CARI /

Instituto de Seguridad Internacional y Asuntos Estratégicos

BOLETÍN DEL ISIAE

Noviembre 2015

Número 62

CARI
Consejo Argentino para las Relaciones Internacionales

Presidente
Adalberto Rodríguez Giavarini

ISIAE
Instituto de Seguridad Internacional y Asuntos Estratégicos

Director
Julio A. Hang

Secretario de Redacción
Lic. Alejo M. Ferrandi Aztiria

Contacto
difusionrdnisiae@gmail.com

Web
http://www.cari.org.ar/organos/isiae.html

Uruguay 1037, piso 1º
C1016ACA
Buenos Aires
Argentina
(5411) 4811-0071
www.cari.org.ar
@CARIconsejo

SUMARIO

**Este artículo fue publicado en Rev. Bras. Polít. Int. 58 (1): 230-248 [2015]*

The US experience in contracting out security and lessons for other countries**

Thomas C. Bruneau (*)

Los Estados Unidos han ido más que ningún otro país en la privatización de la seguridad. Otros países pueden encontrar persuasiva la lógica económica o financiera del uso de contratistas. La experiencia estadounidense en la contratación privada de servicios de seguridad, particularmente en Irak, fue problemática y puede servir como moraleja para que otros países aprendan cómo evadir los errores.

Keywords: Iraq; privatization; security; USA.

Introduction

There is an increasing reliance on private security contractors throughout the world. Already private security guards far outnumber uniformed police officers in many countries. In Latin America, for example, the ratio of private security guards to police officers is 6.7 to 1 in Guatemala and 4.9 to 1 in Brazil.[1] There are indications that military personnel will to some degree be replaced by private contractors in several countries. In Argentina for example, the guards at the airports will be privatized rather than rely on the previous Air Force police. And, I know from requests I receive to discuss contracting out security from governments including Brazil, Nepal, and Portugal, that there is interest in the issue of contracting out security more generally. No country has gone further in contracting out security than the United States. While both government officials and scholars have repeatedly highlighted problems in contracting out security, these problems continue. I will draw upon the lessons I have learned from the US experience, particularly in Iraq, to draw what amounts to a cautionary tale regarding the use of private security contractors. The focus here is on private security contractors, those who carry weapons and most closely approximate the traditional roles of the uniformed military. More will be explained on these roles in the paper. This paper is based on data to which anyone energetic and interested can have access, largely from public and official US Government sources, my own research that included eight research trips to Washington, D.C. between 2009 and 2014, and which resulted in Anonymous.

The US experience

That the US is the world leader in the use of contractors can be seen in the Figure 1.[2]

The same data, displayed in Figure 2 shows that it is also as post-Cold War phenomenon with spikes during the wars in the Balkans and then in Afghanistan and Iraq.[3]

[1] Organization of American States, Report on Citizen Security in the Americas 2012 (2012) Washington, DC: OAS Hemispheric Security Observatory, p. 139.

[2] Dew, Nicholas and Bryan Hudgens (2008). The Evolving Private Military Sector: A Survey, 21-22. Published in http://www.acquisitionresearch.org, p. 9. The data is derived from a survey sent to 550 private contracting firms.

[3] Dew and Hudgens (2008, 8).

*Department of National Security Affairs, Naval Postgraduate School, Monterey, CA, USA

**Este artículo fue publicado originalmente en Rev. Bras. Polít. Int. 58 (1): 230-248 [2015]

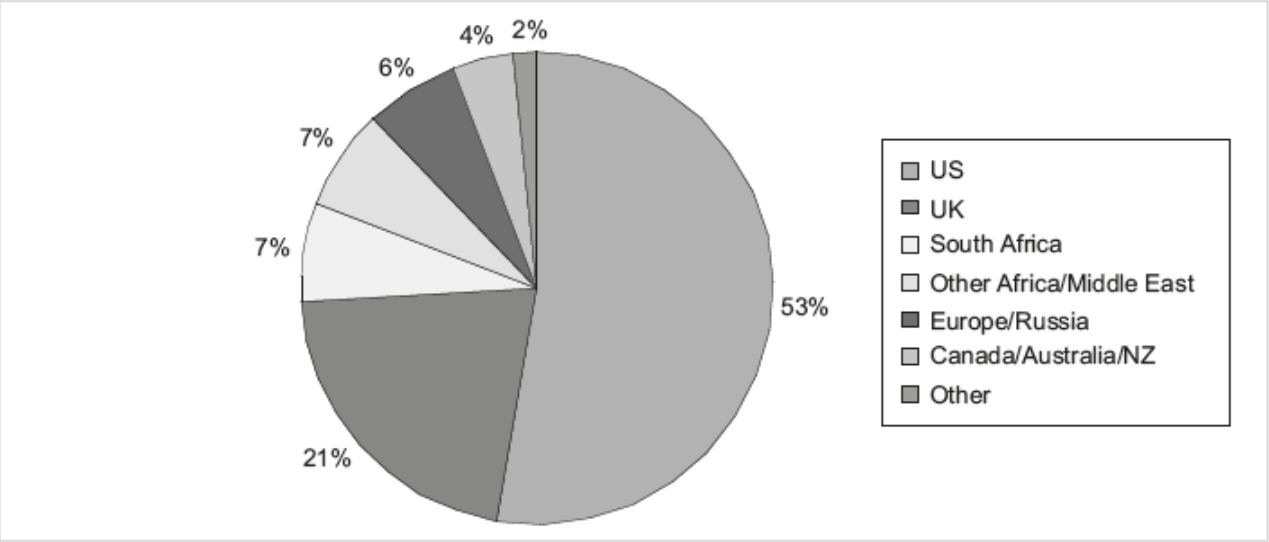


Figure 1. Geographical distribution of private security contractors.

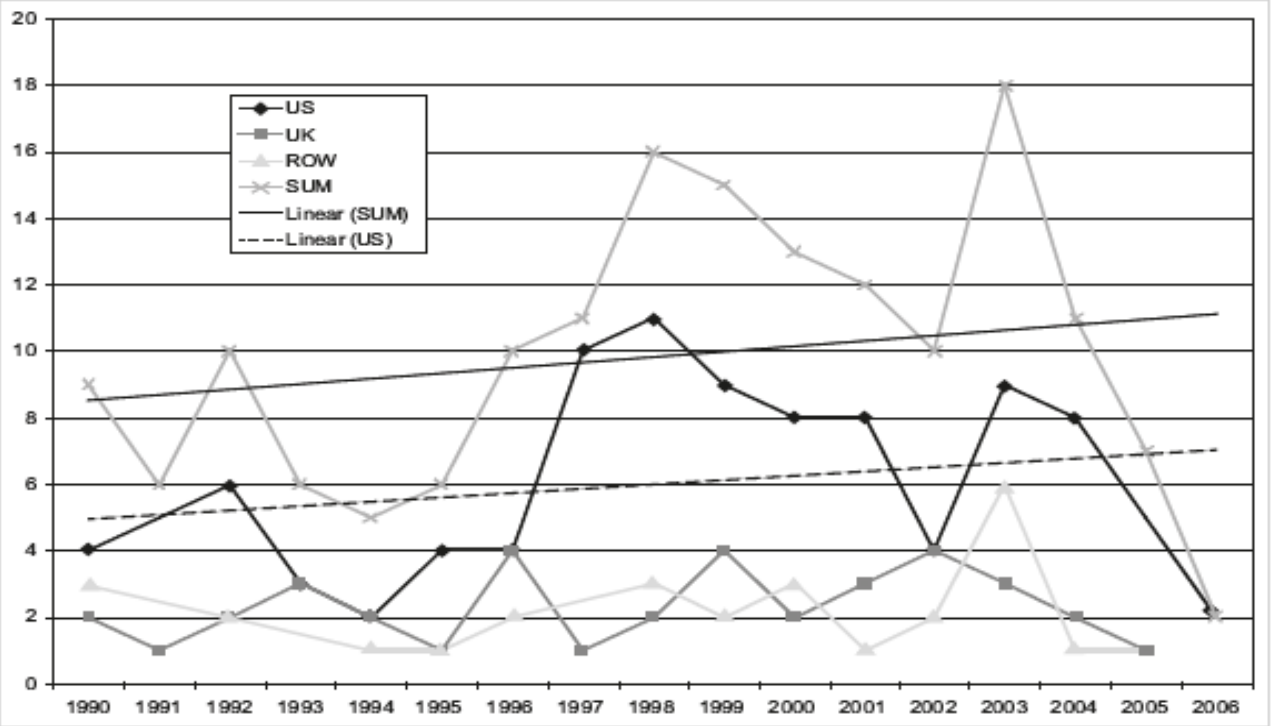


Figure 2. Founding of private security contractors.

But, that the use of contractors is an important phenomenon, there can be no doubt for in 2008 there were 190,000 contractors in the Iraq Theater compared to 200,000 uniformed military personnel.[4]

Despite the lack of reference to contractors in official documents and the main-line press, the use of private contractors continues today as an important phenomenon as is indicated by the fact that even after the departure of US troops from Iraq in December 2011, there still remained almost 11,000 private contractors.[5] As a very respectable scholar researching and publishing on contracting out security states in a recent article: "…when the US withdrew its

[4] Congressional Budget Office (CBO), (2008) Contractors' Support of US Operations in Iraq Washington, DC:CBO, p. 13.

[5] Schwartz, Moshe and Jennifer Church, (2013) Department of Defense's Use of Contractors to Support Military Operations: Background, Analysis, and Issues for Congress Congressional Research Service, p. 25. "Table A-2. Contractor Personnel and Troop Level in Iraq." These included private security contactors and others.

troops from Iraq in December 2011, the State Department sent in 5500 private security contractors to protect the embassy and American diplomatic interests there. To set this number in context, consider that it is roughly double the number of security contractors working for the State Department in Iraq prior to the withdrawal."[6] Even more telling, despite the lack of public attention in the current return by the US to fight the Islamic State in Iraq, the US Army Contracting Command published a "Sources Sought" in August 2014 for Security Assistance Mentors and Advisors Services in Iraq to "…focus on core process and systems which involve, but are not limited to administration, force development, procurement and acquisition, contracting, training management, public affairs, logistics, personnel management, professional development, communications, planning and operations, infrastructure management, intelligence and executive development".[7]

In sum, contracting out security remains a central characteristic of how the US operates, in combat and in general. To put the issue in perspective, as stated in a recent official report: "The Department of Defense (DOD) relies extensively on contractors to equip and support the US military in peacetime and during military operations, obligating more than US$ 300 billion in contracts in FY 2013."[8] To put this figure in perspective, the estimated total budget for DOD was US$ 613.9 billion in FY 2013.[9]

The focus in this paper is on the PSCs because they are armed, thus most closely approximating what military personnel have done in the US in the past and what most armed forces in other countries do today. Since they are armed it is not surprising that the US Congress, have paid a great deal of attention to the PSCs. This focus is captured in the title of SEC. 862 of the National Defense Authorization Act (NDAA) for Fiscal Year 2008, Public Law 110-181 (5 December 2007): "Contractors Performing Private Security Functions in Areas of Combat Operations".[10] The Special Inspector General for Iraq Reconstruction (SIGIR), which was founded by the US Congress in 2004 to audit the use of public funds in Iraq, published a "Comprehensive Plan for Audits of Private Security Contractors to Meet the Requirements of Section 842 of Public Law 110-181," updated on 8 May 2009, which provides detailed information on the PSCs and the audits and other studies being conducted on them.[11] Moreover, the main focus at the Office of the Secretary of Defense (OSD), Assistant Deputy Under Secretary (Logistics & Material Readiness/Program Support) is on implementing the guidance of Section 862.

As of 16 October 2008, SIGIR had identified seventy-seven individual PSC companies that provided security services to US agencies working in Iraq since 2003. In a May 2009 update of the report, SIGIR identified another sixteen, bringing the total to ninety-three companies that have provided physical security services in Iraq. The report estimates that since the war's inception in 2003 until early 2009, Department of Defense, Department of State, and United States Agency for International Development had spent US$ 5.9 billion on contracts and subcontracts for PSCs. In interviews at SIGIR officials emphasized that the PSCs are extremely important in the overall reconstruction effort, and would likely become even more important as US forces withdrew, first from the major cities and finally from the country at the end of 2011.[12] Considering the data provided above from Molly Dunigan on

[6] Dunigan, Molly (2014) The future of US military contracting: Current trends and future implications, International Journal Published online.
[7] Federal Business Opportunities, Solicitation Number – W560MY-14-R-004. accessed September 30, 2014. Emphasis added https://www.fbo.gov/index?s=opportunity&mode=form&id=2eec28ef1768665f2a6310916c50dff9&tab=core&_cview=0
[8] Schwartz, Moshe (2014) Summary "Defense Acquisition Reform: Background, Analysis and Issues for Congress" CRS Report for Congress
[9] For data on the overall DOD budget see Office of the Under Secretary of Defense (Comptroller) "National Defense Budget Estimated for FY 2013" available at accessed January 22, 2015 http://comptroller.defense.gov/Portals/45/Documents/defbudget/fy2013/FY13_Green_Book.pdf
[10] Contractor Performing Functions in Areas of Combat Operations, (2007) SEC. 862 of the National Defense Authorization Act (NDAA) for Fiscal Year 2008, Public Law 110-181.
[11] Bowen, Stuart and David R. Warren (2009) Comprehensive Plan for Audits of Private Security Contractors to Meet the Requirements of Section 842 of Public Law 110-181, SIGIR.
[12] Author interviews at SIGIR with the Deputy Director, the Assistant Inspector General for Audits, and several auditors, Arlington, Virginia, 26 February and 16 June 2009.

the 5,500 private security contractors remaining in Iraq after the departure of US troops, they were accurate.

A later SIGIR Report to Congress, in 2009, estimated that there were 25,500 private security personnel under contact in Iraq.[13] SIGIR does not claim to have developed a precise definition of just what is a PSC. However, several federal agencies, including SIGIR, define a PSC in terms of the following four tasks or functions:

- Static Security: protect fixed or static sites, such as housing areas, reconstruction work sites, or government buildings.
- Convoy Security: protect convoys traveling in Afghanistan and Iraq.
- Security Escorts: protect individuals traveling in unsecured areas in Afghanistan and Iraq.
- Personal Security Details –provide protective security to high-ranking individuals.

While these particular tasks or functions may not be associated with what are often referred to as "trigger pullers," they were previously carried out by personnel who were part of the highly-regulated, civilian-controlled military structure that I have described elsewhere.[14] That is, they are the closest to the military in terms of being armed and protecting people, things, and places.

The motivations to contract out

There are several "drivers" or justifications for the contracting out phenomenon in the US. Some of these may apply in other countries. Relying on official sources, the following have been identified as the most important.[15]

First, an authoritative source to establish a baseline description of the general context for contacting out is the testimony of David M. Walker, then US Comptroller General, to the House Subcommittee on Readiness in March 2008. Walker offered a list of the factors that led federal agencies to outsource more and more services:

> *…limitations on the number of authorized full-time equivalent positions; unavailability of certain capabilities and expertise among federal employees; desire for operational flexibility; and the need for "surge" capacity. According to DOD and armed service official, several factors have contributed to the department's increased use of contractors for support services: (1) the increased requirements associated with the Global War on Terrorism and other contingencies; (2) policy to rely on the private sector for needed commercial services that are not inherently governmental in nature; and (3) DOD initiatives, such as competitive sourcing and utility privatization programs.*[16]

These are ongoing and long-term motivations.

Second, with the all-volunteer force, private security contractors are thought by informed experts to be necessary. At the end of the Cold War, the US Army went from 732,000 active personnel in 1990 to 408,000 in 1997; for the three services, including the Marines, the numbers were 2,043,705 in 1990, to 1,438,562 in 1997. As of August 2009, with two wars waging, the size of the US Army stood at 552,425.[17] A number of contractor proponents highlighted to me the personnel shortage to explain the growth of the PSCs.

---

[13] SIGIR, Quarterly Report to the United States Congress October 30, 2009, reports that as of September 30, 2009 there are 25,500 private security contractors in Iraq. There were, at the same time, 120,000 US forces. p. 47.

[14] Specifically in Anonymous.

[15] Dew and Hudgens (2008) pp. 44-50. Singer, P.W. (2003) Corporate Warriors: The Rise of the Privatized Military Industry Ithaca: Cornell University Press, dedicates a chapter to this topic, 4, "Why Security Has Been Privatized", pp. 49-70.

[16] Walker, David M. (2008) Comptroller General of the United States, Before the Subcommittee on Readiness, Committee on Armed Services, House of Representatives, GAO-08-572T: 4-5

[17] The data for 1990 is from "Selected Manpower Statistics Fiscal Year 1990," (AD-A235 849), issued by Washington Headquarters Services, Directorate for Information Operations and Reports, Department of Defense. Data for 1997 and 2009 are found at: http://siadapp.dmdc.osd.mil/personnel/MILITARY/history/tab9

Third, Secretary of Defense Donald Rumsfeld (2001–2006) wanted to demonstrate that the Iraq invasion and pacification could be accomplished with a lean force, and that technology would be a sufficient force multiplier. Such a success would justify his policies promoting defense "transformation" over a traditional build-up of forces, policies that were encouraged by Rumsfeld and others in the George W. Bush Administration. As Richard N. Haass states, the invasion of Iraq in 2003 was a "war of choice" rather than of necessity as its proponents claimed.[18] Whereas the United States deployed 500, 000 troops in the 1991 war against Iraq, in line with the Powell Doctrine premise of using overwhelming force to achieve a clear goal, the 2003 invasion kept troop levels to about 150,000. General Eric Shinseki, Army Chief of Staff, disagreed with this policy while being questioned before Congress. Shortly thereafter Secretary of Defense Rumsfeld announced Shinseki's replacement, about eighteen months before his scheduled retirement. Rumsfeld ignored military advice, and other military leaders did not push back.[19] In interviews, security contractors emphasize the security vacuum that they have been employed to fill, but the vacuum appears to be a result of deliberate policy rather than exigency.

In sum, there are at least three major reasons for the growth in contracting in general, and security in particular, as demonstrated in Figures 1 and 2 and Table 1 above. The result was chaotic as Secretary Rumsfeld's successor, Robert M. Gates, would write. "As the contractor presence developed in Iraq after the original invasion, there was no plan, no structure, no oversight, and no coordination. The contractors' role grew willy-nilly as each US department or agency contracted with them independently, their number eventually climbing to some 150,000."[20] While other countries's armed forces may not be engaged in combat as are US forces, there is still a strong appeal to the logic of contracting out. In theory, at least, contractors should be cheaper than professional military personnel in that they can be let go when there is no longer a need for them, and none of the additional costs, such as health benefits, dependents' allowances, pensions, and the like are required.[21] It is important to stress that it is mainly for these theoretical reasons that contracting out is strongly encouraged in the US not only under Republican but also Democratic administrations.

Contracting out is not only legal, but strongly encouraged in the US

Many outsiders, and critics, do not seem to realize that contracting out is not only legal in the US, but in fact strongly encouraged by laws and policies from President Ronald Reagan (1981–1989) until the present. A 2008 Congressional Research Service (CRS) report gives a sense of what is involved, and the extensive legal basis, for government contracting:

> *Sometimes called contracting out, "outsourcing" refers to an agency engaging a private firm to perform an agency function or provide a service. ...Federal outsourcing policy is governed by the FAR [Federal Acquisition Regulation] and the Federal Activities Inventory Reform (FAIR) Act of 1998 (P.L. 105-270). FAIR requires agencies to produce inventories of "commercial activities" -those that are not "inherently governmental" and able to be acquired from the private sector– that may be put up for competitive sourcing. OMB's Circular A-76*

[18] Haass, Richard N. (2009) War of Necessity War of Choice: A Memoir of Two Iraq Wars New York: Simon & Schuster

[19] Richard Haass refers to "...the effective silencing of the Joint Chiefs of Staff by Secretary of Defense Donald Rumsfeld.". Haass, War of Necessity, pp. 18-19. This key point has been dealt with extensively in credible sources. Joseph Collins lists ten "Errors in Decision making and Execution," of which eight concern lack of manpower. See Collins, Joseph J. (2008) Choosing War: The Decision to Invade Iraq and Its Aftermath, Occasional Paper, Institute for National Strategic Studies, National Defense University, p. 16.

[20] Gates, Robert (2014) Duty: Memoirs of a Secretary at War New York: Alfred A. Knopf, p. 224.

[21] It is worth noting that the Brazilian lower house, the Câmara, approved a bill in January 2015 to outsource labor. See http://www1.folha.uol.com.br/fsp/opiniao/215181-capital-sobe-trabalho-desce.shtml

provides agencies with specific directions for undertaking competitive sourcing.[22]

The Office of Management and Budget (OMB) Circular A-76 provides the legal basis for outsourcing.[23] There is an extensive literature by practitioners on this topic, which conveys a sense of the extremely pro-privatization environment of the US government.[24] There is a "dialogue of the deaf" on this issue. Social scientists, some journalists, and sectors of the general public see contracting out functions in national security and defense as anomalous, even somehow shady, whereas those within government view it as standard operating procedure. And, since almost one half of the DOD budget is currently contracted out, it indeed is.

Awareness of problems in contracting out in recent conflicts

In the US the general issue of the use of public funds, and especially the utilization of contractors, became a very public and polemic issue which motivated the US Congress to not only hold hearings and pass laws to regulate the use of contractors in Iraq and Afghanistan, but also created organizations to focus specifically on the waste of very large sums of money. As noted above, the Congress created SIGIR, and despite efforts by the George W. Bush administration to shut it down, SIGIR continued until 2013 (when there were no more public funds to audit in Iraq). Between its creation in 2004 and its final Report in September 2013, the SIGIR dealt with all imaginable topics surrounding the use of the US$ 60 billion of US funds allocated by the US Congress for the reconstruction of Iraq. The focus on contractors, including private security firms, was a central element of SIGIR's work.[25]

Even more specifically regarding contracting out, in the face of scandals, fraud, and other problems, the U. S. Congress created in 2008 the Commission on War Time Contracting to examine contracting out in Iraq and Afghanistan. In their final report Transforming Wartime Contracting: Controlling costs, reducing risks, of August 2011, the Commission stated that at least US$ 31 billion, and possibly as much as US$ 60 billion had been lost to contract waste and fraud in operations in Iraq and Afghanistan.[26]

Despite the widespread awareness of problems, and the current "sources sought" from the Army Contracting Command for contractors to go to Iraq, the problems continue. A recent official document puts it this way: "Congress and the executive branch have long been frustrated with waste, mismanagement, and fraud in defense acquisitions and have spent significant resources attempting to reform and improve the process. These frustrations have led to numerous efforts to improve defense acquisitions. Since the end of World War II, every Administration and virtually every Secretary of Defense has embarked on an acquisition reform effort. Yet despite these efforts, cost overruns, schedule delays, and performance shortfalls in acquisitions programs persist."[27]

[22] Kosar, Kevin R. (2006) Contracting for Services (Outsourcing) in Privatization and the Federal Government: An Introduction Washington, DC: Congressional Research Service, p. 15.
[23] Luckey, John R. (2003) OMB Circular A-76: Explanation and Discussion of the Recently Revised Federal Outsourcing Policy, CRS Report for Congress, Washington, D.C., updated 10 September 2003.
[24] See for example, Donahue, John D. (1989) The Privatization Decision: Public Ends, Private Means New York: Basic Books and Light, Paul C. (2008) A Government Ill Executed: The Decline of the Federal Service and How to Reverse It Cambridge: Harvard University Press.
[25] The SIGIR Final Report to the United States Congress, dated September 9, 2013, is available at www.sigir.mil. Accessed January 14, 2015. The Special Inspector General for Afghan Reconstruction (SIGAR) still continues.
[26] The Final Report to Congress of the Commission on Wartime Contracting in Iraq and Afghanistan, Transforming Wartime Contracting: Controlling costs, reducing risks dated August 2011 is available at www. Wartimecontracting.gov. Accessed January 14, 2015.
[27] Schwartz, Moshe (2014) Defense Acquisition Reform: Background, Analysis, and Issues for Congress CRS Report, (R 43566), p. i.

Implications for National Security and Defense of contracting out security

The most recent Congressional Research Service Report on the topic of contracting out states, in the first sentences of the Introduction: "The Department of Defense (DOD) has long relied on contractors to provide the US military with a wide range of goods and services, including weapons, food, and operational support. Without contractor support, the United States would currently be unable to arm and field and effective fighting force."[28] As it is certain that contracting out national security and defense is here to stay, what, then, are some of the implications of this phenomenon? Utilizing our framework for analysis of civil-military relations and applying it to the PSCs, the results are displayed in Table 2.[29]

Efficiency, which in my framework is essentially having functioning institutions to investigate and audit where resources go and how they are used, is not currently a problem with regard to the private security contractors. The federal institutions and mechanisms that carry out audit and investigation functions specifically to monitor the efficiency of PSCs are robust. Among many initiatives geared toward improving transparency in Iraq, Congress directed the Congressional Research Service (CRS) to undertake extensive reporting, including a "Congressional Oversight Manual;"[30] the Congressional Budget Office (CBO) to assess budgets and analyze the PSCs' contracts; the Government Accountability Office (GAO) to study all relevant aspects of the contracting phenomenon; and most importantly and provocatively, kept SIGIR funded.[31]

Table 1. Institutional dimensions of public and private national security and defense.

	Efficiency	Control	Effectiveness
Civil-military relations	Monitoring and by full spectrum of institutional	Control exercised by spectrum of oversight mechanisms, and professional education	Problematic due to lack of strategy and weakness of institutions
Private security contractors	Same as above	Minimal control due to uncertain concept inherently functions and sketchy legal controls	Problematic due to of doctrine to include PSCs and absence or shortage of officers and CORs

In reviewing these three dimensions—efficiency, control, and effectiveness— with regard to the US may allow other countries to better prepare for contracting- out than the US was and still is.

Control As the scope of contracting out expanded in Iraq, and scandals were made

[28] Schwartz, Moshe and Wendy Ginsburg, and John F. Sargent Jr, (2015) Defense Acquisitions: How and Where DOD Spends Its Contracting Dollars CRS Report, (R44010), p. 1.

[29] This framework is explained and illustrated in Anonymous.

[30] Kaiser, Frederick M. and Walter J. Oleszek, T.J. Halstead, Norton Rosenberg, and Todd B. Tatelman, (2007) Congressional Oversight Manual, CRS Report for Congress (RL 30240). The manual was updated, and republished on 19 December 2014. It is CRS RL30240.

[31] The GAO details their instruction to study PSCs in "MILITARY OPERATIONS. High-Level DOD Action Needed to Address Long-standing Problems with Management and Oversight of Contractors Supporting Deployed Forces," Government Accountability Office (GAO) Report to Congressional Committees (GAO-07- 145), December 2006, updated from 2003:3.

public by SIGIR, the media, and non-governmental organizations (NGOs), there developed a sense that the PSCs had been allowed to expand their activities into what were previously considered "inherently governmental functions". This concern was palpable in many personal interviews of the author with very senior policy-makers. The issue was raised publicly by members of the US Congress during the last months of 2008, where the ensuing political battle over the definition of inherently governmental exposed some of the different powers and funding sources of different sectors of the security contracting "industry".

That legislative debate, and the fact that the new administration coming into office on 20 January 2009 included not only President Barack Obama but also Secretary of State Hilary Clinton, both of whom had weighed in as senators in that debate on the side of tightening up the definition of "inherently governmental functions," meant that the issue would continue to have a high profile. Consequently, in mid-2009, the Office of Management and Budget (OMB) was tasked with delimiting inherently governmental functions, for which it held a public discussion in June. However, and important to understand concerning the politics of this issue, once contractors took on the missions that were previously inherently governmental, and developed supporters in government through the use of campaign funds and lobbyists, it was extremely difficult to turn the trend around. Proof of this point is that the most recent CRS report on Inherently Governmental Functions, of 23 December 2014, states boldly that there are two primary definitions of "inherently governmental functions" and in the four pages of tables at the end of the report demonstrates that there in fact four different definitions.[32]

If an area of governmental responsibility that originally was considered to be inherently governmental has been opened up to the PSCs, then what kind of control can be exerted to be sure they are acting in the best interests of the country? It is clearly not the robust set of institutions, oversight, and professional norms that apply to the uniformed military—they do not apply even to those contractors who carry out what seem to be military functions. Some experts, especially non-US sources, look to legal controls through enforcement of or modifications of existing law.[33] While this appears promising in theory, in fact the legal basis for reigning in the PSCs is also problematic.

The legal bases for regulating and controlling the PSCs are dealt with in studies by the CBO, CRS, GAO, and by contract law specialists in a number of publications. Even so, it is very difficult to determine the current legal status of contractors, including the PSCs. Under international law, contractors and other civilians working with the military are classified as civilian non-combatants. The application of international laws of armed conflict, including under the 1977 Protocol I to the Geneva Convention on mercenaries, however, is ambiguous, according to this CRS report and others.[34]

Under US law, "US contractor personnel and other US civilian employees in Iraq may be subject to prosecution in US courts. Additionally, persons who are "employed by or accompanying the armed forces" overseas may be prosecuted under the Military Extraterritorial Jurisdiction Act of 2000 (MEJA) or, in some cases, the Uniform Code of

[32] Manuel, Kate M. (2014) Definitions of "Inherently Governmental Function" in Federal Procurement Law and Guidance, CRS Report for Congress; the tables are pp. 22-25.

[33] See for example, Alexandra, Andrew, Deane-Peter Baker and Marina Caparini, eds. (2008) Private Military and Security Companies: Ethics, policies and civil-military relations London and New York: Routledge; and more recently, Sheehy, Benedict, Jackson Maogoto, and Virginia Newell, (2009) Legal Control of the Private Military Corporation Basingstoke: Palgrave Macmillan.

[34] For example, the Montreux Document of 17 September 2008 resulted from a meeting of seventeen countries regarding rules and good practices relating to private military and security companies operating in armed conflicts and relates to the Status of the Protocols Additional to the Geneva Conventions of 1949, and to the protection of victims of armed conflicts. The document "…contains a set of over 70 good practices designed to assist States in complying with these obligations. Neither parts are legally binding, nor are they intended to legitimize the use of PMSCs in any particular circumstance." Summary of United Nations "General Assembly Security Council," (A/63/467-S/2008/636), 6 October 2008.

Military Justice (UCMJ).[35] But even with this statutory authority, some contractors "might fall outside the jurisdiction of US criminal law, even though the United States is responsible for their conduct as a matter of state responsibility under international law and despite that such conduct might interfere with the ability of the Multi-National Forces in Iraq to carry out its US mandate."[36]

In interviews with Mr. Jeff Green, who had been Counsel to the Committee on Armed Services in the US House of Representatives and then President of his own lobbying firm and Doug Brooks, then President of the International Peace Operations Association (IPOA), in mid-June 2009, they concurred with this assessment. Brooks noted that while initially he and the members of IPOA were concerned with the SOFA, its implementation has worked out better than expected. The only thing that becomes apparent from these sources is that at present clear control is exercised over the PSCs neither by international law nor US law. Because the latter system is based on precedent, cases such as the Blackwater shootings in Nisour Square in Bagdad on September 16, 2007 have to work their way through the appeals courts to reach some determination of how existing laws apply, and possibly to point the way toward additional legislation.[37]

Contracting firms are quick to argue that they are more effective than government agencies. And, since setting the bar with this comparison is extremely low, they may be right. However, one cannot look only at one contract but the overall situation of contracting out to understand their effectiveness. Based on research comparatively and in the US, we have developed a concept (within the framework displayed in Table 2), which we apply to the armed forces, the following three requirements for effectiveness: a plan, institutions to implement the plan, and adequate resources (financial and human) to reach the goal.

Consequently, the first question to ask is, is there a plan that defines, coordinates, and implements a strategy for the use of contractors in support of military operations? Even if the combat commander in the field had a strategic vision of how to fight in the theater, as he must, he probably does not have control over the contactors operating in the theater, or have a way to include them in his strategic vision. As an August 2008 CBO report, states:

Although military commanders can directly control the actions of military personnel and government civilians, their control over individual contractor personnel is less direct […]. In practice that authority [laws and regulations of the United States] enables the military commander to allocate the personnel under his or her command among any number of tasks those personnel are able and trained to do. The military commander may also request that additional personnel be reassigned from other parts of the government if necessary. By contrast, the duties of contractor personnel are set out in a fixed written contract […]. The military commander generally lacks the authority either to increase the scope (dollar value) of the contract or to change the contractor's duties except in ways anticipated in the contract language. […] The military commander has less direct authority over the actions of contractor employees than over military or government civilian subordinates.[38]

Currently, there is no doctrine that compels integration of the contractors into a military commander's strategy. Even once formulated, however, this doctrine will have to be adopted and implemented by the three separate services that individually have the authority to recruit, train, and equip the armed forces.

[35] Elsea, Jennifer K. Moshe Schwartz, and Kennon H. Nakamura, (2008) p. 20. 36 Ibid.
[36] Ibid.
[37] On October 22, 2014 a jury in the Federal District Court in Washington, D.C. found four former Blackwater private security guards guilty in the deaths of 17 Iraqi civilians in Nisour Square in 2007. This was the first conviction of private security guards in the US court system. In April 2015 the four were sentences to terms ranging from 30 years to life imprisonment.

[38] "Contractors' Support of US Operations in Iraq," CBO Paper, August 2008: 20.

Indeed there are now some indications of this awareness, but as it is a service responsibility, and it takes a VERY long time to formulate, let along implement, a doctrine. As of late 2011 the United States Army has published a doctrine, Operational Contract Support Planning and Management, signed by General Martin E. Dempsey, at that time Chief of Staff of the Army. It will, however, take some time before this doctrine is assimilated by the troops in the field, including the commanders.[39]

To be effective a security strategy requires institutions to implement it. What kinds of institutions are there, if any, to coordinate the contractors? The Gansler Commission Report, named for its chairman, The Honorable Jacques Gansler who was Under Secretary of Defense for Acquisition, Technology and Logistics during the Clinton Administration and who currently holds a named chair for Public Policy and Private Enterprise at the University of Maryland identifies problems with complexity, an insufficient focus on post-award contract management, inadequate organization and inadequate lines of responsibility to facilitate contracting.[40] Under the heading, "Extremely Poor Interagency Operations," the report finds that there is a lack of institutional orientation and functional inter-agency process in all of the areas listed above.[41] The following quotes, from this section of the report, elaborate these points, rearranged slightly here to follow the line of my argument.

> *In the Cold War environment, it was not envisioned there would be other Departments or Agencies engaged so much on the field of conflict. Today, the military commander who is supported by a "joint" contracting organization actually has a disparate group of well-meaning professionals sitting side-by-side applying different rules to the same situation […]. While it is recognized that the State Department, Justice, Commerce, Treasury, et al. bring impressive tool kits, which represent some of the most effective tools America has to offer and are critically essential to nation-building, in the Cold War era, these players only entered after the battlefield was relatively secure. They were not the integrated partners which successful expeditionary operations may require.*[42]

As the contractors are not under direct control of the commander, but are necessary for the success of his plan or strategy, the absence of coordination or an inter-agency process is especially important. All the sources I consulted, both written and in personal interviews, conclude that there is no overall plan or strategy within the DOD to integrate the contractors into an effective whole, nor is there an institutional mechanism to coordinate their work. The congressional staffers, academics, and GAO personnel interviewed all emphasized this critical weakness. The next question to ask is one regarding human resources (and not financial resources as the US poured money into the campaigns in Iraq and Afghanistan), and the question is what quantity and quality of personnel are in place to award and, even more important, oversee or monitor the contracts?[43] This, however, is an institutional issue that is very difficult to remedy. The scope of the problem is daunting. The Gansler Commission report directly addresses the fact that the contract management workforce has not increased despite a seven-fold increase in the workload.

> *In 1990, the Army had approximately 10,000 people in contracting. This was reduced to approximately 5,500, where it has remained relatively constant since 1996. […] yet both the number of contract actions (workload) and the dollar value of procurements (an*

[39] US Army, "Operational Contract Support Planning and Management," Army Regulation 715-9Washington, DC: Headquarters of the Army June 20, 2011. Available at http://www.apd.army.mil/pdffiles/r715_9.pdf

[40] Gansler Commission Report "Urgent Reform Required: Army Expeditionary Contracting," report of the Commission on Army Acquisition and Program Management in Expeditionary Operations, 31 October 2007.

[41] Gansler Commission Report: 39 –46.

[42] Ibid.: 45-6

[43] According to Belasco, Amy (2014) The Cost of Iraq, Afghanistan, and Other Global War on Terror Operations Since 9/11, Congressional Research Report (RL33110), p. i. the total sum is $ 1.6 trillion of which $ 815 billion was for the war in Iraq.

> *indicator of complexity) have dramatically increased in the past decade while the contracting workforce has remained constant. The dollar value of Army contracts has increased 331 percent from US$ 23.3 billion in 1992 to US$ 100.6 billion in 2006, while the number of Army contract actions increased 654 percent from approximately 52,900 to 398,700 over the same period.*[44]

Furthermore, the overwhelming majority of contract managers are civilians; out of a total of 5,800, there are only 279 military personnel doing this job.[45] This is extremely important as military personnel can be deployed much more easily than can civilians, and the report goes into some detail on why it is difficult to deploy civilians.[46] It means that the contract managers were not in Iraq, or Afghanistan, but rather in the US. The background to this situation of few military contracting officers is found in the reduction of military forces at the end of the Cold War in the 1990s. While overall US Army forces, for example, were reduced 32% from 732,000 in 1990 to 499,301 by 2003, the ranks of contracting officers were reduced 45% from 10,000 to 5,500, including the elimination of all flag and general officer positions during the same period.[47]

Given this chronic shortage of personnel, who then oversees the fulfillment and completion of the contract? This is the contracting officer representative, or COR.

There is agreement among sources on the lack of preparation for CORs, and the unreasonable multi-tasking expected of them. The Gansler Report is very critical of the CORs as an institutional mechanism for oversight.

> *Contracting Officer's Representatives (CORs), who are an essential part of contract management, are at best a "pick-up game" in-theater. CORs represent the "last tactical mile" of expeditionary contracting. However, CORs are assigned as contract managers/administrators as an "extra duty," requiring no experience. A COR is often a young Soldier who does not have any experience as a COR. […] Although being a COR would ideally be a career-enhancing duty, the COR assignment is often used to send a young Soldier to the other side of the base when a commander does not want to have to deal with the person. Additionally, little, if any, training is provided. To further compound matters, generally all COR training is geared for a low-operations, low risk tempo, so it is barely adequate. Despite this, there are still too few CORs. Moreover, COR turnover is high, frequently leaving many gaps in contract coverage.*[48]

In June 2003, GAO issued a comprehensive analysis of problems with DoD management and oversight of contactors that support deployed forces, and released a follow-on report to Congress in December 2006.[49] In the updated report, William M. Solis, GAO's director of Defense Capabilities and Management, noted that GAO began to report in 1997 on shortcomings in DoD's management and training of contractor support to deployed forces, and took on the current study due to the increased use of contractors, and ongoing Congressional interest: "…GAO's objective was to determine the extent to which DOD has improved its

[44] Gansler Commission Report: 30. See also Schwartz, Moshe (2008) Training the Military to Manage Contractors During Expeditionary Operations: Overview and Options for Congress, CRS Report for Congress, p. 1, Figure 1. "However, while a number of contracting officers and other acquisition officials are in Iraq, most of DOD's acquisition workforce is generally not deployed or embedded with the military during expeditionary operations. As the number of contactors in the area of operations has increased, the operational force – the service men and women in the field – increasingly rely on, interact with, and are responsible for managing contractors. Yet, a number of military commanders and service members have indicated they did not get adequate information regarding the extent of contractor support in Iraq and did not receive enough pre-deployment training to prepare them to manage or work with contractors." Schwartz: 3. Schwartz draws heavily on Walker, David M. (2008) Defense Management: DOD Needs to Reexamine Its Extensive Reliance on Contractors and Continue to Improve Management and Oversight, Testimony Before the Subcommittee on Readiness, Committee on Armed Services, House of Representatives. (GAO-08-572T.

[45] Gansler 35, table 9.

[46] Ibid. 36-7.

[47] Gansler Commission Report: 30.

[48] Gansler Commission Report: 43.

[49] Solis, William M. Director, (2006) Defense Capabilities and Management, "MILITARY OPERATIONS: High-Level DOD Action Needed to Address Long-standing Problems with Management and Oversight of Contractors Supporting Deployed Forces" GAO report to Congress (GAO-07-145).

management and oversight of contractors supporting deployed force since our 2003 report."[50] This preface then lists four areas as examples of ongoing problems with contracting, all of which fall within the three analytical dimensions outlined above: planning, institutions, and resources. What is clear is that the problems identified in the report of June 2003 still applied in December 2006.[51]

The report also addresses persistent problems with insufficient resources to conduct oversight:

> *DOD continues to not have adequate contractor oversight personnel at deployed locations, precluding its ability to obtain reasonable assurance that contractors are meeting contract requirements efficiently and effectively at each location where work is being performed. While a lack of adequate contract oversight personnel is a DOD-wide problem, lacking adequate personnel in more demanding contacting environments in deployed locations presents unique difficulties.*[52]

Training is another aspect of the resource dimension:

> *Military personnel continue to receive limited or no training on the use of contractors as part of their pre-deployment training or professional military education. The lack of training hinders the ability of military commanders to adequately plan for the use of contractor support and inhibits the ability of contract oversight personnel to manage and oversee contractors in deployed locations. Despite DOD's concurrence with our previous recommendations to improve such training, we found no standard to ensure information about contractor support is incorporated in pre-deployment training.*[53]

Although resources are the main issue in this observation, it also has implications for both planning and institution-building in that without training to manage and oversee the contractors, a commander and his staff cannot coordinate the contractors' work with the command's actual and evolving needs.

All of the audits and studies that deal with DoD contracting practices come to the same conclusions. And, what applied during the war in Iraq is still the situation. At this point, contracting for services is still not included within a plan or strategy, there is no single responsible institution or inter-agency process to oversee either the awarding or fulfilling of contracts, and oversight personnel are lacking in both numbers and preparation. Currently, based upon the earlier huge reliance on contractors in Iraq and Afghanistan and the unrelenting negative publicity where Blackwater came to symbolize contracting out, the topic of contracting out as the US returns to Iraq is "toxic". The problems have not been resolved, but rather swept under the carpet.

Considerations for other countries

Once contracting begins, and an industry emerges motivated by the profit motive, employing people, and engaging in lobbying and "strategic communications", it will never go away. What was lacking in the US, and the effort since then has been to catch up, is a robust legal framework, a clear definition of what can and, more importantly, cannot be contracted out, and a robust doctrine, with extensive training for all military personnel on how to deal with contractors. In the US all of these were initially missing, and it is only with great, and inconsistent, efforts that there is any progress at all in their being remedied. If a country can focus on these key requirements from the beginning, before contracting out is well established, then it will have a better chance of minimizing the negative aspects of contracting out. It must always be remembered there is a tension between two different mentalities or world views in that

[50] Ibid.: Highlights (no page number).
[51] Ibid: Highlights, Military Operations (no page numbers).
[52] Ibid: Military Operations (no page numbers).
[53] Ibid: Military Operations (no page numbers).

membership in the uniformed services is based on a sense of service and commitment, and PSCs are based on a profit-motive. This contrast can result in tensions in that there may be, and frequently are, armed personnel where one, working for a PSC, is being paid a salary that is three times greater than the uniformed soldier or officer. And, while the uniformed personnel are responsible for all and everything, the PSC is responsible for only what is included in the contract. This tension or contradiction can result in not only misunderstandings, but also recriminations and morale problems.

Conclusion

Contracting out, including in security is well-established in the US. There are many causes and implications of contracting out. The logic of it makes sense, on the face of it, but as they say, "the devil is in the details". As there are many causes or drivers, a simple decision, should one be forthcoming, to stop contracting out is impossible. Other countries must be aware of the possible negative implications prior to contracting out key roles and missions of their military forces.

Bibliographic references

- Avant, Deborah The Market for Force: The Consequences of Privatizing Security New York: Cambridge University Press, 2005.
- Bruneau, Thomas C. Patriots for Profit: Contractors and the Military in U.S. National Security Stanford: Stanford University Press, 2011.
- Commission on Wartime Contracting in Iraq and Afghanistan, Transforming Wartime Contracting: Controlling costs, reducing risks dated August 2011 is available at: www. wartimecontracting.gov.
- Congressional Budget Office (CBO) 'Contractors' Support of U.S. Operations in Iraq' (Washington, D.C.: CBO, August 2008).
- Dew, Nicholas and Bryan Hudgens, (2008) The Evolving Private Military Sector: A Survey, 21-22. Published in http://www.acquisitionresearch.org p. 9.
- Dunigan, Molly Victory for Hire: Private Security Companies' Impact on Military Effectiveness Stanford: Stanford University Press, 2011.
- Gansler Commission Report 'Urgent Reform Required: Army Expeditionary Contracting,' report of the Commission on Army Acquisition and Program Management in Expeditionary Operations, 31 October 2007.
- Gates, Robert M. Duty: Memoirs of a Secretary at War New York: Alfred A, Knopf, 2014.
- Light, Paul C. A Government Ill Executed: The Decline of the Federal Service and How to Reverse It Cambridge, Mass: Harvard University Press, 2008.
- Luckey, John R., Valerie Bailey Grasso, and Kate M. Manuel, "Inherently Governmental Functions and Department of Defense Operations: Background, Issues, and Options for Congress," CRS Report for Congress, (15 June 2009).
- Manuel, Kate M. "Definitions of 'Inherently Governmental Function' in Federal Procurement Law and Guidance," CRS Report for Congress, (23 December 2014).
- Office of the Under Secretary of Defense (Comptroller) 'National Defense Budget Estimated for FY 2013' available at: http://comptroller.defense.gov/Portals/45/Documents/defbudget/ fy2013/FY13_Green_Book.pdf
- Organization of American States, Report on Citizen Security in the Americas 2012 Washington, DC: OAS Hemispheric Security Observatory (2012).
- Schwartz Moshe and Jennifer Church, "Department of Defense's Use of Contractors to Support Military Operations: Background, Analysis, and Issues for Congress," CRS Report for Congress (17 May 2013).
- Schwartz, Moshe "Summary" 'Defense Acquisition Reform: Background, Analysis and Issues for Congress' CRS Report for Congress (23 May 2014).
- Schwartz, Moshe, Wendy Ginsberg, and John E. Sargent Jr., "Defense Acquisitions: How and Where DOD Spends Its Contracting Dollars. CRS Report for Congress (30 April 2015).
- Singer, Peter Corporate Warriors: The Rise of the Privatized Military Industry Ithaca: Cornell University Press, 2003.
- Solis, William M. Director, (2006) Defense Capabilities and Management, "MILITARY OPERATIONS: High-Level DOD Action Needed to Address Long-standing Problems with Management and Oversight of Contractors Supporting Deployed Forces" GAO report to Congress (GAO-07-145).
- Stanger, Allison One Nation Under Contract: The Outsourcing of American Power and the Future of Foreign Policy New Haven: Yale University Press, 2009.
- Under Secretary of Defense for Acquisition, Technology, and Logistics, Performance of the Defense Acquisition System 2014 Annual Report (Washington, D.C.: USD[AT&l], June 13, 2014, 4. Available at http://www.acq.osd.mil/
- SIGIR Final Report, Learning from Iraq, March 2013 available at www.sigir.mil
- Walker, David M. Comptroller General of the United States, Before the Subcommittee on Readiness, Committee on Armed Services, House of Representatives, GAO-08-572T: 4-5. (2008).

"Ciber Ius ad bellum": Aportes para definir las reglas de empeñamiento militar de Argentina y de otros países de la Región en los casos de Ciber Conflictos entre estados naciones

Prof. Dr. Roberto Uzal (*)

Introducción

Las reglas de empeñamiento [1] [2] [3] ("rules of engagement" – ROE -)[54] constituyen, en el ámbito militar, directivas cuyo contenido y significado describen las circunstancias en las cuales las Fuerzas Armadas iniciarán un combate continuado con fuerzas oponentes.

Formalmente las reglas de empeñamiento se refieren a las órdenes emitidas por una autoridad militar competente que describe cuándo, dónde, cómo y enfrentando a quién debe ser utilizado el poder militar. Dichas reglas establecen qué acciones militares se pueden llevar adelante sustentadas en su propia autoridad y cuáles son las que requieren la intervención de niveles superiores de comando. Las reglas de empeñamiento contribuyen a definir qué procedimientos y qué estándares son esenciales en el contexto de una conducción eficaz y civilizada de los conflictos bélicos.

El presente trabajo intenta inducir el inicio de un intercambio de opiniones entre autoridades políticas y comandantes militares que lleve a las Fuerzas Armadas de Argentina y de otros países de la Región a contar con un conjunto de reglas de empeñamiento que impliquen un sustantivo agregado de valor, específicamente, en el ámbito de la Defensa Cibernética.

Se menciona "Fuerzas Armadas de Argentina y de otros países de la Región" pues, desarrollar y poner en vigencia Ciber reglas de empeñamiento a nivel Región evidencia numerosas ventajas competitivas. Sólo como un ejemplo de dicha sinergia positiva se cita la posibilidad de desarrollo conjunto de capacidades que llevan al plano de las realizaciones concretas a las Ciber reglas de empeñamiento más sofisticadas, tanto desde el punto de vista tecnológico como en el de su implementación política.

El proceso de intercambio de opiniones propuesto, necesariamente, deberá tener un enfoque de perfeccionamiento continuo. Bastan como justificación de ello los cambios tecnológicos permanentes en el "quinto dominio"[55] de los conflictos militares entre estados naciones. Dichos cambios en el "quinto dominio" son de una velocidad tal que, ni siquiera admite ser comparada con la velocidad con la que evolucionan las características de los cuatro dominios anteriores.

Las reglas de empeñamiento en el "quinto dominio", que surjan como consecuencia de la aplicación de un enfoque metodológico robusto y claro, no deberán estar restringidas, necesariamente, por las actuales capacidades; todo lo contrario, la aplicación del citado enfoque metodológico deberá también ser orientadora respecto del esfuerzo de investigación y desarrollo que lleve a la adquisición de nuevas capacidades que resulten necesarias.

[54] Encyclopædia Britannica http://www.britannica.com/topic/rules-of-engagement-military-directives

[55] Primer dominio: operaciones terrestres; segundo dominio: operaciones navales; tercer dominio: operaciones aéreas; cuarto dominio: operaciones en el espacio exterior y quinto dominio: operaciones en el ciberespacio (dominio virtual)

** Director del Doctorado en Ingeniería Informática de la Universidad Nacional de San Luis - Argentina. Investigador Categoría I – Programa de Incentivo a la Investigación en Universidades Nacionales de Argentina. Consultor en Ciberdefensa.*

El presente trabajo, en su primera parte, pone énfasis en una cierta "zona gris" que se verifica en los Ciber Conflictos militares entre estados naciones. Al respecto: Cuando los efectos de un Ciber Ataque militar, reconocido como tal, sean equivalentes a los causados por "Ataques Armados" o "Desembarcos hostiles de unidades militares", dicho Ciber Ataque militar deberá, en principio, tener un tratamiento que guarde analogía y proporcionalidad con las citadas equivalencias. Sin embargo, otras Ciber Agresiones, por ejemplo, la toma de control de un satélite de comunicaciones por parte del estado agresor o acciones de Ciber Reconocimiento (detección de vulnerabilidades), quedan comprendidos en la mencionada "zona gris". Como se anticipó, este artículo intenta acotar este espacio de problema suministrando elementos de juicio en el campo de las denominadas Ciber Contramedidas. Casualmente, existe una tendencia a denominar "Ciber Contramedidas" a las acciones militares llevadas a cabo para contrarrestar Ciber Agresiones comprendidas en dicha "zona gris" [4]. Las "Ciber Contramedidas" deberán constituir un ámbito prioritario en el ámbito de las Ciber reglas de empeñamiento.

Este trabajo, en su segunda parte y a partir de las ideas del estudioso australiano Tobias Feakin [5][6], intenta suministrar algunas de las bases necesarias para elaborar un enfoque metodológico robusto y claro en el ámbito de las reglas de empeñamiento. Una de las características más saliente de los Ciber Conflictos militares la constituyen los plazos dramáticamente breves en los que deben tomarse decisiones muy importantes. Si un Ciber Ataque militar provoca un estado deliberativo prolongado entre autoridades políticas del área Defensa y comandantes militares, dicha agresión ya puede ser considerada exitosa. La expresión "la ignorancia lo vuelve todo estratégico"[56] cobra en este ámbito una inusitada importancia. Por ejemplo, decisiones relacionadas con la ejecución de "backtracking" (identificación del Ciber Agresor) deberán ser tomadas en algunos segundos para que sean exitosas, por ejemplo; esto deviene en dramático cuando el Ciber Agresor utiliza esquemas del tipo "onion routers" (ruteadores enmascarados) para incrementar su anonimidad.

Finalmente este trabajo incluye propuestas dirigidas a autoridades políticas del área Defensa de Argentina y de otros países de la Región. Los comandantes militares que directa o indirectamente tengan incumbencias en el ámbito de los Ciber Conflictos militares también son destinatarios deseados de las sugerencias y modestos aportes contenidos en este artículo.

El autor se sentiría honrado si este escrito fuera evaluado académicamente en instituciones de formación de alto nivel de oficiales jefes y oficiales superiores de las Fuerzas Armadas de Argentina y de otros países de la Región. La opinión profesional de integrantes de elementos de Defensa Cibernética, a nivel conjunto y de cada una de las FFAA[57], será también bienvenida.

El propósito autoimpuesto del autor se cumpliría plenamente si logra aportar, aunque lo sea mínimamente, a la definición de Ciber reglas de empeñamiento militar para Argentina y otros países de la Región acordes con el escenario global actual de los conflictos militares en el Ciberespacio. También sería gratificante si se logra contribuir en el sentido de que, en la definición de Ciber reglas de empeñamiento, se utilice un enfoque metodológico robusto y claro y si las citadas Ciber reglas de empeñamiento quedan comprendidas en un efectivo proceso de mejora continua.

El estudio de las contribuciones de Katharine Hinkle, de la Universidad de Yale y de Tobias Feakin, del Council on Foreign Relations de Australia posibilitaron, al autor de esta contribución, la elaboración de las propuestas

[56] Dicha expresión en realidad deriva de algunas escuelas de pensamiento estratégico de Francia. El autor solía utilizarla con frecuencia años atrás. Se refiere a los mandos medios con características pusilánimes que requieren un estado de "consulta permanente" con sus superiores.

[57] También de Argentina y otros países de la Región.

contenidas en este escrito. Los mencionados estudiosos están citados varias veces en este artículo.

1. Las Ciber Agresiones militares entre estados naciones y sus potenciales contramedidas

Los Ciber Conflictos, que involucran al poder militar de estados naciones, están evolucionando muy rápidamente desde una posibilidad teórica analizada por estudiosos, hacia amenazas muy concretas e inminentes. Muchos analistas del tema se han focalizado en dirimir cómo el derecho internacional [7][8][9] podría ser aplicado en este nuevo ámbito de problema.

En este entorno, un tema muy sensitivo ha venido siendo objeto de debates específicos: Cómo definir qué tipos de Ciber Ataques constituyen claramente "Ataques Armados" o son equivalentes a "Desembarcos Hostiles de unidades militares". En otras palabras, cuándo el estado nación agredido adquiere el derecho a ejercer su legítima defensa amparado en el Artículo 51 de la Carta de las Naciones Unidas.

Las respuestas a este interrogante que lucen más adecuadas provienen de estudios basados en los efectos de las Ciber Agresiones. En este ámbito, la clave consiste en determinar en qué casos el impacto de un Ciber Ataque en particular se parece o es análogo a los causados por una fuerza militar "tradicional". Un ejemplo específico encuadrado en esta catalogación lo constituye la voladura, mediante Ciber Armas, de importantes instalaciones nucleares o refinerías de petróleo. El problema de este enfoque es que, en principio, dejaría fuera del concepto de "Ataque Armado" o "Desembarcos Hostiles de unidades militares", según el derecho internacional, a una amplia gama de daños producidos por Ciber Incidentes. La toma de control de un satélite de comunicaciones por un período prolongado o el recorrido de la grilla eléctrica del estado nación agredido, detectando sus vulnerabilidades, son ejemplos comprendidos en la citada "zona gris".

Recapitulando parcialmente: En el contexto de un análisis "basado en los efectos", un amplio rango de Ciber Acciones destructoras y/o disruptivas quedarían fuera del ámbito de "Ataque Armado" o "Desembarcos Hostiles de unidades militares" según lo que define el derecho internacional. Aplicar Ius ad bellum (legítimas razones) con criterios "tradicionales" exclusivamente, posiciona al país agredido en una situación de extrema debilidad.

El escenario que se está describiendo se complica aún más pues las Ciber Hostilidades que no sobrepasan el umbral de "Ataque Armado" o de "Desembarcos Hostiles de unidades militares", están teniendo un predominio creciente en el contexto internacional. Conviene destacar que aquellos usos aparentemente menores del "Ciber Poder" pueden tener efectos disruptivos importantes y también constituyen graves amenazas. Es un hecho que los estados naciones necesitan reaccionar ante ellos rápida y efectivamente.

A esta altura conviene citar que se ha dado en denominar "contramedidas" [10] a las acciones temporariamente lícitas, emprendidas por el estado nación agredido, en respuesta a conductas equívocas de otros estados naciones. Las contramedidas constituyen respuestas aceptables en el contexto del derecho internacional. Como tales, las contramedidas tienen el potencial necesario como para jugar un rol central en las respuestas que los estados naciones agredidos elaboren para encarar reacciones ante determinadas Ciber Intrusiones.

En los ejemplos ya expuestos de la toma de control de un satélite de comunicaciones y en el de la Ciber detección de vulnerabilidades en la grilla eléctrica de un país, la destrucción de los

Servidores de Comando y Control de las mencionadas Ciber intrusiones, desarrollada como respuesta por el estado agredido, sería

un claro ejemplo de "contramedida" según el uso que se le da a ese término en este artículo.

Dicho en otros términos: Respaldado por normas consuetudinarias del derecho internacional [4], un estado tiene derecho a reaccionar, legalmente, ante una violación de sus derechos o soberanía, por parte de otro estado. Esta reacción puede serlo mediante una contramedida, la que, sin la violación origen del conflicto, violaría el derecho internacional; este tipo de contramedidas pueden prolongarse tanto tiempo como los hechos y/o situación que la justifica se mantengan.

A pesar de que las contramedidas pueden tener alguna aplicabilidad importante en los conflictos en el Ciberespacio, poco ha sido escrito respecto de cómo sería (o es) exactamente el marco legal que regule su aplicación. Este trabajo busca contribuir, fundamentalmente siguiendo a la estudiosa de la Universidad de Yale, Katharine Hinkle [4], a llenar el vacío mediante aportes y sugerencias que podrían quedar incluidos en la Estrategia de Ciber Defensa de Argentina u otros países de la Región.

Un tópico a ser estudiado seriamente lo constituye la presunción de algunos expertos de que, Ciber Tácticas asociadas a las contramedidas, por su naturaleza y aspectos instrumentales, perturban la evaluación de los requisitos de necesidad y proporcionalidad que deben ser respetados para que, las contramedidas encaradas por el estado nación atacado, sean aceptadas como legítimas por la comunidad internacional.

En particular, las contramedidas "en reciprocidad", las cuales han sido citadas por el Departamento de Defensa de EEUU[58] y varios estudiosos como un efectivo y aceptable modo de reacción, en el contexto del Ciberespacio, presentan problemas serios para encontrarles sustento en diversos regímenes legales. Esto constituye un desafío de búsqueda de un marco legal apropiado y ampliamente aceptado, a las respuestas que deben encarar los países atacados, en un escenario de Ciber Conflictos entre estados naciones posicionados en la "zona gris" citada más arriba.

Las "contramedidas" que se incluyan en las Ciber reglas de empeñamiento deberán ser minuciosamente estudiadas por los expertos de mayor nivel en derecho internacional de Argentina y otros países de la Región.

2. Respuesta adecuada a Ciber Ataques lanzados o respaldados por estados naciones

Como ya se ha venido mostrando, la naturaleza virtual de las Ciber Agresiones militares dificulta una definición sencilla de Ciber reglas de empeñamiento militar, precisas y tajantes. Tobias Feakin, estudioso perteneciente al Council on Foreign Relations de Australia y director del Centro Internacional de Ciber Políticas en el Instituto Australiano de Políticas y Estrategia [5][6], recientemente ha desarrollado interesantes aportes que se tendrán en cuenta en el desarrollo de este punto del presente artículo.

Basado ampliamente en el derecho internacional, Feakin asevera que, cuanto la componente cibernética de un ataque militar, proveniente de otro u otros estados naciones sea predominante, las autoridades del estado nación atacado deberán encarar el desafío de desarrollar respuestas militares que provoquen, en los atacantes, perjuicios y daños proporcionales a los recibidos.

Definir una respuesta militar oportuna, proporcional, legal y dirigida a los blancos militares correctos, es complicado; es difícil evaluar ajustadamente y "en tiempo real" el daño causado por el oponente a los intereses nacionales. Entre otras razones las dificultades devienen por el uso frecuente de proxies (servidores en los que se "delega" las tareas de Comando y Control del Ciber Ataque). Que sea complicado elaborar las citadas respuestas no significa que no haya que trabajar en este

[58] https://fas.org/irp/doddir/dod/i8500_01.pdf

ámbito sino todo lo contrario; requieren una muy profunda dedicación.

Es sabido que los autores del ataque pueden, con cierta facilidad, negar sus responsabilidades sustentando "sólidamente" sus aseveraciones. Esto frustra los esfuerzos para dirimir responsabilidades en los estados no preparados para estas circunstancias. La experiencia acumulada en este contexto lleva a pensar que, las políticas seguidas para elaborar la mayoría de las respuestas a Ciber Ataques, lo han sido del tipo "ad hoc". En este caso "ad hoc" tiene un alcance semántico muy cercano a "improvisación".

Para determinar la respuesta adecuada a un Ciber Incidente (agresión), originado o solventado por un estado nación, las autoridades del país agredido deben considerar tres variables: i) la confianza de la propia comunidad de inteligencia en lo que respecta a su capacidad para lograr la atribución de responsabilidades, ii) para evaluar el impacto causado por el incidente y iii) para estimar la capacidad de "apalancamiento" (uso conjunto) de las capacidades a disposición del estado nación agredido.

Si bien los tres aspectos mencionados ayudarán en la elaboración de los lineamientos para definir la respuesta a un Ciber Ataque militar disruptivo o destructivo, las autoridades de un estado nación también tendrían que dar dos pasos deseablemente previos al primer Ciber Incidente. En primer término las autoridades del estado nación deberían trabajar con líderes del sector privado para determinar (evaluar "ex ante") el efecto esperado de un Ciber Incidente en el contexto de la operatoria de sus respectivos negocios. En segundo lugar, los gobiernos deberían desarrollar un menú de opciones de respuesta planeadas / determinadas de antemano y evaluar el impacto potencial en el agresor de cada opción de respuesta, lo sea en lo político, en la economía, en la inteligencia y en ámbitos / instalaciones específicamente militares.

2.1. Algunos fundamentos conceptuales y fácticos: Los incidentes cibernéticos y la incertidumbre

Aun cuando, en el panorama internacional, el número de ocurrencias de Ciber Ataques altamente disruptivos y destructivos crece, muchos gobiernos continúan sin prepararse adecuadamente.

En otras áreas, llamativamente, las respuestas del poder político de estados naciones, a potenciales agresiones patrocinadas por otros estados, están bien establecidas. Por ejemplo, un país puede tener previsto expulsar a diplomáticos como respuesta a un escándalo de espionaje; si un estado nación considera que su soberanía territorial ha sido violada, puede presentar una demanda ante organismos internacionales y asimismo puede hacer uso de la fuerza en respuesta a un ataque armado.

En contraposición no existen, en la mayoría de los casos, políticas vigentes ni reglas de empeñamiento militar que aporten para definir respuestas claras a Ciber Ataques militares; esto lo es por dos razones:

En primer lugar, es difícil evaluar "casi en tiempo real" los daños causados por los Ciber Incidentes. Sirven como comparación los siguientes ejemplos: Puede tomar semanas, incluso meses, a expertos en informática forense, la determinación, en forma precisa y concluyente, del alcance de los daños causados a las redes informáticas y otros sistemas de una organización afectados por un Ciber Ataque. Por ejemplo, para las autoridades sauditas fueron necesarias aproximadamente dos semanas para estimar la magnitud de los daños del Ciber Incidente Shamoon (Saudi Aramco)[59]. Se borraron los datos de treinta mil de las computadoras de la Saudi Aramco. Aunque estas dos semanas pueden ser poco tiempo para estándares de informática forense con un enfoque policial / judicial, como contraposición se destaca que, un militar idóneo en el tema,

[59] https://www.iiss.org/en/publications/survival/sections/2013-94b0/survival--global-politics-and-_strategy-april-may-2013-b2cc/55-2-08-bronk-and-tikk-ringas-e272

debería poder llevar a cabo una evaluación de los daños de incidentes en tan sólo unas horas. En casos de incidente que utilicen herramientas de Ciber Anonimidad las primeras decisiones militares deberían tomarse en plazos aún mucho más breves.

En segundo lugar, el atribuir los Ciber Incidentes a su patrocinador, sigue siendo un desafío significativo. Enmascarar el verdadero origen de un Ciber Incidente es fácil. Los estados naciones agresores a menudo utilizan proxies o equipos "representantes", basados en otras jurisdicciones, para ocultar sus huellas.

Respecto de la Ciber Anonimidad viene al caso mencionar al "Ciber Califato", grupo que se adjudicó la responsabilidad de la toma del control de la televisora francesa TV5 Monde, manteniéndola fuera del aire, mediante un Ciber Ataque, en abril de 2015; el "Ciber Califato" también se adjudicó la utilización de otros medios de comunicación social de dicha empresa televisiva para publicar contenidos en apoyo al autoproclamado Estado Islámico. Dos meses más tarde, medios de comunicación franceses, informaron que los verdaderos agresores habrían sido, en realidad, grupos patrocinados por Rusia[60] y no elementos pro Estado Islámico.

Aún en los casos en los que es posible identificar al Ciber Agresor, eso no garantiza que dicha identificación sea creíble, tanto respecto de la opinión pública doméstica como para la internacional; esta falta de crédito se verificará a menos que las autoridades del país agredido expongan, creíblemente, los conceptos, métodos y herramientas utilizados para resolver el "Problema de la Atribución", es decir, cómo se trabajó para determinar la identidad del Ciber Agresor.

En un contexto de fuerte presión y plazos perentorios, suele ocurrir que las respuestas respecto de la identidad del Ciber Agresor se suministren, frecuentemente, con evidencia incompleta; lo mencionado provoca un alto grado de escepticismo en el público, tanto interno como externo. Errores en la atribución de un Ciber Incidente podrían provocar una respuesta orientada a blancos equivocados, provocando serias crisis.

Asimismo, evaluaciones de daños apresuradas, podrían llevar a una sobreestimación de los efectos de un Ciber Incidente, provocando que el estado nación agredido responda de manera desproporcionada.

2.2. El desarrollo de una respuesta proporcionada

Las autoridades de un estado nación deben considerar tres variables antes de elaborar la respuesta a un Ciber Ataque.

En primer lugar deben contar con una ajustada evaluación del nivel de confiabilidad que sus agencias de inteligencia tienen para resolver el "Problema de la Atribución" (de un Ciber Ataque). Aunque existen registros de éxitos de agencias de inteligencia detectando actividad maliciosa en el Ciberespacio, el Ciber análisis forense no está suficientemente perfeccionado en muchos países. El grado de certeza en la resolución del "Problema de la Atribución" tendrá un impacto directo en la elaboración de la respuesta. Por ejemplo, si el nivel de certeza de la atribución es bajo, las autoridades estarán limitadas en la selección de la respuesta aunque la severidad del ataque haya sido alta. Esto forzará a seleccionar un objetivo de represalia menos importante para limitar las posibilidades de que escale un conflicto internacional sin fundamentos evidentes y/o recibir críticas desfavorables de la comunidad internacional.

Asimismo pueden registrase casos en los que la evidencia sea tan débil y/o escasa que induzca a una no respuesta por parte del estado nación víctima.

En segundo lugar, las autoridades del estado nación agredido deben evaluar los efectos de

[60] http://blog.trendmicro.com/tv5-monde-russia-and-the-cybercaliphate/

los Ciber Incidentes tanto en la infraestructura crítica, como en la sociedad en general, en la economía y también en los intereses nacionales considerados integralmente. Las preguntas que requieren respuestas confiables en este entorno son del tipo: ¿Cuál fue el daño causado en los sistemas afectados?, ¿Hubo algún impacto a la infraestructura crítica? ¿Qué tipo de servicios esenciales están afectados? ¿Provocó el incidente una importante pérdida de estabilidad en la economía? ¿Cuál fue el impacto de los incidentes en la seguridad nacional y en el prestigio del país?

En tercer lugar, las autoridades deben considerar las alternativas de respuestas diplomáticas, económicas, y militares a su disposición; desde un reclamo diplomático hasta un ataque militar. Las respuestas no deben, necesariamente, limitarse al ámbito del Ciberespacio; nada impide, a un estado nación, el uso de otros canales; eso sí, deberá considerarse que cada uno de ellos, normalmente, tendrá aparejados sus propios riesgos.

Las Ciber respuestas pueden ser llevadas a cabo en forma complementaria de las respuestas diplomáticas, económicas y militares convencionales. Sin embargo ellas se ejecutan, muchas veces, en forma encubierta. Estas respuestas presentarán dificultades para ser desarrolladas rápidamente si el gobierno no ha adquirido, previamente, capacidades para accionar contra un blanco específico. Estas capacidades, posiblemente, habrán sido adquiridas previamente mediante Ciber Reconocimientos / Ciber Análisis de Vulnerabilidades.

Muchas veces, un público reconocimiento de una Ciber Respuesta, por parte del estado nación agredido, puede caer como algo "políticamente poco atractivo". Dicho estado nación podría perder "espacio de maniobra política" para lanzar respuestas similares, en el futuro, contra otros blancos. Aunque los estados pueden trasladar las responsabilidades de respuesta a "proxies" (Servidores de Comando y Control "delegados"), se ha verificado que dicha acción puede limitar su propio control sobre las respuestas y llevar a que el conflicto escale.

2.3. Algunos lineamientos metodológicos para elaborar una respuesta adecuada a Ciber Ataques lanzados y/o respaldados por estados naciones utilizando su poder militar

Considerando la significativa presión a la que seguramente serán sometidos los gobiernos cuando tengan que, efectivamente, dar respuesta a Ciber Ataques, las autoridades políticas y comandantes militares deberían elaborar un marco general que catalogue las respuestas alternativas "tipo" y que contenga sus lineamientos generales, adelantándose a la ocurrencia efectiva de Ciber Incidentes disruptivos o destructivos con características militares.

Aunque cada respuesta tendrá su propia especificidad, dicho marco general permitirá, a las autoridades del estado nación, considerar con la rapidez necesaria las diversas opciones de respuesta para cada caso en particular.

Un esquema general de un marco para dar soporte al proceso de toma de decisiones, en este contexto, se muestra en la siguiente figura a la se denomina "Matriz de Tobias Feakin modificada"[61]. Dicho esquema general debería ser completado / perfeccionado por los integrantes de los elementos de Defensa Cibernética a nivel Conjunto y los correspondientes a cada Fuerza Armada de Argentina (y países de la Región). La intervención de instituciones académico / militares será muy valiosa. En el caso de Argentina se cita a las Escuelas Superiores de Guerra de las FFAA, a la Escuela Superior de Guerra Conjunta, a la Escuela Superior Técnica del Ejército Argentino y al Instituto Universitario Aeronáutico de Argentina

En dicho esquema, en la primera columna, se citan ejemplos de diferentes niveles de

[61] Modificada por el autor de este artículo

severidad de Ciber Agresiones de origen militar.[62] En la segunda columna se mencionan, también a título de ejemplo distintos tipos de respuesta a cada tipo de Ciber Agresión militar.

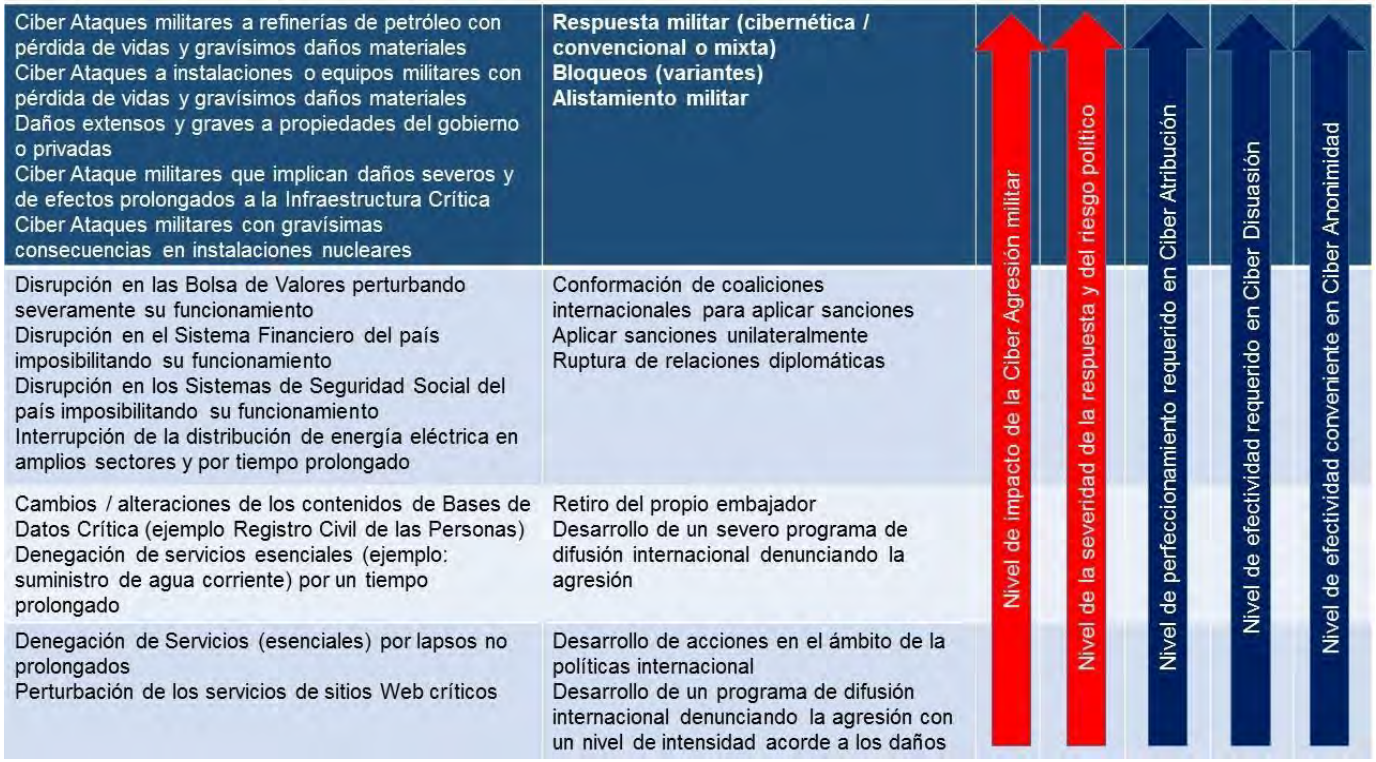
La flecha insertada en la tercera columna consolida el modelado del nivel creciente de la severidad de los daños causados por potenciales Ciber Agresiones militares.

En la cuarta columna la flecha modela el nivel creciente de severidad, esta vez, de la potencial respuesta a una Ciber Atención militar.

resolución de dicho "Problema de la Atribución".

En la sexta columna de la "Matriz de Tobias Feakin modificada" se modela el nivel deseable de capacidad de Ciber Anonimidad que debería disponerse en cada caso.

En la séptima y última columna está modelado el nivel de Ciber Disuasión que es deseable sea alcanzado para no ser percibido como "blanco apetecible" en cada uno de los casos planteados como ejemplo.



La quinta columna contiene una flecha que indica la importancia creciente de la necesidad de que nuestro país adquiera capacidades para resolver las variantes del "Problema de la Atribución", aún en los casos más complejos. Al respecto se ruega tener en cuenta el artículo del autor en el que se tratan, en forma conjunta la Ciber Atribución, la Ciber Anonimidad y la Ciber Disuasión[63]. En este contexto se recomienda no adherir al mito, difundido con gran entusiasmo por diversos actores, de la no

Teniendo en cuenta el impacto del Ciber Incidente, las opciones políticas y el principio de la proporcionalidad y, por otro lado, la Ciber Atribución, la Ciber Disuasión y la Ciber Anonimidad, la figura sugiere cómo podría llegar a tener, completando / perfeccionando dicho esquema, una visión general de las posibilidades de respuesta del estado nación agredido. La "Matriz de Tobias Feakin modificada" facilita la definición de los componentes de la respuestas a Ciber Incidentes varios, especialmente los que manifiesten tendencias a un escalamiento.

El modelo permite ordenar en niveles los posibles efectos de Ciber Ataques militares,

[62] Se presupone que ya se ha desarrollado la capacidad forense para distinguir, con una muy alta probabilidad asociada, las Ciber Agesiones de origen militar del Ciber Terrorismo, del Ciber Crimen, etc

[63] "El Problema de la Ciber Atribución: Aportes para una estrategia de Ciberdefensa" publicado en el blog "Espacio Estratégico" y distribuido por el Consejo Argentino de Relaciones Internacionales

citando como ejemplos desde alteraciones funcionales en sitios web sensitivos, en un extremo de la escala, hasta Ciber Ataques militares a refinerías de petróleo con pérdida de vidas y gravísimos daños materiales, en el extremo opuesto. Esto se grafica mostrando su relación con ejemplos de posibles niveles de las respuestas, las que van desde declaraciones de repudio en los medios de comunicación hasta réplicas eminentemente militares (cibernéticas, convencionales o mixtas).

Considerando el espectro de respuestas posible, habrá distintos riesgos políticos y legales asociados a cada decisión; estos riesgos aumentan al incrementarse el nivel de severidad de la respuesta. Las respuestas definidas utilizando este marco general de referencia son aplicables a Ciber Agresiones militares, es decir, respaldadas por los estados naciones agresores. Para Ciber Agresiones disruptivas y destructivas, causadas por individuos, organizaciones criminales u otras, llevadas adelante sin que conste el respaldo de un estado nación, serán más apropiadas respuestas originadas y elaboradas por organismos policiales nacionales e internacionales.

Tal como ocurre en varias áreas de las relaciones internacionales, la proporcionalidad debe ser un enfoque de práctica habitual en Ciber Defensa.

Las autoridades políticas del estado Ciber agredido tienen varias alternativas previas a la utilización plena del poder militar en el Ciberespacio. La expulsión de diplomáticos, por ejemplo, en respuesta a Ciber Agresiones militares de severidad mediana / leve, que afecten la soberanía, es percibida como una respuesta proporcional, fundamentalmente porque los estados naciones la han venido asumiendo, como práctica habitual, por décadas.

Cuando un estado nación aplica sanciones económicas, el estado sancionado, a menudo, responde del mismo modo. En este contexto Rusia respondió a las sanciones que le fueron aplicadas por la anexión de Crimea[64][65][66]con sus propias sanciones. La misma lógica se suele aplicar en incidentes en el Ciberespacio.

En los casos en los que exista "la tentación" de responder no proporcionalmente, de manera de disuadir o impedir futuros ataques, conviene recordar que el derecho internacional requiere que los estados naciones solo lleven adelante las medidas de fuerza necesarias y adecuadas para repeler o derrotar Ciber Ataques disruptivos o destructivos. Se deben considerar límites claros a la "escala, alcance, duración e intensidad" de las acciones que el estado nación víctima del Ciber Ataque militar pueda tomar en respuesta.

Adicionalmente, cuando las citadas respuestas respetan la proporcionalidad, pueden facilitar la construcción de coaliciones internacionales que a veces son necesarias para aislar y sancionar al estado nación atacante, así como para limitar la probabilidad de que el conflicto escale sin control.

Si, por ejemplo, un país fuera víctima de perturbaciones en el funcionamiento de sitios web sensitivos y ello fuera consecuencia de un Ciber Ataque patrocinado por otro estado, una denuncia pública en foros internacionales, debidamente sustentada, será probablemente la respuesta más apropiada. Yendo más arriba en la escala, cualquier Ciber Agresión militar que implique la manipulación o destrucción de datos importantes para el gobierno podría requerir acciones diplomáticas como respuesta apropiada; estas podrían consistir en declaraciones de tipo políticas en los casos de bajo impacto o en la expulsión de diplomáticos si los Ciber Ataques afectan en forma grave, por ejemplo, la economía de los estados naciones víctimas.

En los casos en los que la economía esté Ciber afectada, se podría utilizar una gama o conjunto de respuestas en el plano económico coordinadas con las acciones diplomáticas. Si

[64] http://www.bbc.com/news/world-europe-26644082
[65] http://www.forbes.com/forbes/welcome/
[66] http://abcnews.go.com/Politics/obama-announces-sanctions-punish-russia-crimea- invasion/story?id=22939730

un Ciber Incidente militar causa daños físicos graves y pérdida de vidas, tal la voladura de una instalación nuclear, podría llegar a considerarse una opción militar, cibernética o no, como respuesta apropiada y proporcional.

La evaluación rápida de la severidad del incidente juega un rol importante en estos casos. Todas estas opciones pueden complementarse con Ciber Acciones encubiertas, las que también, a pesar de su anonimidad, tendrán que ser proporcionales al daño causado por el Ciber incidente.

La infraestructura crítica normalmente constituye una prioridad para los Ciber Atacantes; es importante que los operadores de los componentes de la infraestructura crítica participen en el perfeccionamiento del marco general de respuesta ("Matriz de Tobias Feakin modificada" u otro que la supere). Asimismo, los operadores de los componentes de la infraestructura crítica están en una buena posición para asesorar a las autoridades políticas y a los comandantes militares acerca de Ciber Incidentes que puedan afectar sus operaciones y para definir cuán grave serían las consecuencias dichos incidentes.

Por otro lado, las autoridades políticas y comandantes militares deben evaluar los costos asociados con cada respuesta potencial que derive de la "Matriz de Tobias Feakin modificada".

También se debe considerar que cada respuesta tendrá asociada un determinado impacto en las relaciones diplomáticas del estado y en su reputación internacional en general.

Los Ciber Incidentes requieren de los gobiernos y comandantes militares un conjunto muy complejo de decisiones. Se debe poder evaluar muy rápidamente la gravedad del incidente, analizar las alternativas de respuestas adecuadas y evaluar dinámicamente los riesgos asociados a los diversos cursos de acción.

Un marco de referencia construido con antelación, deliberadamente simplificado, tal como lo es la "Matriz de Tobias Feakin modificada", provee un modelo para elaborar un método que sea útil para definir y para encuadrar las potenciales respuestas alternativas cuando ocurran Ciber Ataques de origen militar promovidos / respaldados por otros estados naciones.

Adicionalmente un modelo elaborado a partir de la "Matriz de Tobias Feakin modificada", podría suministrar a las autoridades políticas del área Defensa de un estado nación y a sus comandantes militares, un punto de partida, útil como referencia, para realizar sus evaluaciones durante el desarrollo de crisis reales.

3. Propuestas

3.1. Las Ciber reglas de empeñamiento deberían constituir un ámbito de estudio prioritario, y con un enfoque de mejora continua, en las Escuelas Superiores de Guerra de las FFAA de Argentina (y las de otros países de la Región), de la Escuela Superior de Guerra Conjunta, de la Escuela Superior Técnica del Ejército Argentino y del Instituto Universitario Aeronáutico de Argentina. Las Ciber reglas de empeñamiento, asimismo, deberían ser motivo de permanente perfeccionamiento en los ámbitos correspondientes a los elementos de Defensa Cibernética a nivel conjunto y de cada una de las FFAA de Argentina. Las autoridades políticas del Ministerio de Defensa de Argentina y de otros países de la Región, interactuando con el área Relaciones Exteriores, deberán definir cuál es la versión de las citadas Ciber reglas de empeñamiento que está en vigencia en un período determinado.

3.2. Las autoridades políticas del área Defensa y los comandantes militares deberían evitar, sistemáticamente, que se recurra al mito de "la no solución del Problema de la

Atribución" en los intercambios de opiniones acerca de las Ciber reglas de empeñamiento. Internacionalmente y en Argentina ya se ha probado, conceptual e instrumentalmente, que dicho "Problema de la Atribución", en varias de sus variantes, admite solución con una muy alta probabilidad de éxito y una muy baja tasa de falsos positivos.[676869707172] La solución de las variantes más complejas del "Problemas de la Atribución" simplemente son indicadoras de la necesidad de un mayor esfuerzo de Investigación y Desarrollo; de ninguna manera el Problema de la Atribución debería ser el respaldo de puntos de vista pesimistas cuando se discutan las Ciber reglas de empeñamiento. Argentina cuenta con RRHH que podrían ser aplicados a la búsqueda permanente de distintas soluciones a variantes diversas, reales y potenciales, del "Problema de la Atribución".

3.3. Las autoridades políticas del área Defensa y comandantes militares de Argentina[73] podrían disponer que las Escuelas Superiores de Guerra de las FFAA de Argentina, la Escuela Superior de Guerra Conjunta, de la Escuela Superior Técnica del Ejército Argentino y el Instituto Universitario Aeronáutico de Argentina, elaboren versiones superadoras de la presente contribución. Los elementos de Defensa Cibernética a nivel conjunto y de cada una de las FFAA de Argentina podrían consolidar dichas versiones superadoras en un documento rector a ser presentado a las autoridades políticas. Se remarca que, si bien debe existir una versión de las Ciber reglas de empeñamiento vigente, dichas Ciber reglas de empeñamiento deberán estar sometidas a un proceso de mejora continua en consideración de la permanente evolución de los aspectos tecnológicos asociados.

3.4. Los trabajos que se propone sean elaborados por las Escuelas Superiores de Guerra de las FFAA de Argentina, la Escuela Superior de Guerra Conjunta, de la Escuela Superior Técnica del Ejército Argentino y del Instituto Universitario Aeronáutico de Argentina y consolidados por los elementos de Defensa Cibernética a nivel conjunto y de cada una de las FFAA de Argentina, deberían corresponderse con el producto de un enfoque metodológico robusto y claro.

3.5. Las autoridades políticas del área Defensa y comandantes militares, a juicio personal del autor, no deberían considerar que Argentina y otros países de la Región poseen desventajas comparativas en el ámbito de la Defensa Cibernética. Ocurre todo lo contrario; existen posibilidades concretas de posicionarse con ventajas, en el contexto global, en el típicamente asimétrico escenario del Ciberespacio visto como escenario muy probable de conflictos militares. El autor, quien posee experiencia en la coordinación de programas de cooperación internacional en el ámbito de la Tecnología de la Información, está plenamente convencido de lo propuesto en este punto. Nuestros RRHH, debidamente entrenados, seguramente permitirán que nuestro país, y otros de la Región, cuenten con Ciber reglas de empeñamiento que constituyan una referencia global.

3.6. Una vez que las autoridades del Ministerio de Defensa hayan definido las Ciber reglas

---

[67] Bilge, Leyla, et al, "DISCLOSURE: Detecting Botnet Command and Control Servers Through Large-Scale NetFlow Analysis", Symantec Research Labs et al, 2012 https://www.acsac.org/2012/openconf/modules/request.php?module=oc_program&action=view.php& a=&id=73&type=4

[68] Evento comprendido en el "PROGRAMA DE VINCULACIÓN Y DIFUSIÓN CIBERDEFENSA Y SEGURIDAD DE REDES DE COMUNICACIONES, JORNADA REGIONAL EN BS. AS, Escuela Superior Técnica del Ejército Argentino, 2 de septiembre de 2014. El autor de este trabajo fue invitado a exponer sobre "Detección de Ciber Agresiones mediante el análisis de flujos de redes a gran escala". Ver detalles en http://wp.iese.edu.ar/?p=3871

[69] Baieli, Claudio, Tesis de Maestría, Universidad Nacional de San Luis (Argentina) / Universidad Federal de Minas Gerais (Brasil), 2015

[70] Uzal, R. et al "Internet Roadmap topics: Freedom and Security in Cyberspace - A Cyber Defense perspective", NETmundial, São Paulo, Brazil, 3, 24 - April 2014 http://content.netmundial.br/contribution/internet-roadmap-topics-freedom-and-security-in- cyberspace-a-cyber-defense-perspective/61

[71] Uzal, R. Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (SBSeg)- Conferencista invitado http://www.sbseg2014.dcc.ufmg.br/programacao/

[72] http://resources.infosecinstitute.com/attribution-problem-in-cyber-attacks/

[73] y también de otros países de la Región.

de empeñamiento correspondientes a Ciber Agresiones militares (es decir patrocinadas por otro/s estado/s) y también hayan definido las pautas metodológicas para mantenerlas permanentemente actualizadas, habrá llegado el momento de consensuarlas / perfeccionarlas interactuando con el área Relaciones Exteriores de la conducción política del estado nación. Las Ciber reglas de empeñamiento entrarán en vigencia cuando así lo disponga quien ejerce el Comando en Jefe de las FFAA (Presidencia de la Nación)

4. Referencias

[1] Elementos de juicio al respecto en: http://www.pbs.org/wgbh/pages/frontline/haditha/themes/roe.html [2] Aportes adicionales en: http://www.loc.gov/rr/frd/Military_Law/Military_Law_Review/pdf-files/27687D~1.pdf

[3] Trama, Gustavo, "Reglas de Empeñamiento I, II y III", Biblioteca de la Escuela Superior de Guerra Conjunta de las FFAA de Argentina, Contribución Académica, 2014

[4] Hinkle, Katharine C., "Countermeasures in the Cyber Context: One More Thing to Worry About", The Yale Journal of International Law Online, 2011.

[5] https://www.aspi.org.au/research/find-an-expert/tobias-feakin

[6]http://www.cfr.org/cybersecurity/developing-proportionate-response-cyber- incident/p36927

[7] Hathaway, Oona et al "THE LAW OF CYBER-ATTACK", Forthcoming in the California Law Review, 2012 http://www.law.yale.edu/documents/pdf/cglc/LawOfCyberAttack.pdf
[8] CCDCOE, "Tallinn Manual identifies the international law applicable to cyber warfare", https://ccdcoe.org/tallinn-manual.html, 2008

[9] Harvard Law School, http://pilac.law.harvard.edu/events/cyber-operations-and-international-humanitarian-law-fault-lines-and-vectors, 2015

[10] CCDCOE, "Peacetime Regime for State Activities in Cyberspace", https://ccdcoe.org/multimedia/peacetime-regime-state-activities-cyberspace.html, 2013

CARI/ Instituto de Seguridad Internacional y Asuntos Estratégicos

ESTIMADO LECTOR

Si desea suscribirse a esta publicación, lo invitamos a solicitarlo a la dirección difusionrdnisiae@gmail.com

Cordialmente,

Equipo de Redacción del RDN ISIAE

DEAR READER

If you want to subscribe to this publication, we invite you to send your request to difusionrdnisiae@gmail.com

Yours faithfully,

RDN ISIAE Editorial staff

ESTIMADO LEITOR

Se você deseja se inscrever a esta publicação, o convidamos a nos enviar a solicitação a difusionrdnisiae@gmail.com

Cordialmente,

O equipe editorial do RDN ISIAE

CARI

Consejo Argentino para las Relaciones Internacionales