CIGI JUNIOR FELLOWS
POLICY BRIEF
NO. 13 › AUGUST 2014

KEY POINTS

- The lines between civilian and military are increasingly blurred, creating ambiguity under international law when private contractors engage in offensive cyber-security operations on behalf of states. These private security companies (PSCs) are being contracted for cyber security to engage in offensive cyber operations.
- States should not contract PSCs for offensive cyber operations. Recognizing the benefits of cyber-security contracting, a transparent distinction should be established between PSCs and state militaries, whereby private actors would only be involved in defensive and supportive operations.
- The North Atlantic Treaty Organization (NATO) is in a prime position to implement a contracting protocol that delineates appropriate classifications for the tasks and personnel required for private cyber-security contracts. Establishing an oversight organization and submitting a proposal to the International Law Commission (ILC) to consider the roles of private security actors would create greater transparency and accountability for contracting.

CONSULT, COMMAND, CONTROL, CONTRACT: ADDING A FOURTH "C" TO NATO'S CYBER SECURITY

JUSTIN ANSTETT AND REBEKAH PULLEN

INTRODUCTION

Cyberspace has become a top national security priority for many countries. Targeted cyber attacks in 2013 have increased by 91 percent and the number of breaches through cyberspace by 62 percent since the previous year, leading many states to outsource the difficulties and high cost of their cyber-security needs to PSCs (Symantec Corporation 2014). As most advanced industrial states are experiencing increased cyber vulnerabilities, several NATO members are becoming major contractors of cyber-security companies. This brief focuses on the contractual relationships between PSCs and NATO, an intergovernmental organization, as well as states that generate an expanding grey area for the application of international law to offensive cyber operations.

NATO's Consultation, Command and Control Agency (NC3A) plays an instrumental role in the procurement and acquisition of PSCs for technical project management of NATO programs, which now includes contracting cyber security. Awarded by the NC3A, NATO's recent contract with Finmeccanica and Northrop Grumman for its Computer Incident Response Capability (NCIRC) Technical Centre sets a precedent for contracting PSCs for traditionally military operations. Recognizing the precedent set by NATO for contracting cyber security, this brief focuses on the necessary fourth "C" in cyber security: contract.

CIGI JUNIOR FELLOWS POLICY BRIEF SERIES

The CIGI Junior Fellows program at the Balsillie School of International Affairs provides students with mentorship opportunities from senior scholars and policy makers. The program consists of research assistantships, policy brief writing workshops, interactive learning sessions with senior experts from CIGI and publication opportunities. Working under the direction of a project leader, each junior fellow conducts research in one of CIGI's program areas. This series presents those policy briefs that met CIGI's publications standards.

The Balsillie School of International Affairs is an independent academic institution devoted to the study of international affairs and global governance. The school assembles a critical mass of extraordinary experts to understand, explain and shape the ideas that will create effective global governance. Through its graduate programs, the school cultivates an interdisciplinary learning environment that develops knowledge of international issues from the core disciplines of political science, economics, history and environmental studies. The Balsillie School was founded in 2007 by Jim Balsillie, and is a collaborative partnership among CIGI, Wilfrid Laurier University and the University of Waterloo.

BACKGROUND

Cyber security covers both defensive and offensive operations conducted in cyberspace. Defensive operations entail protecting cyber infrastructure, for example through the use of firewalls, encryption and antivirus. Whereas an offensive operation refers to any attempt to damage or destroy cyber information or infrastructure, for example targeted malware attacks (such as Stuxnet), espionage (such as APT1) or hacking (see Table 1). International law does not apply directly to PSCs, though several states and intergovernmental organizations are contracting these companies for cyber security, including offensive cyber operations. However, there is a lack of clarity about accountability, oversight and clear understandings of the rules of engagement for PSCs in cyber operations. PSCs and their employees are not directly accountable or protected when they engage in offensive cyber operations as contracted by a state.

TABLE 1: COMMON CYBER-SECURITY OPERATIONS IN PUBLIC AND PRIVATE SPHERES

	Offence	Defence
Public	• problematic • for example, Stuxnet, APT1	• appropriate • encryption, firewalls
Private	• contentious • active defence (for example, CrowdStrike)	• appropriate • defensive software (for example, antivirus, firewalls, encryption)

Source: Authors.

It is unclear to what degree states are responsible or accountable for the actions of contracted companies engaging in offensive military operations, and the status of employees as civilians (and therefore protected) is not certain or guaranteed. The ambiguity caused by the

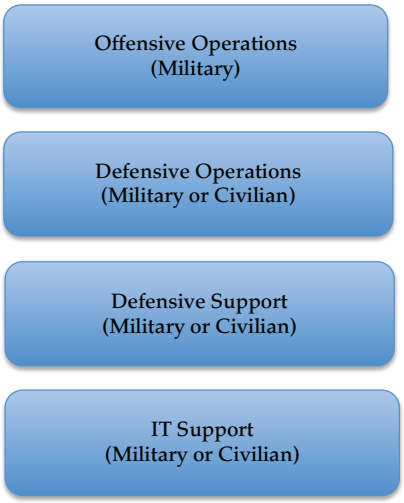
increasing use and capabilities of PSCs in offensive cyber operations is a significant threat to a peaceful cyberspace.

NATO's annual Cooperative Cyber Defence Centre of Excellence conference met June 3–6, 2014. The themed "Active Cyber Defence" conference noted the continually changing perceptions of cyberspace, with specific focus on addressing ambiguities of cyber threats. With the upcoming NATO Information Assurance Symposium in Mons, Belgium, September 16–18, 2014, it is recognized that NATO continues to address contemporary cyber-security issues. However, this brief encourages NATO to address the difficult questions beyond those of developing and implementing any necessary cyber defence capabilities. NATO can continue to be a model of international cooperation by considering the important implications of the blurred lines between "civilian" and "military," precipitated by the unclear status of PSCs under international law.

GROWTH OF CYBER-SECURITY INDUSTRY AND OFFENCE DOMINANCE

States rely increasingly on innovative private sector solutions to protect their critical infrastructure and to enhance their information security. The private sector owns and operates 80 percent of worldwide information infrastructure (NATO 2013). The private sector encompasses the information technology experts who have the skills to develop the most advanced and current cyber security. In 2011, global cyber-security spending reached US$60 billion and is projected to grow 10 percent each year over the next three to five years (PwC 2014, 5). Private cyber-security companies currently provide products and services for cyber security, ranging from engaging in offensive and defensive operations to providing defensive and IT support (see Figure 1).

FIGURE 1: RANGE OF CYBER-SECURITY OPERATIONS



Source: Authors.

One reason for relying on private contractors is due to the knowledge gap between IT experts and policy makers, strategists and often the actual operators of cyber-security mechanisms. In addition, details of actual past attacks and potential future methods are indeterminate. This considerably increases the difficulty of preparing and enacting defences in cyberspace, often leading to diminished confidences in defensive strategies overall. These issues are exacerbated by the incredible speed and advancement of technology. Experts agree that cyber attacks are perpetrated so rapidly that "if you're defending in cyber[space], you're already too late" (Astore 2008).

Accordingly, offensive strategies for cyber security have been advocated by much of the private sector and adopted by many countries' militarized cyber-security forces. This has led companies such as CrowdStrike to develop "active defence" technologies, whereby the response to any detected attack is a counterattack. The relatively low barriers to entry for this offensive technology make this type of behaviour more common globally.

NATO members are among the countries with the fastest growing cyber-security expenditures. Along with several of its member states, NATO has been urgently bolstering capacity for its cyber defences to protect all 50 NATO sites and headquarters across 28 countries. On February 29, 2012, NATO awarded a €50 million contract to Finmeccanica, in partnership with Northrop Grumman, to "develop, implement, and support" the NCIRC. The NCIRC provides the "capability to detect *and respond* to cyber security threats and vulnerabilities rapidly and effectively" (Northrop Grumman 2012, emphasis added).

INTERNATIONAL LAW AND THE PRIVATE PROVISION OF CYBER SECURITY

The application of international law to offensive cyber operations against a state requires clear attribution of the attack to an aggressor. The use of the Internet and other cyber technologies make it difficult to officially assign responsibility to a state or states. Given the existence of offence dominance in cyberspace, states increasingly rely on the private sector for their knowledge, innovation and efficiency in cyber security. However, often excluded from cyber-security contracts are the conditions for appropriate oversight of the contracted company by the state. This is due to poorly defined contracts that do not ensure proper transparency and accountability, as a result of the blurred distinction between private/civilian and public/military. Attributing culpability is therefore further complicated, obscuring the state's responsibility for both the company and the attack. It is difficult to currently determine under what conditions a state has international legal responsibility for the potential offensive cyber actions of its contractors.

If a cyber attack is fully attributable, it can only be permissible if it conforms to both *jus ad bellum* (justice of war) and *jus in bello* (justice in war) requirements. *Ad bellum* regulations dictate when an attack is permissible and the principal document for determining this is the Charter of the United Nations (United Nations 1945). According to Article 2 (4), states are prohibited from threatening or implementing the use of force against another state (ibid.). The only exception is found in Article 51: should an armed attack against a state be attributable to another state, the attacked state may legally retaliate in accordance with the right of self-defence (ibid.).

The Geneva Conventions and Additional Protocols are sources of *in bello* regulations, dictating what kinds of attacks are permissible (International Committee of the Red Cross 1977). Included is the degree of protection of individuals, which is dependent on their classification as civilian, combatant or dual use. The latter applies to objects and locations that are of both military and civilian significance and their protection is adjusted according to the relationship between the military and civilian components.

Cyber-security PSCs are not clearly protected under international law. Their dual-use nature designates them and their employees as non-civilian due to their potential role in offensive operations. However, these companies are not military entities and their employees are not combatants. This ambiguity means that these companies, their employees and installations can be significantly exposed to legitimate attack under international law. Should a company's relationship to the state be misinterpreted, any attack or "active defence" directed against contracted PSCs could lead to war.

Due to a lack of accountability and protection under current international law applicable to contracting for cyber security, NATO should refrain from contracting private companies for offensive cyber operations. PSCs and their employees must not be contracted to function

as combatants for offensive cyber operations, or engage in active defence.

APPROPRIATE RESPONSE

Due to the speed of attacks in cyberspace, there are strong incentives to delegate authority to the private company to decide the appropriate response to the cyber attack, including NATO's contract with Finmecannica and Northrop Grumman. Based on current interpretations, an offensive cyber operation can constitute a response in cyberspace; the private sector refers to these measures as active defence. These private actors are not required to follow pertinent international law and are not bound by political allegiance, although they have the authority and discretion to determine how to respond.

Without direct oversight from state-military officials, private companies should not be able to authorize offensive cyber operations that could lead to military conflict and war. If a cyber-security contractor caused disproportionate damage to the enemy or a contractor's actions were perceived as an act of war it is unclear who is responsible.

Because the right to self-defence permits certain retaliating behaviours, it is highly desirable that any attack against a state be clearly attributable to the responsible party. Right of self-defence responses also depend on accepted interpretations of "defence." Therefore, ambivalence regarding attribution for attacks or "active defence," under international law, creates unnecessary risk. Ambiguity may lead to a confusion of responsibility and potentially short circuit deliberative processes of the attacked state and international community. Consequently, an escalation of reprisals and further attacks becomes more likely.

PRECEDENT FOR STATE RESPONSIBILITY

The ILC's Draft Articles on State Responsibility for Internationally Wrongful Acts reflect existing customary law regarding the "Attribution of Conduct to a State," among other state responsibilities (International Law Commission 2008). In particular, it addresses the need for less ambiguity concerning the relationship between states and organs imbued with state power. An organ of the state refers to a "person or entity" that represents some facet of state power and decision making, "in accordance with the internal law of the State" (ibid., 40). Regulations clarifying the responsibility of such organs under international law, as well as what constitutes a state organ, should be applied to cyber-security contracting.

The Draft Articles have been endorsed by the UN General Assembly (UNGA) multiple times, without vote, most recently in 2013 (UNGA 2013). Additionally, various NATO member states have spoken highly of the Draft Articles. On behalf of the Nordic countries (including NATO members Denmark and Iceland), NATO member state Norway claimed that "the draft articles have...become the most authoritative statement available on questions of State responsibility" (UNGA 2007, 3). The United Kingdom described them as "an authoritative statement of international law," referencing the Articles numerous times for "guidance on issues of State responsibility that arise in day-to-day practice" within the state (ibid., 6).

This demonstrates international support for the encompassed standards of the articles and the support of NATO member states specifically. The organization is in a position to set an example for the international community by taking steps to implement these norms and standards, in reference to offensive cyber operations and the contracting of private security companies. This would inform future policies of states that currently form

contracts with PSCs for offensive cyber operations, as well as for states that may choose to do so in the future as their technological capabilities increase.

As the prevalence of state dependence on cyber technology increases globally, internationally endorsed regulations could operate as best practices. Concerning state responsibility for private contractors, classifying PSCs and their employees as combatants or non-combatants would provide clarification regarding their ambiguous dual-use status. A lack of classification of state responsibility under international law creates ambiguities regarding state control of PSCs. Without recognized control over PSCs, NATO may be liable for the damage, destruction, injury and death done to or caused by the contracted firm and its employees (Schmitt 2012, 288). Moreover, there is risk of costly attacks against PSCs and their employees because of their roles in NATO cyber defence operations.

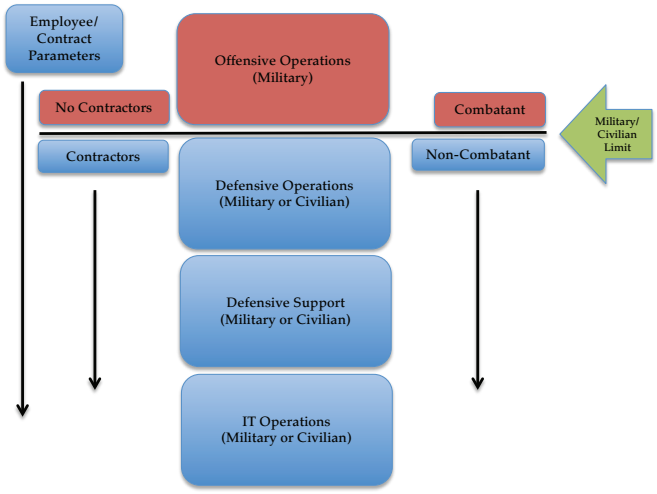
RECOMMENDATIONS

NATO can lead the way for cyber-security contracting by considering the risks associated with blurred lines between private contractors (non-combatants) and military personnel (combatants) engaging in offensive operations. The following recommendations are based on the assumption that once implemented into NATO's cyber defence policy, all of its member states would independently adopt and implement these recommendations into their own national cyber strategies.

NATO should develop a classification protocol for cyber-security contracts that delineates the roles and functions of contracted private security companies, as related to the responsibility of the contracted firm(s), NATO and its member states.

- The North Atlantic Council could create this protocol to classify cyber-security operations into four categories: offensive operations, defensive operations, defensive support and IT support (see Figure 2). Offensive operations should only be carried out by those considered combatants within the military, while defensive and support operations can be carried out by either military or civilian units. To eliminate the dual-use ambiguities, PSCs and their employees should be operationally defined as non-combatants. This scale should clearly define which employees, companies and NATO units should be afforded appropriate protections, in addition to clear accountability in reference to their status under international law as combatants or non-combatants, and as military or civilian objects.

FIGURE 2: CLASSIFICATION PROTOCOL FOR CYBER-SECURITY CONTRACTING



Source: Authors.

NATO should submit all cyber-security contracts to a third-party monitoring and verification organization for review and assessment of the adherence to the classification protocol.

- There should be an oversight mechanism that involves a third-party international organization, ensuring all NATO's cyber-security contracts adhere to the classification protocol. This organization would receive, review and assess the development and implementation of cyber-security contracts, ensuring they were fair, well defined and consistent. It would have the ability to strongly encourage NATO to reassess the classification parameters of a contract. If NATO chooses not to assent to such a recommendation, the organization could publicize its concerns.

- The United Nations Office of Disarmament Affairs (UNODA) has experience in oversight, transparency and confidence-building mechanisms for international security and armed conflict. The UNODA has done research on creating dialogue on the norms, rules, principles and responsible behaviour of states for their actions in cyberspace. It works to develop possible cooperative measures to address and examine the existing and potential threats in cyberspace, and is an example of a possible third-party organization (UNODA 2013).

- The costs associated with establishing a new third-party international oversight organization would be significant. Utilizing a previously established oversight mechanism saves time and resources, as well as increasing greater cooperation across intergovernmental organizations. Oversight mechanisms are often not factored into defence contracting, so NATO should define the costs of oversight within the contract, appropriately balanced between itself and the contracted company.

NATO should encourage its member states to submit proposals to the ILC for consideration, to determine the status of PSCs and their employees engaging in offensive cyber operations, under international law.

- These proposals should comment on the classification protocol used by NATO, as mentioned in our previous recommendation. They should encourage the ILC to consider how a protocol might be translated into broader regulations corresponding to existing international law. In addition, proposals should include the member state's perspective on NATO's use of PSCs since the implementation of the classification protocol.

- The ILC represents the best avenue to translate the classification protocol into a regulatory system, reflecting existing international law. Its connection to the UNGA represents an ideal venue for commentary and endorsement, with prospects for international implementation. The ILC's experience drafting the Articles for State Responsibility and their international support demonstrate that a relationship between it and NATO would be a prudent next step for norms of state responsibility.

- Soft law regulations advocated by the ILC would be better suited for embracing future changes in cyber technology and the nature of offensive cyber operations, as well as less costly than writing new treaties. Such a proposal is a core government task that involves relatively little in the way of external resources. Costs to the ILC are already encompassed by its statute (UNGA 2005).

CONCLUSION

Current difficulties classifying the associated actors under international law could put NATO, contracted PSCs and their employees at risk. By considering the relevant concerns involved in cyber-security contracting to detect

and respond to cyber threats and vulnerabilities, NATO would be in a better position to protect itself, its member states and contracted companies. These recommendations could ameliorate these ambiguities, contributing to accountability and protection for those involved in private cyber-security contracts. By implementing these recommendations, NATO can initiate a framework for clearer and more prudent defence contracting between PSCs and states.

ACKNOWLEDGEMENTS

We would like to express our sincere gratitude to our supervisors Mark Raymond and Samantha Bradshaw for their invaluable leadership, encouragement and guidance throughout the project, and a special thanks to Carol Bonnett and Vivian Moser for their support and assistance during the publication process.

WORKS CITED

Astore, William J. 2008. "Geeks and Hackers, Uncle Sam's Cyber Force Wants You!" *The Nation*, June 5. www.thenation.com/article/geeks-and-hackers-uncle-sams-cyber-force-wants-you.

International Committee of the Red Cross. 1977. "The Geneva Conventions of 1949 and Their Additional Protocols." www.icrc.org/eng/war-and-law/treaties-customary-law/geneva-conventions/.

International Law Commission. 2008. "Draft Articles on Responsibility of States for Internationally Wronful Acts, 2001, with Commentaries." United Nations.

NATO. 2013. "Media Backgrounder: NATO Cyber Defence." NATO, Public Diplomacy Division. www.nato.int/nato_static/assets/pdf/pdf_2013_10-/20131022_131022-MediaBackgrounder_Cyber_Defence_en.pdf.

Northrop Grumman. 2012. *NATO Computer Incident Response Capability.* www.northropgrumman.com/Capabilities/Cybersecurity/Documents/Literature/NATO_CIRC.pdf

PwC. 2014. "Cyber Security M&A: Decoding Deals in the Global Cyber Security Industry." www.pwc.com/gx/en/aerospace-defence-and-security/publications/cyber-security-mergers-and-acquisitions.jhtml.

Schmitt, Michael N. 2012. "'Attack' as a Term of Art in International Law: The Cyber Operations Context." In *2012 4th International Conference on Cyber Conflict*, 283–93. Tallinn: NATO CCD COE Publications.

Symantec Corporation. 2014. "Internet Security Threat Report." Volume 19. www.syman-tec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf

United Nations. 1945. *Charter of the United Nations*. www.un.org/en/documents/charter/.

UNGA. 2005. "Statute of the International Law Commission, 1947." United Nations: UNGA. http://legal.un.org/ilc/texts/instruments/english/statute/statute_e.pdf.

———. 2007. "Responsibility of States for Internationally Wrongful Acts: Comments and Information Received from Governments." March 9: 62/63. General Assembly, Sixty-Second Session. United Nations.

———. 2013. "Resolution Adopted by the General Assembly on 16 December 2013: 68/104. Responsibility of States for Internationally Wrongful Acts." United Nations: UNGA.

UNODA. 2013. "Fact Sheet: Development in the Field of Information and Telecommunications in the Context of International Security." UNODA. www.un.org/disarmament/HomePage/factsheet/iob/Information_Security_Fact_Sheet.pdf.

ABOUT THE AUTHORS

Justin Anstett is a candidate for the University of Waterloo's M.A. in Global Governance at the Balsillie School of International Affairs (BSIA). He completed his B.A. at Wilfrid Laurier University in global studies, specializing in peace and conflict studies. His research explores emerging global security trends, with particular interest in cyber security and private military and security companies. He is currently researching national cyber security strategies and the divergence between cyber programs run by civilian and military departments.

Rebekah Pullen is a candidate for a Master's of Global Governance at the BSIA, based at the University of Waterloo, in Waterloo, Ontario. She has her B. Arts Sc. (honours) with combined honours in political science, from the Arts & Science Program at McMaster University. Her research interests include nationalism and military culture, international law and cyber security.

ABOUT CIGI

The Centre for International Governance Innovation is an independent, non-partisan think tank on international governance. Led by experienced practitioners and distinguished academics, CIGI supports research, forms networks, advances policy debate and generates ideas for multilateral governance improvements. Conducting an active agenda of research, events and publications, CIGI's interdisciplinary work includes collaboration with policy, business and academic communities around the world.

CIGI's current research programs focus on three themes: the global economy; global security & politics; and international law.

CIGI was founded in 2001 by Jim Balsillie, then co-CEO of Research In Motion (BlackBerry), and collaborates with and gratefully acknowledges support from a number of strategic partners, in particular the Government of Canada and the Government of Ontario.

Le CIGI a été fondé en 2001 par Jim Balsillie, qui était alors co-chef de la direction de Research In Motion (BlackBerry). Il collabore avec de nombreux partenaires stratégiques et exprime sa reconnaissance du soutien reçu de ceux-ci, notamment de l'appui reçu du gouvernement du Canada et de celui du gouvernement de l'Ontario.

For more information, please visit www.cigionline.org.

CIGI MASTHEAD