Cybersecurity and Cyberwarfare as Emerging Gaps in Private Military and Security Company Regulation: Thoughts for the UN Working Group on the Use of Mercenaries

Hin-Yan Liu

Faculty of Law, University of Copenhagen

The broad brief that I received was to provide a comparative analysis and global overview on the national experience of legislation. In preparing for the panel, however, I encountered a repeating theme in the impetus of legislative drives: the focus of regulation was placed upon the provision of *physical* security and military services. This emphasis is readily apparent with the interest of the Working Group on points (e) and (f) of the Concept Note: the rules on the acquisition of weapons and the use of force and firearms. The implicit consideration of physical security is also discernible in many of the other points: for example, (c) and (d) on the selection and training of personnel and permitted and prohibited activities, which voice concerns about excessive use of physical force.[1]

This raised a persistent question in my mind, and I hope that I would not be overstepping my brief to introduce this concern to the Working Group here. While the national legislative experience in the brief suggests a retrospective account, I have instead looked forward to identify emerging gaps in PMSC legislation. Thus, the question is whether, in seeking to plug the legislative gaps that have emerged from the previous practices of PMSCs, we are blinded to the new activities that PMSCs now engage in, and miss the regulatory implications of these industry transformations.[2] The PMSC industry has demonstrated nimble reaction to market forces in the past. With the increasing importance of the cyber domain as the fifth domain of warfare,[3] the question that I raise here is whether the regulation we are urging upon States actually has the effect of targeting a previous iteration of the PMSC? If this is the case, while we fill the existing legislative gaps, are we in the process of creating the next set of regulatory gaps?

What I hope to do in my remaining time is to sketch out why PMSCs are, and will likely continue to be, in the business of providing military and security services in the cyber domain and the regulatory gaps that continued neglect might create. The initial considerations are, of course, whether these activities fall within the definition of private military and security activities and whether these would fall within the Working Group's mandate. In this context, it is worth noting that the Working Group's definition of military services encompass 'technical support to armed forces and other related activities', and that security services

[1] It may also be that point (g) also follows this vein. The violations at stake within the purview of PMSC activities tend to involve excessive uses of force, especially with regard to human rights concerns.

[2] For an overview of regulatory initiatives regulating the previous iteration of the PMSC, see Sarah Percy, 'Regulating the Private Security Industry: A Story of Regulating the Last War' (2012) 94 International Review of the Red Cross 941.

[3] 'War in the Fifth Domain' [2010] *The Economist* <http://www.economist.com/node/16478792> accessed 16 November 2015.. In May 2010, the US Department of Defense established its new Cyber Command (Cybercom) alongside land, sea, air and space.

include the 'development and implementation of informational security measures and other related activities'. This expansive definition would readily encompass security and military activities in the cyber domain.

PMSCs, like other service industries, will rush to fill profitable gaps that they identify and this will certainly be the case with cybersecurity.[4] Beyond the agility of the PMSC industry to fill in the gaps emergent gaps of the cybersecurity world, structural pressures favour private cybersecurity provision. The high demand, coupled with the limited supply, of upper-tier cybersecurity personnel result in high wages that the public sector and the military will find difficult to match: bureaucratic rules and employment practices may provide further obstacles.[5] As the discrepancy in pay between those who work in the public and private sectors is likely to be quite pronounced, allegations of mercenarism may resurface.

Part of the issue arising out of cybersecurity services, however, is that these are beyond the usual skill set possessed by today's PMSCs. The result is that PMSCs either have to acquire the necessary expertise by buying up existing firms, or they have to monetise the defensive measures that they have developed from when defending themselves from cyberattacks.[6] Yet, because a different industry sector already has greater expertise in the cyber domain, there is the real risk that companies not normally categorised as PMSCs will offer services within the expansive PMSC definition. This creates a serious legislative challenge because parts of the industry may look quite different from the PMSCs that we have become familiar with today, with different players possessing different capabilities and performing different activities. Indeed, it may be that we will have to be on the lookout for seemingly parallel industries, whose activities converge or intersect with military and security concerns in some instances, but which may avoid the designation or treatment as a PMSC. This initial categorisation is critical:[7] the real risk is that companies which engage in military or security activities in the cyber domain will not be treated as PMSCs in legal terms, and thereby avoid the appropriate legislative scrutiny that such activities would justify. Combining these features together, the fear here is these trend will blend together an under regulated PMSC industry with under regulated forms of cyber activity.

---

[4] Personal communication with Christopher Kinsey, 22 November 2015.

[5] There are a number of factors favouring the private provision of cybersecurity: high specialisation and quicker innovation, higher pay and greater autonomy, and lower levels of accountability. See Jesse McMurdo, Cybersecurity Firms — Cyber Mercenaries? (December 12, 2014). Available at SSRN: http://dx.doi.org/10.2139/ssrn.2556412

[6] WJ Hennigan, 'Defense Contractors See Opportunity in Cybersecurity Sector' *LA Times* (21 January 2015) <http://www.latimes.com/business/la-fi-0122-cyber-defense-20150122-story.html> accessed 22 November 2015, see also, Shane Harris, 'The Mercenaries' (12 November 2014) *Slate* <http://www.slate.com/articles/technology/future_tense/2014/11/how_corporations_are_adopting_cyber_defense_and_around_legal_barriers_the.single.html> accessed 17 November 2015.

[7] This perspective on categorisation draws analogies from the argument I have developed elsewhere. This argument proposed that mercenary activities that conducted under the juridical form of the corporation has deflected legal attention and scrutiny because of the formal corporate status and the apparent legitimacy that this provides. See further, Hin-Yan Liu, *Law's Impunity: Responsibility and the Modern Private Military Company* (Hart Publishing 2015) ch 4.

The actual nature of the services offered by PMSCs will be in flux as a reaction to operations in the new domain. The contemporary assertions made by industry advocates that PMSCs engage *only in defensive security operations* may no longer be tenable.[8] This is because the retreat from offering offensive military services occurred in reaction to the lack of market demand, rather than as the result of regulation or external control. In other words, few barriers have been erected against the provision of offensive military services by PMSCs, aside from the dampening of demand in the marketplace.

A quick profile of the cybersecurity industry confirms this concern. Cybersecurity firms are not, and arguably cannot be, merely on the defensive for the simple reason that the cyber domain has been characterised as 'an offense-dominant environment, [in which] a fortress mentality will not work'.[9] Instead, cybersecurity firms are involved with 'active defence', which includes launching pre-emptive or retaliatory strikes.[10] This suggests that offensive operations are necessary, even to maintain a purely defensive posture. Thus, a potential gap is revealed between existing legislation that has been designed to regulate domestic PSCs engaged in defensive security services, and the regulation the emergence of PMSCs operating in the cyber domain.

In this regard, the broad lack of domestic legal provisions which address the direct participation in hostilities is particularly problematic.[11] The urgency to legislate for direct participation in hostilities had dwindled as a result of the recent industry shift towards the provision of security services.[12] Thus, the legislative focus on security provision overlooks the fact that military and security activities in the cyber domain straddle the divides between military and security services, and between defensive and offensive services. At the very least, it is now becoming clear that legislation needs to encompass PMSC capacity for offensive operations and direct participation in hostilities to be effective. Such legislation would also have the benefit of accounting for more traditional PMSC activities.

---

[8] Insofar as the PMSC industry shift towards security provision and away from offering military services is not a result of legislative or regulatory pressures, the inference is that the transition is a response to low market demand and lack of profitability. Were PMSCs to offer offensive military or security services in the cyber domain, this would vindicate my previous assertion that neither structural shifts nor normative boundaries could be deduced from the recent PMSC retreat from offensive capability provision. ibid 107.

[9] William J Lynn, 'Defending a New Domain' (September/October 2010) *Foreign Affairs* <https://www.foreignaffairs.com/articles/united-states/2010-09-01/defending-new-domain> accessed 23 November 2015.

[10] Shane Harris, 'The Mercenaries' *Slate* (12 November 2014) <http://www.slate.com/articles/technology/future_tense/2014/11/how_corporations_are_adopting_cyber_defense_and_around_legal_barriers_the.single.html>

[11] Anton Katz, 'Annual Report 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' (UNHRC 2013) A/HRC/24/45 para 38; Patricia Arias, 'Annual Report 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' (UNHRC 2014) A/HRC/27/50 para 23. Swiss legislation is a notable exception in prohibiting and punishing direct participation in hostilities, 'Annual Report 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' (UNHRC 2015) A/HRC/30/34 para 28 and 35.

[12] Percy (n 2) 945, and 950–3.

The prospect for PMSC personnel to directly participate in hostilities through their activities in the cyber domain may resuscitate more traditional forms of mercenarism.[13] On this note, it seems that cyber military and security professionals could readily fit the definition of a mercenary because specific recruitment, actual participation in hostilities and material motivation would both be more likely to take place in practice, as well as being easier to demonstrate.[14] The high level of technical expertise required to conduct such operations makes it conceivable that individuals will be hired for specific operations.[15] And the high salaries that professionals in the industry are likely to receive raises the prospect of material motivation being reignited.[16] If the doctrinal and interpretive hurdles associated with equating the conduct of cyber-attacks with direct participation in hostilities can be overcome, then there appears to be some urgency to develop legislation to take mercenary activities into account.

Unfortunately, it appears that domestic laws rarely include provisions that regulate mercenary activities as a result of the legacy of the PMSC industry transition towards security provision. A further issue arises from the few legislative models that can be drawn upon as guidance for States seeking to implement effective domestic law. This issue is compounded by the fact that those few States with domestic mercenary provisions had usually been confronted with modern manifestations of mercenary activity themselves, and are unlikely to be neutral with respect to their laws as a result. That these States are disproportionately clustered in the African region, and had gained their experience of mercenarism during the period of decolonisation, suggests that a cautious approach needs to be taken when developing mercenary legislation.

Turning now to national legislation and its ability to regulate these developments, there are the two major issues: first that legislation is retrospective, and second that legislation is introspective. In looking backwards, legislation can provide predictability and stability by remedying issues that have proved to be problematic in the past. Yet, there is a very real risk that legislation will be caught up in filling in old regulatory gaps while the PMSC industry moves forward to exploit new and emerging markets and opportunities.[17] For legislation to be effective, it would need to anticipate at least the general nature of these trends; yet there is little evidence that this is taking place.

---

[13] David Turns, 'Cyber Warfare and the Notion of Direct Participation in Hostilities' (2012) 17 Journal of Conflict and Security Law 279, 294.

[14] ibid. This analysis suggests that this would be the case in 'certain very limited circumstances'. Yet, this assumption is based upon the premises that the required technology and training are widely available. While these claims may be factually correct, however, there is a large difference between the availability of 'complex computer technology... and the ubiquity of information technology' and the actual expertise in conducting such operations, which is likely to remain relatively rare.

[15] Dan Goodin, 'For Hire: Elite "Cyber Mercenaries" Adept at Infecting Windows and Macs' (*Ars Technica*, 25 September 2013) <http://arstechnica.com/security/2013/09/for-hire-elite-cyber-mercenaries-adept-at-infecting-windows-and-macs/> accessed 29 November 2015.

[16] Martin C Libicki, David Senty and Julia Pollak, 'Hackers Wanted: An Examination of the Cybersecurity Labor Market' (RAND Corporation 2014). There may be difficulties in comparing remuneration levels due to the generally attractive salaries that professionals in this sector can expect.

[17] For an outline of the industry's nimbleness and the attendant international regulatory lag, see Percy (n 2).

In looking inwards to govern activity on its territory, legislation may be inadequate to govern activities that fluidly cut across physical borders – this is a concern that has been raised repeatedly in the Working Group's reports on national legislation. Yet, domestic law may have the upper hand when it comes to regulating at least some activities in the cyber domain because the problematic extraterritorial dimension need not become a hindrance. Unlike the provision of more traditional military and security services that require personal physical presence in the field, the personnel engaged in such activities in the cyber domain need not go abroad to render those services. This disaggregating feature of the cyber domain has the potential to collapse the distinctions drawn between home, hiring and host States that has hindered legislative efficacy with the PMSC industry in the past. Thus, domestic law has the potential to play an important role in PMSC regulation in the future if developed appropriately.

In the final few minutes, I would like to raise a final point related to the protection of human rights in this context. To date, only lukewarm human rights concerns have been expressed in reaction to cyberwarfare. Indeed, the human rights community appears to be more alarmed by governmental overreactions to cyber-threats that create incursions into internet freedom.[18] This raises the question as to whether human rights standards would be incorporated into domestic legislation seeking to regulate PMSC activities in the cyber domain at all. And even if human rights protections are contemplated, it may still be that their focus is placed upon issues other protecting the victims. Appropriate legislative provisions to ensure accountability and access to remedies for victims appear a long way off in this context, and this does not take into account the practical hurdles of accountability ascription that are introduced by the cyber domain.

In summary, the constantly shifting nature of the Private Military and Security Company industry makes it a moving target for legislators. That the industry has recently, and visibly, shifted towards the provision of defensive and security services may have had the effect of lulling legislators into a false sense of security. The appearance of the PMSC industry engaging primarily in security tasks may be reinforced by the lack of reports that allege excesses in the use of force and other human rights violations. This upright image of the industry could be reinforced by the various self-regulatory initiatives, which regardless of their actual merit, have the effect of signalling intent to adhere to appropriate standards. This backdrop may leave legislators complacent in relation to the PMSC industry, and makes the situation especially perilous. As PMSCs move to provide services in the cyber domain, two risks converge: first that industry-specific legislation is not up to the task of regulating activities that may amount to direct participation in hostilities, and second that there is a failure to grasp the implications of PMSC activities in the cyber domain that will be the source of future gaps in domestic law.

[18] David P Fiddler, 'Cyberattacks and International Human Rights Law' in Stuart Casey-Maslen (ed), *Weapons Under International Human Rights Law* (Cambridge University Press 2014).