyd, *CYBERCOM Awards Spots on New $360M Cyber Operations Contract*, FEDERAL TIMES (May 23, 2016), http://www.federaltimes.com/2016/05/23/cybercom-awards-spots-on-new-460m-cyber-operations-contract/; Defense Systems, *Army Awards $125 Million Contract for Cyber Operations*, DEFENSE SYSTEMS (Oct. 5, 2014), http://defensesystems.com/articles/2014/10/15/army-netcom-nci-contract-cyber-operations.aspx; MAURER, *supra* note 26, at 73-79, discussing the United States' use of contractors for both cybersecurity and offensive cyber operations; CrowdStrike, *CrowdStrike Global Threat Report: 2013 Year in Review*, CROWDSTRIKE, Jan. 2014, at 26 (noting that an active operator in the cyber domain during 2013 may actually be "an India-based security firm known as *Appin Security Group* that may have been contracted by the Indian government" to target numerous entities including "Pakistani military and political entities").

150. *See supra* Part III.

151. Eichensehr, *supra* note 32, at 479-80, 494.

152. In the course of its discussions regarding the attribution standard now reflected in Article 5 ARSIWA, the ILC did not refer specifically to the possibility of empowerment via the actions of a state's judiciary. *See, e.g.*, *Third Report on State Responsibility*, *supra* note 71, at 262-67; *Summary Records of the 1258th Meeting*, [1974] 1 Y.B. Int'l L. Comm'n 32-36, U.N. Doc. A/CN.4/SER.A/1974, http://legal.un.org/ilc/publications/yearbooks/english/ilc_1974_v1.pdf; *Summary Records of the 1259th Meeting*, [1974] 1 Y.B. Int'l L. Comm'n 36-40, U.N. Doc. A/CN.4/SER.A/1974, http://legal.un.org/ilc/publications/yearbooks/english/ilc_1974_v1.pdf; James Crawford (Special Rapporteur), *First Rep. on State Responsibility*, *supra* note 64, at 37-39, 56.

153. Eichensehr, *supra* note 32, at 480.

154. *See, e.g.*, Brief re Motion for Limited Authority to Conduct Discovery Necessary to Identify and Serve Doe Defendants, Microsoft Corp. v. Does 1-18, Controlling a Computer Botnet Thereby

Therefore, subcontracting is likely to be lawful only if the court specifically agreed that the relevant function could be reallocated to another entity.[155] Relatedly, if the legal instrument delegating powers to a PMSC specifically provides for that PMSC to subcontract, then the resulting actions of the subcontractor are potentially attributable to the state.[156] If, however, the contract or other form of legal authorization does not envisage a right to subcontract, then the issue of attribution is less clear.

For example, if a state grants PMSC A authorization to operate military equipment and PMSC A then subcontracts a portion of these functions to PMSC B without the state's consent, the state has not directly empowered PMSC B to exercise elements of its governmental authority.[157] It is therefore arguable that any acts committed by PMSC B when operating that equipment are not attributable to the state. This is particularly the case if the state takes action, as soon as it becomes aware of the unauthorized sub-contracting, to prevent the continued operation of the equipment by PMSC B.[158] The position may be different, however, if the state is aware of, and tolerates, PMSC B's performance of the function, or authorizes PMSC B's conduct in a way that does not accord with the state's domestic law.[159]

While a state's subsequent endorsement of private conduct may give rise to attribution under Article 11 ARSIWA,[160] it is also pertinent to consider the potential for attribution pursuant to Article 5 if an entity is empowered by the state to exercise elements of governmental authority, but that delegation is not carried out in accordance with the state's internal law.

Consider, for example, the position of the Shabbiha, or "ghost" forces that fought on behalf of the Syrian regime during the early stages of the recent conflict. According to the November 2011 report of the United Nations Commission of Inquiry, the Shabbiha forces were "composed of an estimated 10,000 civilians, who [were] armed by the Government and [were] widely used to crush anti-Government demonstrations alongside

---

Injuring Microsoft and its Customers, No. 1:13-cv-00139-LMB-TCB, (E.D. Va. Feb. 13, 2013). In the brief, Microsoft requested authority to conduct discovery into the relevant sources itself.

155. *Id.* A company's ability to lawfully subcontract an activity authorized by a court will depend upon the terms of the authorization granted.

156. TONKIN, *supra* note 46, at 111.

157. It may also be the case that the original contractor acted outside the terms of the contract when sub-contracting. *See infra* Part V for a further consideration of *ultra vires* conduct.

158. *Id.* As discussed in Part V, *infra*, a private entity's conduct may be attributable to a state pursuant to Article 5 ARSIWA even if the entity acts in excess of its authority or in contravention of instructions issued by the state. However, if the acts in question are committed by a separate entity that exercises powers as an unauthorized sub-contractor, the legal position is less clear. In such a situation, the way in which the state reacts to the unauthorized sub-contracting may be key to determining the issue of attribution.

159. *Id.*

160. This would occur if the state subsequently acknowledged and adopted the conduct as its own. *See supra* Part II.

national security forces."[161] While such forces were integrated into the government in early 2013,[162] their status prior to that date is unclear. It may be that they were *de facto* state organs of the Syrian regime, meaning that their conduct was attributable to the state pursuant to Article 4 ARSIWA.[163] However, such a status is "exceptional" in nature, requiring proof of a particularly high level of state control.[164] Attribution pursuant to Article 8 ARSIWA is also difficult to prove, requiring evidence of state instructions, direction, or control relating to the particular operations during which the relevant violations of the state's international human rights obligations were committed.[165] It may be that neither basis of attribution could apply to the Shabbiha's actions, particularly given that the group reportedly acted with a sense of total impunity.[166]

The Shabbiha clearly exercised public powers within Syria prior to their integration into the government – they acted alongside state security forces, carrying out law enforcement functions on behalf of the regime. However, it appears that the requisite authority to do so was not delegated to the Shabbiha in accordance with Syrian law. Instead, in early 2011, the Syrian regime reportedly "began to use money and services to buy the allegiance of unemployed youth, to distribute guns, cars, and security clearances to trusted loyalists and their families, essentially weaponizing the vast web of

---

161. Human Rights Council, Rep. of the Independent International Commission of Inquiry on the Syrian Arab Republic, ¶ 20, U.N. Doc. A/HRC/S-17/2/Add.1 (Nov. 23, 2011), http://www.ohchr.org/Documents/Countries/SY/A.HRC.S-17.2.Add.1_en.pdf. *See also* Expert Report of Ewan Brown at ¶ 126, Colvin v. Syrian Arab Republic, No. 1:16-cv-01423-ABJ, (D.D.C. Mar. 2, 2018) ("Evidence indicates that such [pro-regime paramilitary] groups were used in security operations that included the suppression of demonstrations, the guarding of facilities, employment on checkpoints and operationally securing territory taken back from the opposition control.").

162. *Syria: Pro-Government Paramilitary Forces*, CARTER CTR. (Nov. 5, 2013), at 8 http://www.cartercenter.org/resources/pdfs/peace/conflict_resolution/syria-conflict/pro-governmentparamilitaryforces.pdf.

163. ARSIWA, *supra* note 3, art. 4. *See supra* Part II for further discussion regarding *de facto* state organs.

164. Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosn. & Herz. v. Serb. & Montenegro), Judgment, 2007 I.C.J. Rep. 43, ¶ 393 (Feb. 26).

165. *Id.* ¶¶ 397-406; Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. Rep. 14, ¶ 115 (June 27). The Shabbiha are reportedly "responsible for or complicit in the commission of human rights abuses in Syria," including firing into crowds of peaceful demonstrators, shooting and killing demonstrators, arbitrarily detaining Syrian civilians, and shooting Syrian soldiers who refused to fire on peaceful demonstrations. *See* Press Release, U.S. Dep't of the Treasury, Treasury Sanctions Al-Nusrah Front Leadership in Syria and Militias Supporting the Asad Regime (Dec. 11, 2012), www.treasury.gov/press-center/press-releases/pages/tg1797.aspx.

166. *See, e.g.*, Human Rights Council, Rep. of the Independent International Commission of Inquiry on the Syrian Arab Republic, Annex V, U.N. Doc. A/HRC/22/59, at ¶ 6 (Feb. 5, 2013), http://www.ohchr.org/Documents/HRBodies/HRCouncil/CoISyria/A.HRC.22.59_en.pdf (referring to a raid in Homs during which the Shabbiha took a man into the street, shot, and killed him; the military appeared disgusted by this but seemed powerless to stop the Shabbiha). Examples such as this indicate a lack of state control over the Shabbiha's actions.

client networks constructed over four decades of Assad family rule."[167] In this way, the regime empowered the Shabbiha to act but did not do so by law, meaning that the Shabbiha's actions are not attributable to the state under the terms of Article 5 ARSIWA.

The situation of the Shabbiha is by no means unique. Also in Syria, Shi'a militias have augmented government forces on the battlefield with the apparent sanction of the Syrian regime, but with no clear legal authority to do so.[168] Meanwhile, in neighboring Iraq, the Prime Minister established the Popular Mobilization Forces (PMF) to fight the Islamic State in June 2014, but did not do so in compliance with Iraq's domestic law until the PMF's subsequent integration into the security forces in 2016.[169] Therefore, although such militia groups conducted offensive combat operations on the state's behalf, in the absence of legal empowerment, their conduct is not attributable to the state under the terms of Article 5.[170]

The requirement for empowerment by law also impacts the potential attribution of cyber activities to the state. In contrast with the contractual relationships common between states and PMSCs, "the public-private collaborations in cybersecurity are informal, de facto partnerships, operating outside a contractual framework."[171] As such, it may be that they are not established in accordance with the state's internal law. This is all the more

---

167. Aron Lund, *Who Are the Pro-Assad Militias?*, CARNEGIE MIDDLE EAST CENTER (Mar. 2, 2015), http://carnegie-mec.org/diwan/59215?lang=en.

168. *See, e.g.*, MARISA SULLIVAN, INSTITUTE FOR THE STUDY OF WAR, HEZBOLLAH IN SYRIA (Apr. 2014), http://www.understandingwar.org/sites/default/files/Hezbollah_Sullivan_FINAL.pdf; Nicholas Blanford, *The Battle for Qusayr: How the Syrian Regime and Hizb Allah Tipped the Balance*, CTC SENTINEL (Aug. 2013) at 18-22, http://ctc.usma.edu/app/uploads/2013/08/CTCSentinel-Vol6Iss86.pdf; Anne Barnard, Hwaida Saad & Eric Schmitt, *An Eroding Syrian Army Points to Strain*, N.Y. TIMES (Apr. 28, 2015), http://www.nytimes.com/2015/04/29/world/middleeast/an-eroding-syrian-army-points-to-strain.html; Michael Knights, *Iran's Foreign Legion: The Role of Iraqi Shiite Militias in Syria*, WASH. INST. (June 27, 2013) http://www.washingtoninstitute.org/policy-analysis/view/irans-foreign-legion-the-role-of-iraqi-shiite-militias-in-syria.

169. *See, e.g.*, Kirk H Sowell, *The Rise of Iraq's Militia State,* CARNEGIE ENDOWMENT INT'L PEACE: SADA (Apr. 23, 2015), http://carnegieendowment.org/sada/?fa=59888. Sowell notes that Iraqi Prime Minister Nouri al-Maliki created an umbrella organization for the militias, offering volunteers roughly $750 per month without any "legal basis for doing so aside from his constitutional office as commander-in-chief." *Id.*; *see also* Bill Roggio & Amir Toumaj, *Iraq's Prime Minister Establishes Popular Mobilization Forces as a Permanent 'Independent Military Formation,'* FDD'S LONG WAR J. (July 28, 2016), http://www.longwarjournal.org/archives/2016/07/iraqs-prime-minister-establishes-popular-mobilization-front-as-a-permanent-independent-military-formation.php. Examples of unlawful delegations of governmental authority are not confined to Iraq and Syria. For instance, in the United States, allegations have been made of state officials acting "off the books" by hiring contractors to carry out public functions. *See, e.g.*, Dexter Filkins & Mark Mazzetti, *Contractors Tied to Effort to Track and Kill Militants*, N.Y. TIMES (Mar. 14, 2010), http://www.nytimes.com/2010/03/15/world/asia/15contractors.html.

170. The conduct of the Popular Mobilization Forces prior to 2016 may also not be attributable to Iraq under Article 8 ARSIWA due to a reported absence of state control over the militia's activities. *See, e.g.*, Farah Najjar, *Iraq's Second Army: Who Are They, What Do They Want?*, AL JAZEERA (Oct. 31, 2017), http://www.aljazeera.com/news/2017/10/iraq-army-171031063012795.html.

171. Eichensehr, *supra* note 32, at 510.

likely in cases where private hackers carry out state-sponsored malicious cyber activity.[172] The relationship that exists between such actors and the state is frequently nebulous and ill understood. Moreover, non-state cyber operators take numerous guises, ranging in character from autonomous patriotic hackers to entities acting in complete dependence on the state that amount to *de facto* state organs.[173] Within China, for example, the environment is complex. Private individuals, companies, and civilian agencies are all involved in cyber activity for the benefit of the state, but the level of government involvement in their actions ranges from mere tolerance to government control.[174] In such circumstances, even if it is possible to establish that a state empowered a particular hacker group to act, the likelihood of proving that it was done in accordance with the state's domestic law appears extremely slim.

B. The "Legal" Aspect of the Empowerment Requirement

The requirement for legal empowerment thus imposes "a substantial restriction on the scope of the rule of attribution [set out in Article 5] by excluding acts whose attribution to the State was not permitted by internal law."[175] This constraint does not accord well with the overall aims of the law

---

172. *See, e.g.*, MAURER, *supra* note 26, at 16-18. Maurer divides non-state actors operating on behalf of a state in the cyber domain into three categories: (1) individual actors; (2) groups of people that are organized informally and as a networked structure; and (3) more formal, organized groups of people and hierarchical organizations. While the third category includes private companies that may enter into a contractual relationship with the state, the first two categories encompass cyber criminals and individual hackers with whom the state is less likely to conclude a formal contract in accordance with its internal laws.

173. *See, e.g.*, Yoon, *supra* note 27 (discussing how "cyber warriors" train within North Korea to operate undercover in third countries). With regard to patriotic hackers acting against Estonia in 2007, *see* ENEKEN TIKK ET AL., INTERNATIONAL CYBER INCIDENTS: LEGAL CONSIDERATIONS 23 (2010), http://ccdcoe.org/ publications/books/legalconsiderations.pdf. *See also* Levi Gundert, Sanil Chohan & Greg Lesnewich, *Iran's Hacker Hierarchy Exposed*, RECORDED FUTURE (May 2018), http://go.recordedfuture.com/hubfs/reports/cta-2018-0509.pdf (assessing Iran's use of "a network of people unofficially associated with the IRGC and the Iranian government" to carry out cyber operations on the state's behalf).

174. Mara Hvistendahl, *China's Hacker Army*, FOREIGN POL'Y (Mar. 3, 2010), http://foreignpolicy.com/ 2010/03/03/chinas-hacker-army/; MAURER, *supra* note 26, at 107-19; KREKEL *supra* note 28, at 33 ("Since approximately 2002, the [People's Liberation Army (PLA)] has been creating [information warfare] militia units comprised of personnel from the commercial IT sector and academia, and represents an operational nexus between PLA [cyber network] operations and Chinese civilian information security (infosec) professionals."); RAUD *supra* note 28, at 26-27 (noting that the cyber militias consist of over eight million "hackers, IT companies, scientists, network engineers, foreign language speakers, and others with useful skills . . . the extent of the cyber militias' connections and accountability to the government and the PLA remains unclear . . ."); FIREEYE, INC., *supra* note 28, at 15 ("[T]he 72 groups we have observed are based in China or otherwise support Chinese interests, although we question whether there is much consistency in the level of state direction or support that each of these groups may receive from the Chinese Government.").

175. *Summary Records of the 2553rd Meeting*, *supra* note 9, at 236, ¶ 23 (comments of Mr. Herdocia Sacasa).

of state responsibility. While the ARSIWA commentary acknowledges the relevance of internal law in assessing responsibility,[176] it also emphasizes the primacy of international law.[177] Moreover, the focus of international law is upon the reality of a situation, rather than the apparent structures created by a state's domestic law.[178] Thus, in the words of the Appeals Chamber of the International Criminal Tribunal for the Former Yugoslavia (ICTY), "[S]tates are not allowed on the one hand to act *de facto* through individuals and on the other to disassociate themselves from such conduct when these individuals breach international law."[179] Although the ICTY's observation related to attribution pursuant to Article 8, the ARSIWA commentary highlights the overarching principle that "states cannot use their internal law as a means of escaping international responsibility."[180]

It would be anomalous if the same theory did not apply to the role of internal law within the terms of Article 5. As illustrated by the example of the Shabbiha, a state should not be able to delegate elements of its governmental functions in a manner that does not accord with the requirements of its domestic law and thereby evade international responsibility for any unlawful acts committed by that entity. Instead, there is force in the argument made by the government of Japan that "an internal law is only a presumptive factor in determining whether an act of an entity is attributed to the State."[181] Under this rationale, the definitive factor is the exercise of elements of governmental authority. Therefore, the state should bear responsibility where outsourcing is carried out contrary to, or in the

176. ARSIWA, *supra* note 3, art. 3 commentary, ¶ 8.

177. *See, e.g.*, ARSIWA, *supra* note 3, art. 3 ("The characterization of an act of a State as internationally wrongful is governed by international law. Such characterization is not affected by the characterization of the same act as lawful by internal law."). *See also* art. 3 commentary, ¶ 8 (asserting that "where issues of internal law are relevant to the existence or otherwise of responsibility . . . it is international law which determines the scope and limits of any reference to internal law").

178. Différend Dame Mossé, 13 Rep. of Int'l. Arbitral Awards, 486, 493 (Fr.-It. Concil. Comm'n 1953) http://legal.un.org/docs/?path=../riaa/cases/vol_XIII/486-500.pdf&lang=O ("The internal organization to which the international juridical system refers is that which in fact really exists within the State. In that connection, international law does not consider as the organization that which should exist, according to internal rules, but that which does exist, effectively and positively."). *See also* Prosecutor v. Tadić, Case No. IT-94-1-A, Appeals Chamber Judgment, ¶ 121 (Int'l Crim. Trib. for the former Yugoslavia July 15, 1999) ("[T]he whole body of international law on State responsibility is based on a realistic concept of accountability, which disregards legal formalities and aims at ensuring that States entrusting some functions to individuals or groups of individuals must answer for their actions . . . .").

179. Prosecutor v. Tadić, Case No. IT-94-1-A, Appeals Chamber Judgment, ¶ 117 (Int'l Crim. Trib. for the Former Yugoslavia July 15, 1999) ¶ 117. *See also* Yeager v. Iran, 17 Iran-U.S. Cl. Trib. Rep. 92 ¶ 45 (1987) ("Under international law Iran cannot, on the one hand, tolerate the exercise of governmental authority by revolutionary 'Komitehs' or 'Guards' and at the same time deny responsibility for wrongful acts committed by them.").

180. ARSIWA, *supra* note 3, art. 3 commentary, ¶ 8.

181. Comments and Observations Received from Governments, *supra* note 64, at 48-49 (noting that the Japanese government suggested deleting the wording "by the law of that State" from the draft article).

absence of, authorizing national laws on the basis that it has either interpreted its domestic legal regime to allow for the delegation, or it has knowingly derogated from such laws.[182]

Such a loosening of the requirement for legal empowerment does not align with the wording of Article 5 ARSIWA, but is nevertheless consistent with certain case law on the issue, as well as the earlier work of the ILC.[183] In particular, in the *Armed Activities* and *Bosnian Genocide* cases, the International Court of Justice failed to mention any need for empowerment through domestic law in the context of Article 5.[184] Similarly, the ILC did not initially consider legal empowerment to be a prerequisite for attribution, emphasizing the significance of the public nature of the functions carried out by the private entity as opposed to the formal relationship between that entity and the state.[185] As Special Rapporteur Ago stated in the ILC's third report on state responsibility in 1971, "[I]t is logical that the act of a private person who, in one way or another, is performing a function or task of an obviously public character should be considered as an act attributable to the community and should engage the responsibility of the state at the international level."[186]

In the report, Ago referred to certain case law supporting this proposition.[187] For example, the *Zafiro* case concerned the attribution to the United States of certain acts performed by the crew of a merchant vessel. The Arbitral Tribunal held that "the liability of the State for [the *Zafiro*'s] actions must depend upon the nature of the service in which she is engaged and the purpose for which she is employed."[188] Irrespective of the legal regime under which the vessel operated, the Tribunal concluded that it functioned as a supply ship for the U.S. navy, under the command of the officer on board.[189] Therefore, by virtue of the "nature of service and

182. CAMERON & CHETAIL, *supra* note 58, at 169-70.

183. *Third Rep. on State Responsibility*, *supra* note 71, at 264 ¶ 191.

184. Armed Activities on the Territory of the Congo (The Democratic Republic of the Congo v. Uganda), Judgment, 2005, ¶ 160 (Dec. 19), http://www.icj-cij.org/files/case-related/116/116-20051219-JUD-01-00-EN.pdf ("In the view of the Court, the conduct of the MLC was not that of 'an organ' of Uganda (Art. 4 [ARSIWA]), nor that of an entity exercising elements of governmental authority on its behalf (Art. 5)"); Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosn. & Herz. v. Serb. & Montenegro), Judgment, 2007 I.C.J. Rep. 43, ¶ 414 (Feb. 26) ("The acts constituting genocide were not committed by persons or entities which, while not being organs of the FRY, were empowered by it to exercise elements of the governmental authority (Art. 5) . . . .").

185. *Third Rep. on State Responsibility*, *supra* note 71, at 264, ¶ 191.

186. *Id.*

187. *Id.* at 264, ¶ 192.

188. Earnshaw (Gr. Brit.) v. United States, 6 Rep. of Int'l Arbitral Awards, 160, 162 (Am.-Brit. Cl. Arb. Trib. 1925), http://legal.un.org/docs/?path=../riaa/cases/vol_VI/160-165_Earnshaw.pdf&lang=E.

189. The Tribunal's conclusion as to attribution was not based upon the level of control exercised by the officer on board over the activities of the crew. Instead, the Tribunal found that the United States was "highly culpable to let this particular crew go ashore without effective control in

purpose for which [the vessel was] employed," the United States was responsible for the crew's actions.[190]

The draft article formulated by Special Rapporteur Ago in 1971 to express this principle made no reference to any requirement for the entity exercising public functions to be empowered by the law.[191] When, three years later, the wording of the draft article changed to incorporate a requirement for legal empowerment, the ILC did not clearly express the basis for this amendment, or cite any precedents in its support.[192] The requirement appears to be grounded in the fact that entities exercising elements of governmental authority normally do so pursuant to a delegation under the state's domestic law, while situations involving a lesser means of empowerment are adequately covered by Article 8.[193] However, the conduct

---

circumstances prevailing at the time." *Id.* at 160, 163. *See also Third Rep. on State Responsibility*, *supra* note 71, at 264, ¶ 192.

190. Earnshaw (Gr. Brit.) v. United States, 6 R.I.A.A. 160, 160 (Am.-Brit. Cl. Arb. Trib. 1925).

191. *Third Rep. on State Responsibility*, *supra* note 71, at 267. Draft article 8 provides:

> The conduct of a person or group of persons who, under the internal legal order of a State, do not formally possess the status of organs of that State or of a public institution separate from the State, but in fact perform public functions or in fact act on behalf of the State, is also considered to be an act of the State in international law.

192. *Report of the Commission to the General Assembly*, [1974] 2 Y.B. Int'l L. Comm'n 157, 277, U.N. DOC. A/CN.4/SER.A/1974/ADD.1 (PART ONE), http://legal.un.org/ilc/publications/yearbooks/english/ilc_1974_v2_p1.pdf. Draft article 7(2) provided that:

> The conduct of an organ of an entity which is not part of the formal structure of the State or a territorial government entity, but which is empowered by the internal law of that State to exercise elements of the governmental authority, shall also be considered as an act of the State under international law, provided that organ was acting in that capacity in the case in question.

See also id. at 282, ¶ 18 (providing commentary to draft article 7).

> The justification for attributing to the State, under international law, the conduct of an organ of one or other of the entities here considered still lies, in the final analysis, in the fact that the internal law of the State has conferred on the entity in question the exercise of certain elements of the governmental authority.

In their comments regarding the earlier draft of the article, certain members of the International Law Commission referred to the "exceptional" nature of the situations contemplated by the article and a need for the rule to be suitably circumscribed, but they did not set out any clear basis for the requirement that an entity should be "empowered by the law." *See, e.g.*, *Summary Records of the 1258th Meeting*, *supra* note 152, at 36, ¶ 33 (comments of Mr. Tsuruoka); *Summary Records of the 1259th Meeting*, *supra* note 152, at 38, ¶ 13 (comments of Mr. Pinto).

193. *See First Rep. on State Responsibility*, *supra* note 64, at 56 (art. 7 commentary ¶ 4).

> The reference to internal law was deleted from article 5 [the predecessor to article 4] . . . and there is a case for doing the same in relation to article 7. On balance, however, the reference to internal law has been maintained. By definition, these entities are not part of the formal structure of the State, but they exercise governmental authority in some respect; the usual and obvious basis for that exercise will be a delegation or authorization by or under the law of the State. The position of separate entities acting in fact on behalf of the State is sufficiently covered by article 8.

See also Summary Records of the 2555th Meeting, 1 Y.B. Int'l L. Comm'n 241, 246, ¶ 35, U.N. DOC. A/CN.4/SER.A/1998, http://legal.un.org/ilc/publications/yearbooks/english/ilc_1998_v1.pdf.

> The reference to internal law in paragraph 2 of article 7 should be retained owing to the exceptional nature of the situations addressed, which was flagged earlier in the article, and

of militias such as the Shabbiha and Iraq's PMF demonstrates an accountability gap often left unaddressed by Article 8, due to insufficient evidence to prove the existence of state instruction, direction, or control in relation to the entity's activities.

In light of the above, it is arguable that the requirement for legal empowerment included within the ILC's formulation of Article 5 is not reflective of customary international law.[194] This conclusion is supported by the Customary International Law Study completed by the International Committee of the Red Cross, according to which, "A State is responsible for violations of international humanitarian law attributable to it, including: . . . (b) violations committed by persons or entities it empowered to exercise elements of governmental authority."[195] Again, there is no stipulation that the requisite empowerment must be effected by a state's domestic law. In the absence of such a requirement, it follows that all forms of state authorization, whether they accord with the domestic legal regime or not, should be taken into account when considering whether the state has empowered a private entity to perform governmental functions.[196] Evidence of such empowerment may include the provision of training or equipment to the non-state actor concerned, such as authorization to use cyber tools developed by the state, or the issuance of instructions or inducements in relation to the exercise of the relevant public functions.

If one accepts this principle, there is nevertheless a need to consider how far it should extend. State empowerment remains a clear requirement of the attribution standard, implying a necessity for positive action by the state in delegating public functions, rather than a mere failure to prevent the exercise of such powers. Accordingly, evidence of a clear link between the state and the private entity must exist; mere performance of governmental

---

> all the situations in which a non-State entity was not authorized by internal law would then come under article 8.

(statement of Mr. James Crawford).

194. Neither the ICJ, nor any other international court or tribunal, has commented upon the customary nature of Article 5 ARSIWA. When the ICJ referred to Article 5, it made no mention of any requirement for the entity to be empowered by the law of the state. *See supra* note 164. There is little state practice or *opinio juris* to demonstrate states' views regarding this basis of attribution. Governments did not raise objections to draft Article 5 as a whole, although several states sought greater clarification as to its terms. *See First Rep. on State Responsibility*, *supra* note 64, at 38-39; Comments and Observations Received from Governments, *supra* note 64, at 48-49.

195. 1 CUSTOMARY INTERNATIONAL HUMANITARIAN LAW 530-36 (Jean-Marie Henckaerts & Louise Doswald-Beck eds., 2005) (Rule 149).

196. Such a conclusion seems to be supported by certain comments made by Crawford in 1998. *See Summary Records of the 2555th Meeting*, *supra* note 193, at 243, ¶ 12.

> Article 7 was necessary because of the number of entities which were not organs of the State but exercised State functions, for example, private airlines which exercised functions in connection with immigration. Internal law was certainly the most important factor *but it was not the only one, and sometimes even the practice could be more relevant than the texts.*

(emphasis added).

functions without such evidence will not give rise to attribution.[197] To illustrate, consider the position of a company that takes steps to defend its computer networks through "hacking back."[198] Although such activity is unlawful within the United States, one commentator suggested that "the [U.S.] legal authorities might end up simply turning a blind eye to companies' cyber defenses, even when they appear to cross the line."[199] Indeed, reporting indicates that such activity may be occurring already.[200] If a company's "hack back" activities fall within the scope of governmental authority, and the state, despite being aware of such activities, takes no steps to prosecute or to bring an end to the conduct, this alone would not amount to an empowerment by the state. Instead, such activity would potentially breach the state's obligations to exercise due diligence with regard to activities occurring on its territory that may adversely affect other states.[201] In such circumstances, the legal consequences that flow from a state's breach of its due diligence obligations are likely less severe than if the state bears responsibility for the offending "hack back" activity itself.[202]

---

197. The attribution standard reflected in Article 5 ARSIWA relates to the conduct of private entities authorized by the state to exercise governmental authority. *See* ARSIWA, *supra* note 3, art. 5 commentary, ¶ 7. In contrast, Article 9 ARSIWA deals with the attribution to the state of the conduct of private entities exercising governmental functions in the absence or default of the official authorities. *See id.* art. 9.

198. *See supra* Part III for further discussion of "hacking back."

199. Hannah Kuchler, *Cyber Insecurity: Hacking Back*, FIN. TIMES (July 27, 2015), http://www.ft.com/content/c75a0196-2ed6-11e5-8873-775ba7c2ea3d (referring to comments made by Benjamin Wittes, Senior Fellow, Brookings Institution).

200. *See, e.g.*, Craig Timberg, Ellen Nakashima & Danielle Douglas-Gabriel, *Cyberattacks Trigger Talk of 'Hacking Back,'* WASH. POST (Oct. 9, 2014), http://www.washingtonpost.com/business/technology/cyberattacks-trigger-talk-of-hacking-back/2014/10/09/6f0b7a24-4f02-11e4-8c24-487e92bc997b_story.html.

201. *See* TALLINN MANUAL 2.0, *supra* note 25, at 30-43 (Rule 6 provides that "[a] State must exercise due diligence in not allowing its territory, or territory or cyber infrastructure under its governmental control, to be used for cyber operations that affect the rights of, and produce serious adverse consequences for, other States.").

202. A state's failure to comply with the principle of due diligence is an internationally wrongful act involving legal consequences, including an obligation on the responsible state to make full reparation for any injury caused and a right of the injured state to take countermeasures. *See* ARSIWA, *supra* note 3, pt. 2 (Content of the International Responsibility of a State) and pt. 3 (The Implementation of the International Responsibility of a State). In the case of a due diligence violation, the relevant breach of international law is the state's failure to take all feasible measures to put an end to cyber operations that affect a right of, and produce serious adverse consequences for, other states. *See* TALLINN MANUAL 2.0, *supra* note 25, r. 7, at 43-50. In contrast, if the conduct of a company undertaking "hack back" activity is attributable to the state pursuant to Article 5 (or any other basis of attribution), the state bears responsibility for any breach of its international law obligations resulting from the "hack back" activity, such as a violation of the prohibition of intervention. *See* TALLINN MANUAL 2.0, *supra* note 25, r. 66, at 312-25. In such circumstances, the legal consequences for the responsible state are likely to be more severe than those resulting from a due diligence violation. In particular, the reparation for injury is likely to be more significant, and stricter countermeasures are likely to be considered proportionate in the circumstances. Further discussion regarding the scope of states' due diligence obligations, or the legal consequences of an internationally wrongful act, is beyond the scope of this article.

The boundaries of empowerment may, however, be more difficult to ascertain in cases where a private entity takes the lead in conducting the relevant activity, but does so with governmental assistance. For example, when the cybersecurity firm Mandiant publicly attributed certain instances of cyber espionage and data theft to China in 2013, it reportedly did so with the benefit of intelligence provided by the U.S. government.[203] Whether such state assistance amounts to empowerment is case-specific, and a question of fact. However, the more a private entity depends on government intelligence or assistance to perform the relevant function, the greater the likelihood such a backing amounts to an empowerment by the state.

V. ULTRA VIRES ACTS

Once it is determined that a state has empowered a private entity to exercise elements of its governmental authority, the third criterion for attribution under Article 5 ARSIWA requires that the entity was, in fact, acting in that capacity at the time it committed the act in question. As previously noted, there is no additional requirement for the state to direct the way in which a delegated task is carried out.[204] Instead, the public powers exercised by a private entity may involve "an independent discretion or power to act,"[205] meaning that the entity makes its own decisions with regard to when and how it acts, without governmental oversight. If the entity exceeds its authority, the state nevertheless bears responsibility for its activities provided the entity was performing the relevant public function at the time the act in question was committed.

This aspect of Article 5 is reflected in Article 7 ARSIWA, which provides that:

> The conduct of an organ of a State or of a person or entity empowered to exercise elements of the governmental authority shall be considered an act of the State under international law if the organ, person or entity acts in that capacity, even if it exceeds its authority or contravenes instructions.[206]

Thus, state responsibility may arise even if the entity's conduct was *ultra vires*, meaning that it was carried out either in excess of its authority or in contravention of any instructions given by the state. But this principle holds true only if, during the incident in question, the entity was performing

203. Eichensehr, *supra* note 32, at 490.
204. *See supra* Part II.
205. ARSIWA, *supra* note 3, art. 5 commentary, ¶ 7.
206. ARSIWA, *supra* note 3, art. 7.

governmental functions. It is therefore necessary to draw a distinction between conduct that is deemed "official," in exercise of the delegated public functions, and that which is "private," and carried out either in an entity's personal capacity or on behalf of a client other than the state.

This distinction is illustrated by abuses committed by contractors working for PMSCs. Commentators have raised considerable concerns regarding the issue of accountability for legal breaches involving PMSCs, such as the detainee abuse at Abu Ghraib.[207] When working in combat zones, contractors have also been involved in numerous incidents involving civilian deaths. Examples include the killing of seventeen Iraqis by Blackwater employees escorting a U.S. Department of State convoy.[208] Despite the frequency with which PMSC misconduct occurs, it is rare for such activity to be authorized by the hiring state.[209] It is therefore necessary to determine whether the abuses committed were private acts that are not attributable to the state or *ultra vires* activities carried out in the contractor's official capacity that lead to state responsibility.

The determination as to whether particular conduct relates to the exercise of governmental authority is a question of fact in each case.[210] As the ARSIWA commentary makes clear, "If it is to be regarded as an act of the State for purposes of international responsibility, the conduct of an entity must . . . concern governmental activity and not other private or commercial activity in which the entity may engage."[211] A clear disaggregation of the activities carried out by an entity assists in this respect. It must then be determined whether the act in question was connected to the performance of public functions, or to another task carried out either for the state, or for another beneficiary.

---

207. *See, e.g.*, Mark W. Bina, *Private Military Contractor Liability and Accountability after Abu Ghraib*, 38 J. MARSHALL L. REV. 1237 (2005); Laura A. Dickinson, *Governments for Hire: Privatizing Foreign Affairs and the Problem of Accountability under International Law*, 47 WM. & MARY L. REV. 135 (2005); Nigel D. White, *Due Diligence Obligations of Conduct: Developing a Responsibility Regime for PMSCs*, 31 CRIM. JUST. ETHICS 233 (2012); Stanger, *supra* note 89.

208. In 2014, a federal jury found one of the contractors guilty of first-degree murder and a further three contractors guilty of voluntary manslaughter and attempted voluntary manslaughter. One of the convictions was subsequently overturned. *See* Matt Apuzzo, *In Blackwater Case, Court Rejects a Murder Conviction and Voids 3 Sentences*, N.Y. TIMES (Aug. 4, 2017), http://www.nytimes.com/2017/08/04/world/middleeast/blackwater-contractors-iraq-sentences.html.

209. *See* Youmans (U.S.) v. United Mexican States, 4 R.I.A.A. 110, 116 (Gen. Cl. Comm'n 1926), http://legal.un.org/riaa/cases/vol_IV/110-117.pdf. When considering the application of the *ultra vires* principle to state organs, the Commission stated, "Soldiers inflicting personal injuries or committing wanton destruction or looting always act in disobedience of some rules laid down by superior authority. There could be no liability whatever for such misdeeds if the view were taken that any acts committed by soldiers in contravention of instructions must always be considered as personal acts."

210. ARSIWA, *supra* note 3, art. 7 commentary, ¶¶ 7-8.

211. ARSIWA, *supra* note 3, art. 5 commentary, ¶ 5.

Where a company acts pursuant to private contracts, entirely distinct from the public functions performed for the state, such conduct will not give rise to state responsibility.[212] Therefore, if a PMSC provides armed security to protect a military base in a combat zone as well as security services for a mineral extraction company operating in the region, only its activities in relation to the former are attributable to the state. Similarly, if a cybersecurity company that is empowered to conduct cyber defense of military networks also performs information security services for private clients, its conduct in respect of the latter is not attributable to the state.[213]

Activities carried out in a contractor's personal capacity likewise do not engage the state's responsibility. To be considered private in nature, the relevant conduct must be "so removed from the scope of [the individual's] official functions that it should be assimilated to that of private individuals, not attributable to the State."[214] Accordingly, an offence committed by a PMSC contractor when he is off duty, not in uniform and away from his place of work is unlikely to engage the responsibility of the state. Equally, if the employees of a cybersecurity company performing digital forensics functions on behalf of the state engage in activities that are unrelated to the government mandate, such as cybercrime, then the state bears no responsibility in respect of their conduct.[215]

Where, however, the conduct in question is "carried out by persons cloaked with governmental authority"[216] then it is attributable to the state, even if it exceeds the scope of the delegated powers. For example, interrogators working for CACI International Inc. at Abu Ghraib engaged in detainee abuse that included beatings, starvation, sexual violations, and sleep deprivation.[217] While such activities were not authorized by the U.S. government and may have specifically been prohibited under the terms of the contract, they were undoubtedly carried out in the exercise of delegated governmental authority.[218] This is because the abuses were incidental to the contractors' official role as interrogators within the prison. On this basis, therefore, the abuses committed by private contractors at Abu Ghraib in 2003 are attributable to the United States.[219] The same reasoning applies to the killings in Baghdad's Nisour Square by Blackwater employees,

212. *Id.* art. 7 commentary, ¶ 7.

213. TALLINN MANUAL 2.0, *supra* note 25, ¶ 11 (discussing Rule 15).

214. ARSIWA, *supra* note 3, art. 7 commentary, ¶ 7.

215. TALLINN MANUAL 2.0, *supra* note 25, ¶ 12 (discussing Rule 15).

216. ARSIWA, *supra* note 3, art. 7 commentary, ¶ 7 (citing Petrolane, Inc. v. Iran, Iran-U.S. C.T.R., vol. 27, 64 at 92 (1991)).

217. *See* Weiner, *supra* note 2.

218. TONKIN, *supra* note 46, at 113.

219. *Id.*

committed while the contractors were acting in their official capacity, providing convoy security.[220]

Equivalent considerations apply in the cyber domain. Thus, the Tallinn Manual 2.0 gives the example of a state that empowers a private company to use passive measures in defense of its governmental cyber infrastructure.[221] If the company then engages in active defense, by "hacking back" in excess of the delegated governmental authority, such *ultra vires* conduct is attributable to the state, as it is incidental to the company's activities in defending the government networks.[222]

Such distinctions between public and private acts are not always clear-cut. The United Kingdom government, for example, raised a query with the ILC regarding the conduct of a private security firm empowered to act as railway police.[223] The facts of that example may equally be applied to a PMSC that is authorized to use force in guarding a facility within a military base in a combat zone. Consider the position if one of the contractors working for the PMSC acts, whilst in uniform, in excess of the authority granted by the state by using force to detain an individual whose conduct does not threaten the security of the facility, at a location not in its immediate vicinity. The question arises as to whether that would be an example of an *ultra vires* act attributable to the state, or an act committed in the individual's private capacity. Further information would be required to determine whether the contractor was "purportedly or apparently carrying out [his] official functions"[224] at the time of the incident. If at the relevant time he was on duty and relied upon his uniform or the appearance of authority that this bestowed upon him when detaining the individual, thereby giving the impression that he was acting in his official capacity, then his actions are likely to be attributable to the state.[225] If, however, he was off duty and detained the individual with no reliance whatsoever upon his

220. *See, e.g.*, Apuzzo, *supra* note 208.

221. TALLINN MANUAL 2.0, *supra* note 25, ¶ 12 (discussing Rule 15).

222. *Id.*

223. *Comments and Observations Received from Governments*, [1998] 2 Y.B. Int'l L. Comm'n 81, 109, ¶ 4, U.N. Doc. A/CN.4/SER.A/1998/Add.1 (Part 1). If one of the employees of the private security firm acted, while in uniform, in excess of the authority granted by the state by arresting a suspected criminal (whose crime had nothing to do with the railway) in a place near to but not within the railway station, the U.K. government queried whether that would be an example of an *ultra vires* act attributable to the state, or an act committed in the individual's private capacity.

224. ARSIWA, *supra* note 3, art. 7 commentary, ¶ 8.

225. *See* Estate of Caire (Fr.) v. United Mexican States 5 R.I.A.A. 516 (Fr.-Mex. Cl. Comm'n 1929). The Claims Commission found that Mexico was internationally responsible for the acts of two of its Army officers who shot a French national after he refused to give the officers a sum of money on the basis that the officers "acted under cover of their status as officers and used means placed at their disposal on account of that status." In particular, the officers used their insignia when carrying out the arrest, thereby giving the appearance of acting in an official capacity.

uniform as an indication of authority, then his actions may be considered those of an ordinary citizen and not attributable to the state.[226]

According to the ARSIWA commentary, the distinction between official and private acts "may be avoided if the conduct complained of is systematic or recurrent, such that the State knew or ought to have known of it and should have taken steps to prevent it."[227] This can, again, be illustrated through the example of the PMSC empowered to guard an installation on a military base. If the contractors working for the PMSC exceed their authority on a regular basis, such that this behavior should come to the attention of the state but the state does nothing to address the matter, then the acts in question are attributable to the state. This is the case even if, on a one-off basis, it is found that the contractor concerned was acting in his private capacity, rather than in the exercise of public powers.[228]

As these examples illustrate, it is not always straightforward to determine whether a private entity is exercising public powers at the time it commits an act potentially engaging the responsibility of the state. This is a question of fact in each case that rests largely on the nexus between the activity concerned and the relevant governmental function. It also depends, to an extent, upon how broadly the notion of an entity's capacity, when acting in the exercise of governmental functions, is construed. Although its application is problematic at times, the rule encompassed in Article 7 ARSIWA is a necessary means to exclude private conduct from the scope of the attribution standard, including under Article 5 ARSIWA. It also ensures that any conduct that is related to a private entity's performance of public functions is potentially attributable to the state.

VI. CONCLUSION

Despite the blurring of the lines between public and private activity in recent years, some functions, such as offensive combat and law enforcement, retain an inherently governmental character. Other conduct that is not quintessentially public in nature may also fall within the scope of governmental authority when viewed through the lens of the "private person" test, or in its wider context. In respect of the latter, it may help to consider factors such as the location in which the relevant activities are carried out and the identity of the persons for whose benefit they are performed. Although such considerations may bring a broader range of functions within the scope of governmental authority, it is only those activities that amount to a breach of the state's international obligations that

226. *Id.*
227. ARSIWA, *supra* note 3, art. 7 commentary, ¶ 8.
228. *Id.*

engage the responsibility of the state. In respect of PMSC conduct, this is far more likely to arise in the context of armed security or functions with a direct operational effect, than it is in relation to tasks performed in support of personnel or equipment, such as maintenance or cleaning.

In the cyber domain, equivalent considerations apply when determining whether a private cyber operator's conduct amounts to an exercise of governmental authority. Cyber activities undertaken in support of military operations, as well as law enforcement functions undertaken by cybersecurity companies, are likely to be governmental in nature. The scope of Article 5 ARSIWA with regard to activities in the cyber domain may thus be wider than commonly perceived. The Tallinn Manual 2.0, for example, includes scenarios within the commentary relating to Article 8 ARSIWA that may equally fall within the scope of Article 5.[229] These involve the defense of government computer networks, offensive cyber operations against another state, or cyber support to ongoing military operations,[230] and as such, are all likely to amount to an exercise of governmental authority, potentially falling within the scope of Article 5.

The activities of a private entity performing governmental functions are attributable to the state provided that the entity acts in its public, as opposed to private capacity when committing the acts in question. Evidence that the state empowered the entity to exercise such functions is also required. When considering the issue of empowerment, a preliminary consideration is whether the relevant powers were delegated in accordance with the state's internal law. In this respect, any form of legal empowerment will suffice, whether this is effected through legislation, regulation, contract, or any other means permitted under the domestic legal regime. In the absence of legal empowerment, however, it is submitted that other forms of state authorization become relevant. Provided the state positively empowered the private entity to act, even in a manner inconsistent with domestic laws, then the pursuant conduct of the entity should be attributable to the state. The contrary conclusion goes against the spirit of ARSIWA and offers an incentive to states to outsource public functions in an illegitimate manner.

A more inclusive interpretation of the basis of attribution reflected in Article 5 is justified in view of the nature of the functions concerned, which are traditionally reserved to the state and frequently affect the rights of individuals. Moreover, this construction of the attribution standard closes, to some extent, the accountability gap that emerges when considering the activities of militia groups such as the Shabbiha, as well as certain operators in the cyber domain. As the rule of attribution reflected in Article 5 does not include any requirement for state supervision of the entity's activities, a

229. TALLINN MANUAL 2.0, *supra* note 25, at 94-100 (Rule 17 commentary).
230. *Id.* ¶¶ 4, 7, 12, 14, at 95-98.

state may bear responsibility for the actions of an entity exercising public functions without proof of state instructions, direction, or control. This is particularly relevant in the contemporary conflict environment, where states are likely to continue acting via proxies for the foreseeable future.

* * *