CARI /

Instituto de Seguridad Internacional y Asuntos Estratégicos

BOLETÍN DEL ISIAE

Julio 2016

Número 64

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

The impeachment of president Dilma Rousseff: old politics meets new standards in Brazil

Thomas C. Bruneau (*)

On May 28, 2016, the Brazilian Minister of Defense, Raul Jungmann, gave a long interview with the Estado de São Paulo newspaper. In the long interview he barely touched upon military or defense issues, merely lauding the military's neutrality in the current chaotic political situation. However, he did highlight an important aspect of Brazilian politics. He noted that while the Constitution of 1988 strengthened accountability institutions, naming specifically the Public Ministry, the Federal Police, and the Judiciary, politics had not changed. In his terms, politics is a hostage to itself.

These observations by a seasoned politician, one who has twice served as both federal minister and federal deputy, permit us to better understand the impeachment of President Dilma Rousseff. Despite allegations by President Rousseff that she was deposed in a golpe, a coup, the process is in accord with the Constitution of 1988. This is notwithstanding the fact that many other issues have contributed to the situation, including her narrow reelection in 2014, lackluster governance, dubious economic policies, exposes of massive graft and corruption, and miserable public opinion poll rating. While President Rousseff cannot be blamed for all of these problems, she is being held to answer for at least one of the 37 charges levied against her, which is a "crime of fiscal responsibility": fiddling with government accounts to facilitate her reelection in 2014.

Scholars who study the process whereby the Constitution of 1988 was formulated and the resulting document are extremely critical. In my writing I argue that the Constitution did not represent an "elite settlement" ensuring democratic consolidation, as was the case in Spain, for example. Law professor, Keith S. Rosenn, states the following: "The process by which Brazil's 1988 Constitution was adopted practically assured that the end product would be a hodgepodge of inconsistent and convoluted provisions."[1] Despite the 245 articles and 70 transitional provisions, the framers were unable to resolve whether Brazil would be a monarchy or republic, and if the latter, a presidential or parliamentary system. These fundamental decisions were left for a referendum in 1993 that favored a presidential republic. The framers of the constitution, which were the 559 members of the Brazilian Congress, maintained intact both the institutional defects of the political system and the extensive prerogatives of the armed forces that governed Brazil between 1964 and 1985. Whereas the institutional defects of the political system continue until the present, since the system is, as Jungmann puts it, hostage to itself, the prerogatives of

[1] Keith S. Rosenn, 2010, "Conflict Resolution and Constitutionalism: The Making of the Brazilian Constitution of 1988," in Laurel E. Miller, editor, with Louis Aucoin Framing the State in Times of Transition: Case Studies in Constitution Making (Washington, D.C. United States Institute of Peace, 2010), p. 458.

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

the armed forces have been diminished and the accountability institutions have become robust and active. These three processes, the diminishing of the prerogatives of the military, the vicious circle of the political system, and the emergence of strong accountability institutions are the focus of this paper.

Both Rosenn and I detail the extensive prerogatives of the armed forces that resulted from the negotiated transition from military to civilian rule and the reliance of President Sarney on the armed forces during his five year tenure (1985 – 90). The most extensive work on this topic, however, is found in Alfred Stepan's Rethinking Military Politics: Brazil and the Southern Cone where he demonstrates, by describing 11 prerogatives, that Brazil had little progressed between military and civilian rule. More recently, twenty – eight years after Stepan published his book, scholars demonstrate that the prerogatives that were mainly high when Stepan wrote are today either low or moderate. Some of the high points of the process whereby the prerogatives were diminished or eliminated include the creation of a civilian – led ministry of defense in 1999, which resulted in the decrease of military – led ministries from six to zero, and a large package of laws in 2011 which further delimited and restricted the autonomy of the armed forces. Today, the armed forces receive 1.29 % of GDP and 73% of this goes to salaries and pensions, and the political influence of the armed forces is minimal. Illustrative of the change from the military regime to the present day is the elimination of the National Information Service, (Serviço Nacional de Informações SNI), which was the intelligence arm of the military regime, by President Collor in 1990, and the creation, only after nine years, of the Brazilian Intelligence Agency (Agência Brasileira de Inteligência ABIN). ABIN is prohibited from conducting intercepts, has a minimal budget, and lacks a direct link to decision – makers. In short, the politicians had incentives to diminish the influence and roles of the armed forces, thereby increasing their own.

While the Constitution of 1988 included a great many items that could lead to an improved socio – economic situation for Brazilians, it changed nothing regarding the political institutions that put those 559 politicians into the position of writing the constitution, and have made only most minimal changes in the intervening 28 years. As Rosenn states "The constituent assembly also did nothing to reform the malfunctioning of the political party system, which is one of the world's worst."[2] They did not establish a minimum number of votes for a party to be recognized, resulting in the current situation with 35 political parties at the national level with 19 having deputies in the lower house, the Câmara. They did not change the open – list system of proportional representation in which each state is a single, and at – large multi – member district. They did not change the gross misrepresentation whereby all states, and the federal district, have three senators or the provision stipulating that all states, regardless of population, would have a minimum of eight and a maximum of seventy deputies.

There was supposed to be a wholesale revision of the Constitution in 1993 that would require only an absolute majority of the deputies. That revision never happened. Instead, there have been piecemeal revisions. In reviewing the various initiatives to revise the constitution between 1988 and today, they amount to very little. This is the consensus view of the experts on the issue including David Fleischer, Alfredo Montero, Timothy Power, and Keith Rosenn. The Constitution of 1988 was full of contradictions. The issue of parliamentary vs.

[2] Ibid, p. 458.

presidential form of government was never resolved, neither in the constituent assembly nor after. On the one hand the constitution gave the congress a role in approving annual budgets and allowed them to overrule presidential vetoes with absolute majorities rather than a two-thirds vote. On the other hand, it gave the presidency the exclusive right to initiate and execute annual budgets and to force 45 – day limits on the congress to review bills defined as "urgent" by the president, the power to appoint a cabinet, subject to Senate approval, and the power to issue executive decrees (medidas provisórias) which had the force of law while congress had 30 days to review the measure. Post – 1990 presidents utilized these measures, and others, to govern.

Even with these gimmicks, the need to assemble a coalition, since no president since the first directly elected, President Collor, has belonged to a party with a majority in either house of congress, all presidents would have to attract the support of other parties. Brazil has one of, if not the most fractured, party system of any democracy. This form of government, commonly called coalitional presidentialism (presidencialismo de coalizão), could, and did, easily evolve into corruption. The most famous, but not the only, corruption scandal of President Luis Inácio Lula da Silva –Lula (2002 – 2010) was the "big monthly" (as in big monthly payments to members of congress to support his government's policies in the congress), mensalão scandal. Alfred Montero has this to say on this topic. "The need to engage in vote – buying emerged from the limited options the Lula administration had for composing the same kind of legislative coalition that Cardoso enjoyed."[3] Several top Workers' Party (PT) officials were implicated in this vote – buying scheme. The scandal ultimately led to the convictions of twenty-five people, including Lula's former chief of staff, José Dirceu de Oliveira e Silva, who has more recently been sentenced to 23 years in jail in the Lava Jato corruption scheme.

There are so many corruption scandals currently in play in the investigation and sentencing phases, that only the experts can keep straight the modalities of Mensalão, Lava Jato, Petrolão, Zelotes, and Operation Aequalis to mention only the biggest and most current. So far the wave of illegal, extralegal, and simply corrupt practices have resulted in the impeachment hearing of President Rousseff, the investigation of ex-President Lula, the conviction of 84 persons for crimes associated with Lava Jato, the majority of them politicians and businessmen. While not all of the crimes involve politicians, most of them do, and virtually all of them involve sources of funds, as in Petrobras, under the control of the Brazilian State, and thus of necessity involve politicians.

It must be acknowledged that corruption is nothing new in Brazil. In fact, according to the late Samuel Huntington in his influential Political Order in Changing Societies corruption is seen in positive terms in the process of modernization. Huntington calls specific attention to Brazil. Further, there is a very influential article published in 1990 in the important Revista de Administração Pública of the Fundação Getúlio Vargas by Anna Maria Campos that argues in great detail why there is no concept or meaning to the term "accountability" in Portuguese. Most Brazilian and foreign authors refer to the Brazilian propensity to use "angles" or "gimmicks", jeitinhos, to get around laws. Or, as was said in positive terms of a mayor of São Paulo, he robs but he accomplishes things. Rouba mas faz.

And, in line with Jungmann's observations above, while politics has not

[3] Alfred P. Montero, Brazil: Reversal of Fortune (Cambridge, Mass: Polity Press, 2014), p. 43

changed, including the use of corruption to govern, what is now permissible in politics and business in general in Brazil is changing. There is no single cause for the change, and I have identified at least five.

First, the 1988 Constitution created, or recreated, a large spectrum of oversight and investigation mechanisms, and these have been expanded in number during the intervening 28 years. Today they include the Comptroller General, the Accounting Tribunal, the Federal Police, the Public Ministry, and the courts. There is a huge literature on these institutions in both Portuguese and English, and the approach that I find most convincing to explain their increasing influence, culminating in the current wave of imprisonments, is that of Sérgio Praça and Matthew M. Taylor who demonstrate that the capacity of these institutions increases not by a single event or factor, but through bureaucratic interaction. The capacity increase is contingent and interactive. In short, these oversight, investigatory, and punishment institutions can only be understood in a specific national and international context, which is why I include the following four factors.

Second, whereas in the past, the main weakness of the accountability mechanisms was the inability or unwillingness of the courts, and especially the Supreme Court, to process and convict individuals, today this is changing due to personalities and the gradual modification of processes similar to those noted in the prior paragraph. This change is best highlighted by the actions of Judge Sérgio Moro of Curitiba who has taken the lead in the Lava Jato scandal. He is extremely active not only in pursuing corruption, but also in writing on the importance of plea - bargaining and the Italian experience in countering the mafia.

Third, much of the momentum to impeach President Rousseff is related to allegation of corruption involving the Workers' Party, and was established by the information provided by Senator Delcídio do Amaral, who was the leader of the party in the Senate. He was arrested, and due to plea - bargaining (delação premiada) he provided information on the spread of corruption throughout the Brazilian government. Those familiar with criminal law in the United States are aware that plea - bargaining is probably the single most important mechanism for gathering evidence on white - collar crime. Plea- bargaining was established in Brazil only in 2013 with law 12,850/2013. I have been informed by lawyers involved in the introduction of plea – bargaining that it was one of several laws that were required for Brazil to reach OECD standards. Since June 2015 there was a Co-Operation Agreement in place between Brazil and the OECD, which has been followed by an OECD-Brazil Programme of Work.

Fourth, Brazil's population of over 200 million is increasingly invested in the system. An important indicator of this vesting is their paying taxes. According to one source, in 2013 over 50% of those who declared income, paid income tax, whereas a decade earlier only 36% paid income tax[4]. Just as important, according to data analyzed by the Instituto Brasileiro de Planejamento e Tributação, of the thirty countries where taxes are the highest, Brazil is the worst in terms of return to the population in investments in the quality of life.

Fifth, Brazilians are today very much aware of the low return on investment for their high taxes. Indeed, the huge anti – government demonstrations in June 2013

[4] *Pulsamérica* available at http://www.pulsamerica.co.uk/2013/02/25/brazil-over-12-million-currently=pay-income-tax/ accessed June 2, 2016.

were mainly caused by this awareness of high taxes, mediocre services in health, education, and transportation, while the government invested massively in stadiums and other infrastructure for the World Cup in soccer in 2014 and the Olympics in 2016. In addition to all – pervasive radio and television stations there is today extremely high penetration by social media. According to comScore, which claims to be the global leader in digital analysis, Brazil leads the world with a 99.9% reach of social media. And, with 8.8 hours of use in the month of June 2015, Brazil is the world leader in that similar data for Europe is 6.1 hours, and the U.S. 5.2 hours[5].

In sum, traditional politics, in which the lubricant is public funds, has now encountered a wide spectrum of accountability mechanisms, supported by processes and attitudes, which no longer tolerate the traditional lackadaisical approach to ethics in politics. While the incentives to reform politics are not as obvious as they were to assert control over the armed forces and intelligence services, they are nevertheless present in the expectations of the Brazilian population and international organizations.

References

Bruneau, Thomas (1992) "Brazil's political transition," in John Higley and Richard Gunther, eds., "Elites and Democratic Consolidation in Latin America and Southern Europe" (Cambridge: Cambridge University Press, 1992), pp. 257 – 281.

Bruneau, Thomas C. and Scott D. Tollefson (2014) "Civil – Military Relations in Brazil: A Reassessment," Journal of Politics in Latin America, pp. 107 – 138.

Bruneau, Thomas C. (2015) "Intelligence Reform in Brazil: A Long, Drawn – Out Process," International Journal of Intelligence and CounterIntelligence, pp. 502 – 519.

Campos, Anna Maria (1990) "Accountability: Quando Poderemos Traduzi-La Para O Português?" Revista de Administração Pública, pp. 30 – 50.

Couto, Cláudio G. and Rogério B. Arantes, (2008) "Constitution, Government and Democracy in Brazil," World Political Science Review, pp. 1 – 33.

Fleischer, David (2016) "Attempts at Political Reform: (1985 – 2015): Still a 'Never Ending Story'" Paper Presented at BRASA Conference, Brown University, March 31 – April 2, 2016.

Huntington, Samuel P. (1968) Political Order in Changing Societies (New Haven: Yale University Press, 1968)

Instituto Brasileiro de Planejamento e Tributação "Estudo sobre a Carga Tributária/PIB X IDH Maio 2015. Available at www.idpt.com.br Accessed May 30, 2016.

Montero Alfred P. (2014) Brazil: Reversal of Fortune (Cambridge, Mass.: Polity Press, 2014)

Power Timothy J. and Matthew M. Taylor, eds. (2011) Corruption and Democracy in Brazil: The Struggle for Accountability (Notre Dame, Indiana: University of Notre Dame Press, 2011).

Power, Timothy J. (2010) "Brazilian Democracy as a Late Bloomer: Reevaluating the Regime in the Cardoso – Lula Era," Latin American Research Review, pp. 218 – 247.

Praça Sérgio and Matthew M. Taylor, (2014) "Inching Toward Accountability: The Evolution of Brazil's Anticorruption Institutions, 1985 – 2010," Latin American Politics and Society, pp. 28 – 48.

Rosenn, Keith S. (2010) "Conflict Resolution and Constitutionalism: The Making of the Brazilian Constitution of 1988," in Laurel E. Miller, editor, with Louis Aucoin, Framing the State in Times of Transition: Case Studies in Constitution Making (Washington, D.C.: United States Institute of Peace, 2010).

[5] ComScore & Shareablee (2015) "The State of Social in Brazil" available at https://www.comscore.com Accessed June 2, 2016.

Rosenn, Keith S. (2014) "Recent Important Decisions by the Brazilian Supreme Court, Inter-American Law Review, pp. 297 – 334.

Stepan, Alfred (1988) Rethinking Military Politics: Brazil and the Southern Cone (Princeton: Princeton University Press, 1988).

Ciber Disuasión.
Un capítulo particularmente sensitivo de la Ciberdefensa

Prof. Dr. Ing. Roberto Uzal (*)

Resumen

Los conflictos bélicos entre estados naciones se han extendido, desde hace algo más de una década, a un nuevo dominio o ámbito: el Ciberespacio. Es decir, a los "tradicionales" Tierra, Mar, Aire y Espacio Exterior, se ha sumado un nuevo ámbito de confrontación, esta vez de naturaleza virtual: el ya mencionado Ciberespacio.

La participación o no de los estados naciones, en los muchas veces graves conflictos que se han venido llevando a cabo en el Ciberespacio, no constituye un acto voluntario ni es exclusivamente consecuencia de una decisión gubernamental. El desarrollo de capacidades de Ciberdefensa ha pasado a ser mandatorio para todos los estados naciones. Se trata de un asunto de alcance global e integral.

La peor situación que podría enfrentar un gobierno, en este contexto, puede modelarse imaginando una gran catástrofe en la Infraestructura Crítica del país (voladura de refinerías de petróleo, de instalaciones nucleares, de oleoductos, de redes de distribución eléctrica, etc.) y, por no haber desarrollado las capacidades mínimas necesarias de Ciberdefensa, no pueda dicho gobierno distinguir si se ha tratado de una infortunada catástrofe accidental o de una Ciber Agresión proveniente de otro estado nación.

Este artículo aborda un capítulo particularmente sensitivo de la Ciberdefensa: La Ciber Disuasión.

La esencia de un esquema de Ciber Disuasión es muy simple y clara: Lograr que los estados naciones agresores, reales y potenciales, perciban claramente que los costos esperados (económicos, políticos, militares, geopolíticos, de imagen) asociados a una Ciber Agresión a la Infraestructura Crítica Nacional de otro estado nación, superan ampliamente a los resultados esperados de dicha hipotética Ciber Agresión. En síntesis: Que no atacar sea percibido claramente como un "mejor negocio" que atacar.

El propósito del artículo es el de suministrar elementos de juicio, a la autoridades políticas y comandantes militares, para definir, si así se decide, un esquema de Ciber Disuasión acorde con la Estrategia de Ciber Defensa que se establezca a nivel estado nación.

1. Introducción

Incumben a la Ciberdefensa los conflictos en el Ciberespacio entre estados naciones [1]. Conviene distinguir a la Ciberdefensa del Ciberterrorismo, del Cibercrimen, del Ciberespionaje y del Activismo Hacker[2]. Los

[1] http://www.esgcffaa.mil.ar/numero7/40.html

[2] A la Ciberdefensa incumben los Ciber Conflictos entre estados naciones. Ciber Crimen implica la concreción de

Miembro del Grupo de Trabajo sobre Criminalidad Organizada Transnacional (COT) y del Instituto de Seguridad Internacional y Asuntos Estratégicos (ISIAE) del Consejo Argentino para las Relaciones Internacionales. Profesor universitario a nivel doctorado y maestría. Investigador Categoría I – Programa de Incentivo a la Investigación..

conflictos en el Ciberespacio entre estados naciones están asociados "al quinto dominio"[3],[4],[5] de dichos enfrentamientos. Está generalmente aceptado que los anteriores cuatro dominios son Tierra, Mar, Aire y Espacio Exterior.

Los aportes de Emilio Iasiello[6] constituyen una referencia insoslayable al abordarse aspectos relacionados con la Ciber Disuasión. Iasiello destaca en sus trabajos que fue el Gobierno de los Estados Unidos el que advirtió tempranamente acerca de la gravedad de las Ciber Agresiones entre estados naciones, particularmente cuando el blanco de dichos Ciber Ataques lo son los componentes de la Infraestructura Crítica del país "blanco" de la Ciber Agresión. De allí que haya sido el Departamento de Defensa de dicho país la primera institución en conferirle al Ciberespacio[7],[8] el carácter de un nuevo dominio o ámbito en el que se materializan los conflictos bélicos entre estados naciones.

A partir de este enfoque del Departamento de Defensa de los Estados Unidos, surgieron intenciones y/o propuestas de utilizar los conceptos y prácticas de la Disuasión utilizados en la Guerra Fría. Se admite en este artículo que, durante la Guerra Fría, "Disuasión" incluía, en muchos casos, a la "Disuasión Nuclear"[9]. La experiencia recogida en la última década muestra claramente que, a diferencia de la Disuasión Nuclear, la Ciber Disuasión implica considerar un muy amplio espectro de "jugadores" con distintos niveles de capacidades reales y potenciales, diversas motivaciones y diversos posicionamientos geopolíticos. Además, la Disuasión en la Guerra Fría, entendida como la amenaza de potenciales lanzamiento de misiles con cabezas nucleares materializando severas represalias, no puede lograrse en los conflictos en el Ciberespacio de manera igualmente tangible. Son ahora necesarios una reconocida capacidad de resolver el "Problema de la Atribución" (efectiva y rápida identificación del estado nación agresor), una creíble capacidad para generar respuestas rápidas, eficaces y proporcionales y una globalmente reconocida política de desarrollo cualitativo permanente en los temas relacionados con la Ciber Defensa.

Se destaca que uno de las escenarios potenciales más desfavorables que se le puede presentar a un estado nación es recibir Ciber Agresiones y, por incapacidad tecnológica y/o de gestión, terminar adjudicando los desastres ocasionados por dichos ataques a accidentes impredecibles.

Quizás, un aspecto que influye significativamente en las singularidades de la Ciber Disuasión, lo es que la Guerra Cibernética es eminentemente asimétrica. No

importancia los Cibercrímenes Transnacionales como, por ejemplo, el Ciber Lavado Transnacional de Activos. Ciberterrorismo se diferencia del Cibercrimen por sus motivaciones las que en este caso son políticas, sociales, raciales o religiosas. Ciberespionaje refiere a los "tradicionales" actos de espionaje pero, en este caso, en "el contexto de" "o mediante la" utilización de Redes de Computadores complejas. Activismo Hacker tiene asociada una suerte de postura "ideológica" que asume como de libre disponibilidad a los datos, información o conocimiento que resida en el Ciberespacio.

[3] https://peromatech.wordpress.com/2013/07/10/el-ciberespacio-el-quinto-dominio-de-la-guerra/

[4] https://www.facebook.com/emavitic2015/posts/1024460507593752

[5] http://52.0.140.184/typo43/fileadmin/Base_de_Conocimiento/XIII_JornadaSeguridad/CIBERESPACIOElQuintoDominiodelaGuerra.pdf

[6] Iasiello, Emilio. "Is Cyber Deterrence an Illusory Course of Action?." Journal of Strategic Security7, no. 1 (2014): 54-67. DOI: http://dx.doi.org/10.5038/1944-0472.7.1.5 Available at: http://scholarcommons.usf.edu/jss/vol7/iss1/6

[7] En el contexto de este artículo se entiende como "Ciberespacio" al contexto virtual generado por los servicios prestados por las capas más externas del Modelo de Referencia ISO-OSI de comunicación entre computadoras (capa de Red, capa de Transporte, capa de Sesión, capa de Presentación y capa de Aplicación).

[8] https://support.microsoft.com/es-ar/kb/103884

[9] http://www.atomicarchive.com/History/coldwar/page15.shtml

es un "lujo" que incumbe sólo a los países más poderosos. Paradójicamente, aquellos con Fuerzas Armadas que más han avanzado en la adopción de sistemas de Comando y Control integrados, son los que deben esforzarse en cubrir sus "flancos débiles" derivados del uso intensivo de redes teleinformáticas complejas.

Es por ello que, el entonces vice ministro de Defensa de los Estados Unidos, William J. Lynn III, estableció claramente: Tenemos en el US Cyber Command[10],[11],[12] (Comando Cibernético de los Estados Unidos) un completo espectro de capacidades, pero la esencia de la estrategia es defensiva. En el mismo artículo, Lynn asevera que Cyber Command / Cyber Space definen un nuevo ámbito de una nueva Fuerza Armada.

Se destaca en este trabajo que, países medianamente desarrollados, que adquieran adecuadas y reconocidas capacidades en Ciber Disuasión, podrán lograr un importante reposicionamiento en el contexto global. Esto no está desconectado del hecho de que, como lo destaca Lynn III, la Estrategia Cibernética prioritaria de los Estados Unidos sea la defensiva. Ocurre que el número de enemigos con capacidad de causar devastación en territorio norteamericano se multiplica en un contexto de Guerra Cibernética. Las contribuciones de William J. Lynn III deberían ser especialmente consideradas en el contexto de un esquema de Ciber Disuasión.

2. Aspectos generales de Ciber Disuasión

Para aproximarnos al concepto Estrategia de Ciber Disuasión conviene consensuar algunos conceptos e instrumentos. La esencia de una Estrategia de Ciber Disuasión es muy simple y En principio, los enfoques de una Estrategia de Ciber Disuasión admiten la siguiente catalogación cuyos componentes no son mutuamente excluyentes[13]:

- Ciber Disuasión basada en una globalmente difundida capacidad de represalia.
- Ciber Disuasión basada en las "Ciber Barreras de Entradas".
- Ciber Disuasión basada en el desarrollo de muy eficaces mecanismos alerta temprana, disponibilidad de capacidades de retardar un ataque en ejecución y una globalmente reconocida y homologada capacidad de identificación del estado nación Ciber Atacante.

Se amplían a continuación las menciones a las citadas tres variantes de la Ciber Disuasión:

a. Ciber Disuasión basada en una globalmente difundida capacidad de represalia.

   Esta variante es quizás la que guarda la mayor analogía con el pensamiento de William Kaufmann (Disuasión Nuclear durante la Guerra Fría)[14],[15]. Uno de los discípulos más destacados del Profesor Kaufmann, Richard A. Clarke[16],[17] década y media atrás, se entusiasmó con el enfoque resultante de adaptar el enfoque de

[10] https://www.foreignaffairs.com/articles/united-states/2010-09-01/defending-new-domain

[11] http://kms1.isn.ethz.ch/serviceengine/Files/ISN/122287/ipublicationdocument_singledocument/bc00084c-fe7f-43e5-a377-27621f88e00c/en/2010_08_Lynn_Report.pdf

[12] http://archive.defense.gov/news/newsarticle.aspx?id=60869

[13] Limitada ampliación de los conceptos expuestos inicialmente por Emilio Iasiello.

[14] http://www.washingtonpost.com/wp-dyn/content/article/2008/12/16/AR2008121602724.html

[15] http://www.rand.org/content/dam/rand/pubs/monographs/2008/RAND_MG636.pdf

[16] http://www.richardaclarke.net/bio.php

[17] http://www.goodreads.com/book/show/7286217-cyberwar

Kaufmann[18] al Ciberespacio pero luego, al verificar que Estados Unidos es, paradójicamente, uno de los países con mayor cantidad de Ciber Vulnerabilidades en el mundo, pasó a recomendar un enfoque eminentemente Ciber Defensivo como herramienta idónea para implementar conceptos y mecanismos de Ciber Disuasión en su país.

b. Ciber Disuasión basada en las "Ciber Barreras de Entradas"

Una referencia casi "obligada" a los enfoques de Ciber Disuación enfocada a las "Ciber Barreras de Entrada" la constituye el denominado "Gran Cortafuegos Chino" ("China Great Firewall" en Inglés). Se trata de una denominación que facilita la asociación a la "La Gran Muralla China" (o Great China Wall en Inglés). Se trata de una gigantesca obra de la Ingeniería Informática llevada a cabo por el Ministerio de Seguridad Pública de la República Popular de China a partir del año 2003.

El "Escudo Dorado" (como también se suele denominar al "Gran Cortafuegos o Firewall Chino") aparentemente nació como una herramienta de censura político / social; como un complejo artificio para vigilar y regular el acceso a Internet de los habitantes de China. Sin embargo, desde hace una década, se han detectado indicios numerosos y consistentes de que el "Escudo Dorado" ha incorporado prestaciones claramente orientadas a la Ciberdefensa.

Todo parece indicar que China es el país mejor preparado para implementar con éxito una Estrategia de Ciber Disuasión basada en las "barreras de entrada". Esto no descarta los numerosos y exitosos desarrollos de China en el ámbito de las Ciber Armas eminentemente ofensivas.

c. Ciber Disuasión basada en el desarrollo de muy eficaces mecanismos de alerta temprana, disponibilidad de capacidades de retardar un ataque en ejecución y una globalmente reconocida y homologada capacidad para identificar al estado nación Ciber Atacante.

Una referencia interesante: El 28 de mayo de 2013 Irán difundió que había detectado la Ciber Arma más sofisticada conocida hasta ese momento[19]. Maher, el equipo de Ciber Emergencias de ese país, publicó en su p. ágina web la arquitectura conceptual y funcionalidades de la citada Ciber Arma la que recibió el nombre de "Flame". La Unión Internacional de Telecomunicaciones (Naciones Unidas)[20] tuvo un destacado rol en el "caso Flame"; uno de sus más brillantes profesionales, el tecnólogo Marco Obiso[21], desempeñó un muy importante papel en este incidente. Rusia, también tempranamente alertada, también participó en el "caso Flame". Poco tiempo después, la prensa de Estados Unidos difundió detalles tecnológicos y políticos del Ciber Ataque materializado mediante la Ciber Arma "Flame"[22].

3. Ciber Disuasión como subconjunto de la Ciber Estrategia: Algunos aportes

Implementar y poner en vigencia operativa un eficaz esquema de Ciber Disuasión no constituye un asunto trivial. La formulación de una Ciber Estrategia con un fuerte

[18] Costo no deseado de la utilización intensiva de Ciber Herramientas en la Defensa y en la Infraestructura Crítica en general.

[19] https://www.youtube.com/watch?v=vrRj-kRofRg
[20] http://www.itu.int/es/Pages/default.aspx
[21] http://www.itu.int/es/Pages/default.aspx
[22] http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against- iran.html?_r=0

componentes de Ciber Disuasión requiere, en principio, la conformación de un equipo de muy alto nivel profesional y de carácter eminentemente multidisciplinario. Ciber Disuasión requiere el concurso armónico de profesionales destacados de disciplinas diversas: Politólogos, militares especialistas en funciones de Estado Mayor, diplomáticos, ingenieros militares con sólida formación de post grado en Ciber Defensa, especialistas en geopolítica, especialistas en comunicación social.

El desarrollo e implementación de capacidades de Ciber Disuasión mal comunicados o que sean mal interpretados por otros estados naciones, pueden conducir a conflictos con tendencia a escalar o, directamente, a niveles de confrontación no deseados ni convenientes para ninguno de los actores. Ciber Disuasión implica un manejo sutil de "gestos o señales" cuya gestión constituye un enorme desafío.

Por otro lado, el "Problema de la Atribución" (efectiva identificación del Ciber Agresor)[23], que es extremadamente importante y complejo en Ciberdefensa en general, cobra especial relevancia en el ámbito de la Ciber Disuasión. El principio de proporcionalidad, de gran importancia en un contexto "Jus in bello - Jus ad bellum"[24], debe ser aplicado en forma inteligente, creativa y eficaz en los esquemas de Ciber Disuasión. Estos aspectos anunciados serán descriptos, a nivel introductorio, en este punto del artículo.

a. Ciber Disuasión y Acciones Comunicacionales

Un capítulo importante de los esquemas de Ciber Disuasión debe estar constituido por acciones de comunicación eficaces. Los mensajes asociados a dichas acciones deberán estar dirigidos, tanto a la comunidad internacional en general, como a aquellos estados naciones con los que se estime exista una alta probabilidad de Ciber Conflictos. Las acciones comunicacionales desempeñan un rol fundamental en cualquiera de las tres variantes de los enfoques de Ciber Disuasión que se han descripto en este artículo. La realimentación correspondiente a los mensajes emitidos debe ser muy inteligentemente aprovechada. La adecuada recepción y el procesamiento de los mensajes enviados por oponentes reales o potenciales, requiere también especial atención.

Se debe tener presente que, determinadas Ciber Armas, pueden superar el poder destructivo al armamento nuclear[25],[26]. Al respecto, cuando la Ciber Disuasión esté sustentada en la capacidad de represalia, la claridad y corrección de las Ciber Reglas de Empeñamiento[27] juegan un papel muy importante. Es más, una creativa, oportuna y correcta difusión de las propias Ciber Reglas de Empeñamiento podrá llegar a constituir una parte importante del núcleo del esquema de Ciber Disuasión.

En general, cuando se tratan temas relacionados con el Ciberespacio, las acciones comunicacionales requieren especiales capacidades para ser elaboradas y ejecutadas. El Ciberespacio se trata de un "dominio" lleno de ambigüedades. Un inteligente y razonable enunciado de Ciber Reglas de Empeñamiento, efectuado por países con antecedentes que los hagan

[23] http://43jaiio.sadio.org.ar/proceedings/SIE/16-SIE704.pdf Este es un ejemplo de varias presentaciones, sometidas a arbitraje internacional, en las que se muestra la viabilidad de resolución del "Problema de la Atribución" en Ciberdefensa.

[24] http://www.cari.org.ar/pdf/boletin62.pdf Ver artículo al respecto en el Boletín Nro 62 del ISIAE del Consejo Argentino para las Relaciones Internacionales.

[25] http://warontherocks.com/2016/02/the-cyber-threat-to-nuclear-deterrence/

[26] https://www.youtube.com/watch?v=vrRj-kRofRg

[27] http://www.cari.org.ar/pdf/boletin62.pdf

creíbles, podría también llegar a constituir "la línea de base" de un esquema normativo que lleve a regular las conductas de los estados naciones en los Ciber Conflictos; en otros términos, una suerte de Ciber Jus in bello – Ciber Jus ad bellum[28].

De acuerdo a relevamientos efectuados entre estudiosos de estos temas, la difusión de Ciber Reglas de Empeñamiento realizadas en forma conjunta por dos o más estados naciones o por estados naciones comprometidos al respecto con organismos internacionales, adquiriría niveles de credibilidad que influirían eficazmente en los esquemas de Ciber Disuasión.

Como conclusión parcial: Los esquemas de Ciber Disuasión que no estén complementados por creíbles, claras, oportunas y eficaces acciones comunicacionales, verían afectada negativamente su efectividad.

b. Gestos o señales complementarios en esquemas de Ciber Disuasión

Gestos o señales entre estados naciones se han venido aplicando, desde hace muchos años, en varias áreas de la política internacional. Estos gestos o señales han incluido acciones pre conflicto bélico, han influido en lo estilos de negociación durante el desarrollo de una crisis, han sido incluidos en la toma de posición en negociaciones económicas internacionales y se consideraron en el enunciado de principios en negociaciones de integración regional; esta enumeración no es excluyente, como se adelantó, gestos y señales han venido utilizándose en numerosos escenarios correspondientes a las relaciones entre estados naciones.

Los gestos o señales en realidad constituyen un subconjunto especializado de las acciones comunicaciones entre estados naciones. Veamos algunos ejemplos no abstractos de gestos o señales en Ciber Disuasión:

- Recorrer (cibernéticamente) la grilla eléctrica de otro estado nación sin causar daños pero mostrando que se posee la capacidad de provocarlos.

- Tomar el control de un satélite de otro estado nación sólo por un par de minutos y sin producir daño alguno. La finalidad es demostrar las capacidades en dicho ámbito[29].

- Acceder a información altamente sensitiva de un tercer estado nación no muy poderoso pero con evidentes y sensitivos esquemas asociativos con otro estado nación muy poderoso. Este último suele ser el verdadero destinatario del gesto o señal. A continuación difundir globalmente la citada información sensitiva causando notorios escándalos. Esto se realiza evitando una confrontación directa con el estado nación muy poderoso, el cual, como se anticipó, es en realidad el destinatario del gesto o señal[30].

- Difundir la organización de un equipo propio de muy alto nivel y evidente efectividad en el ámbito de la Ciber Atribución (detección del verdadero Ciber Agresor con una muy alta probabilidad de

[28] https://www.icrc.org/es/guerra-y-derecho/otros-regimenes-juridicos/jus-bello-jus-ad-bellum

[29] http://www.bloomberg.com/news/articles/2011-10-27/chinese-military-suspected-in-hacker-attacks-on-u-s-satellites

[30] http://www.cbc.ca/news/business/panama-papers-germany-1.3524705 ¿En realidad un conflicto económico-financiero entre dos países muy poderosos?

éxito y una muy baja probabilidad de falla)[31].

Importante: Los gestos o señales utilizados en Ciber Disuasión requieren una muy alta credibilidad alcanzada por el estado nación emisor de dichos gestos o señales. Si esta precondición no se verifica, los gestos o señales no tendrán efecto alguno. Puede también ocurrir, si la citada credibilidad no existe, una suerte de efecto "boomerang"; el emisor de gestos o señales puede desmejorar su posicionamiento como consecuencia de su falta de credibilidad. Gestos o señales que sean interpretados como simples bravuconadas constituyen el peor de los resultados.

Una potencial desventaja relativa de los gestos o señales es que pueden, con facilidad, ser mal interpretados. Un equipo interdisciplinario muy solvente y con un liderazgo de excelencia debe estar a cargo de los gestos o señales utilizados en Ciber Disuasión. La emisión de estas acciones puede realizarse en forma abierta, como una suerte de "broadcasting", en otros casos se podría utilizar canales específicos, diplomáticos o militares. A veces un aparente Ciber Ataque militar (con objetivos de destrucción acotados) podrá tener como finalidad real la de ser el medio de transmisión de un gesto o señal.

c. El "Problema de la Atribución" en Ciber Disuasión

El denominado "Problema de la Atribución" constituye un aspecto central en Ciberdefensa en general y en Ciber Disuasión en particular. Identificar al Ciber Agresor con una muy alta probabilidad de éxito y una muy baja probabilidad de falla. En este contexto "falla" implica atribuir el Ciber Ataque a un estado nación ajeno al conflicto.

La atribución de Ciber Agresiones a un responsable específico constituye un asunto no trivial. La complejidad de la solución del "Problema de la Atribución" ha sido utilizada, por determinados gobiernos, como sustento de importantes campañas comunicacionales destinadas a difundir el mito de la imposibilidad de solucionar el mencionado problema.

Un Ciber Ataque debe poder ser atribuido, con una muy alta probabilidad asociada, antes de que la legítima defensa pueda ser interpretada como tal y quedar incluida en los términos del Artículo 51 de la Carta de las Naciones Unidas.

Un robusto y homologado enfoque forense debe respaldar la atribución de un Ciber Ataque. La atribución, sólidamente sustentada, de un ataque a un estado o a un agente estatal, es una precondición, sine qua non, internacionalmente requerida, para poder alegar la mencionada legítima defensa. Si un ataque es erróneamente atribuido, existe un gran riesgo de dañar víctimas inocentes al definir erróneamente la respuesta.

La atribución en el Ciberespacio es compleja; las identidades y direcciones pueden ser fácilmente disfrazadas o disimuladas. Lo señalado implica "dificultad"; de ninguna manera "imposibilidad".

Criminales, terroristas o activistas hackers podrían atacar a un estado nación, utilizando Ciber Armas, para dañar su Infraestructura Crítica. Es opinable incluir estos temas en Ciberdefensa. En principio no procedería, desde el estado nación

[31] http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf

atacado, una respuesta militar a gran escala. Conclusión parcial: Es muy importante determinar, en la Ciber Atribución, cuándo un atacante es o no un actor estatal.

Conviene citar que, algunas de las medidas "clásicas" para prevenir Ciber Ataques, lo son los sistemas de detección de intrusiones, los firewalls, el encriptado, los "honey pots" (sistemas señuelo) y la detección a partir del análisis de flujos de redes. Ninguno de estos enfoques posee, en sí mismo, elementos que permitan, certera y efectivamente, a dilucidar la identidad del perpetrador y/o el origen de la acción maliciosa. Esto crea un círculo vicioso en el cual la anonimidad impide la atribución del Ciber Ataque, mientras que la carencia de capacidad de atribución lo que trae como consecuencia que los agresores evaden la justicia o la acción de respuesta. Esto, a su vez provoca la caída del nivel de la esencial "Ciber Disuasión". Sin el temor a ser identificados y penalizado, individuos y organizaciones continuarán, posiblemente en forma incremental, sus actividades maliciosas en el Ciberespacio.

No existe un enfoque excluyente e infalible para resolver el "Problema de la Atribución". La solución existe pero generalmente proviene de la actuación de equipos multidisciplinarios evaluando la concurrencia de indicadores provenientes de la aplicación de métodos y herramientas diversas.

Otro aspecto importante: En el contexto de la Ciber Defensa, "backtraking" es el proceso de "trazar hacia atrás" las acciones del atacante de manera de poder identificarlo. Existen diversos y muy efectivos métodos de "backtraking". El transcurso del tiempo es una consideración esencial en este contexto; cuanto antes se dispare el mecanismo de "backtraking" mayor será la probabilidad de identificar exitosamente al atacante.

Cuando un Ciber Ataque en progreso es detectado el análisis de los datos disponibles respecto de la agresión deberían ser analizados casi "en línea" o, mejor aún, en "tiempo real". Ciber Soldados debidamente capacitados y permanentemente entrenados deberían llevar a cabo una evaluación de la información disponible en las primeras etapas del Ciber Ataque para determinar la naturaleza y objetivos de la Ciber Agresión de manera de tomar a tiempo decisiones acertadas para impedir, interrumpir, mitigar, atribuir y eventualmente restaurar las consecuencias del Ciber Ataque.

En forma adicional, Ciber Soldados especializados en operaciones defensivas podrían implantar honeypots (sistemas señuelos) para atraer a los atacantes a este tipo de trampas. Esto podría "dar vueltas las cosas" y transformar a los Ciber Atacantes en objeto de investigación.

Si el uso de honeypot es exitoso, los Ciber Soldados podrían hacerse de información sumamente valiosa acerca de las capacidades, identidad e intenciones del intruso.

Se remarca: Los honeypots son sistemas de hardware / software destinados a atraer la atención del atacante manifestando una verosimilitud tal que haga que el agresor lo confunda con el blanco real. Honeypots inteligentemente utilizados pueden ser incorporados para incrementar la efectividad de esquemas de Ciber Disuasión.

Se ha probado mediante experiencia en laboratorio y casos reales "de campo" que el

"Problema de la Atribución"[32] puede solucionarse aún en el caso de que el atacante utilice sofisticadas herramientas de "anonimidad". El "backtraking" es viable aún cuando los routers incluidos en la ruta de ataque estén enmascarados mediante un enfoque del tipo "Onion Routing"[33],[34].

Onion Routing es una técnica de comunicación y encriptado que preserva la anonimidad en el contexto de redes de computadoras. En este caso los mensajes son constantemente encriptados y luego enviados a través de varios nodos de la Red denominados Onion Routers los cuales conforman un encadenamiento de nodos enmascarados que cambian "sus identidades" luego de que un mensaje específico ha pasado por ellos.

Cada Onion Router (router cebolla) remueve su capa de enmascaramiento más externa inmediatamente después de haber enviado el mensaje específico al próximo "router cebolla". De allí la analogía "Onion Router". Esto previene que los nodos intermedios de la red conozcan el origen, el destino y el contenido del mensaje. Los "Onion Routers" no impiden un enfoque defensivo eficaz en Ciberdefensa; eso sí, constituyen un desafío relevante para Ciber Soldados con una formación de excelencia.

d. Ciber Disuasión y proporcionalidad

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

- En primer lugar deben contar con una ajustada evaluación del nivel de confiabilidad que sus agencias de inteligencia y sus unidades de Ciberdefensa tienen para resolver el "Problema de la Atribución". Por otro lado dicho estado nación debe tener capacidades forenses reconocidas / homologadas internacionalmente. La elaboración de las pruebas creíbles de haber sido víctima de una Ciber Agresión y la oportuna presentación de dichas pruebas ante organismos internacionales constituyen el núcleo de las mencionadas capacidades forenses. La probabilidad asociada a una correcta resolución del "Problema de la Atribución" tendrá un impacto directo en la elaboración de la respuesta. Por ejemplo, si dicha probabilidad es baja, las autoridades del estado nación atacado estarán limitadas en la selección de la respuesta, aunque la severidad del ataque haya sido alta. Esto forzará a seleccionar objetivos de represalia menos importante para acotar la posibilidad de que escale un conflicto internacional sin fundamentos evidentes y/o recibir críticas desfavorables de la comunidad internacional. En casos extremos podrían verificarse 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 los Ciber Incidentes en la Infraestructura Crítica nacional, en la sociedad en general, en la economía y en los intereses nacionales considerados como un todo integrado. En este contexto las preguntas que requieren respuestas confiables 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

[32] Casos y herramientas expuestas el 29 de agosto de 2014 en el contexto del evento "Ciberdefensa y seguridad de redes de comunicaciones" llevado a cabo en las instalaciones de la Escuela Superior Técnica del Ejército Argentino "General Manuel N. Savio" y durante el Desarrollo de un seminario sobre Ciber Atribución / Ciber Anonimidad / Ciber Disuasión en el Ministerio de Defensa de Argentina, 13 de agosto de 2015.
[33] https://www.torproject.org/
[34] http://www.freehaven.net/~arma/cv.html

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 convencionales a su disposición; desde un reclamo diplomático hasta un ataque militar convencional. 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 y consecuencias.

  Las Ciber Respuestas pueden ser llevadas a cabo en forma complementaria de las respuestas diplomáticas, económicas y militares convencionales; muchas veces se decide que la Ciber Respuesta lo sea 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. Las citadas capacidades deberían haber 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.

  Considerando los acuerdos de Ginebra de 1949 sobre el derecho de los conflictos armados y los principios de proporcionalidad, así como los expresados en la elaboración reciente de la OTAN, plasmada en el Manual Tallin[35], se tiende a asimilar aspectos de la Ciberguerra a los de la guerra convencional. Este enfoque sustenta adicionalmente la aseveración de que una acción de Ciber Represalia debe ajustarse al principio de proporcionalidad. El daño de la Ciber Respuesta debería ser proporcional al daño ocasionado al Ciber Ataque inicial. El foco debería estar puesto en evitar una escalada del conflicto.

  El principio de proporcionalidad debe ser tenido en cuenta en la elaboración y en la operación de esquemas de Ciber Disuasión. Proporcionalidad implica "condiciones de contorno" que deben ser consideradas en la Ciberdefensa en general y en Ciber Disuasión en particular.

4. Conclusiones

a. La participación o no de los estados naciones en las agresiones que se han venido llevando a cabo en el Ciberespacio y que continúan con una tendencia creciente, no constituye un acto voluntario ni es exclusivamente consecuencia de una decisión gubernamental. El desarrollo de capacidades de Ciberdefensa ha pasado a ser mandatorio para todos los estados naciones.

b. La peor situación que podría enfrentar un gobierno, en este contexto, puede modelarse imaginando una gran catástrofe en la Infraestructura Crítica del país (voladura de refinerías de petróleo, de instalaciones nucleares, de oleoductos, de

[35] https://ccdcoe.org/research.html

redes de distribución eléctrica, etc.) y, por no haber desarrollado las capacidades mínimas necesarias de Ciberdefensa, no pueda dicho gobierno distinguir si se ha tratado de una infortunada catástrofe accidental o de una Ciber Agresión proveniente de otro estado nación.

c. Ciber Disuasión adquiere especial relevancia cuando un gobierno de un estado nación adopta una Estrategia de Ciberdefensa con enfoque defensivo.

d. La "asimetría" de la Ciberdefensa se extiende claramente a su subconjunto "Ciber Disuasión". Implementar un efectivo esquema de Ciber Disuasión no es un "lujo" exclusivo de las grandes potencias. Con un pequeño equipo de profesionales de alto nivel y con equipamiento accesible, se pueden alcanzar resultados realmente notables.

e. Para un estado nación, alcanzar un adecuado nivel de Ciber Disuasión, constituye una excelente oportunidad de posicionamiento positivo en el contexto global en un plazo no muy extenso y con inversiones razonables.

f. Ciber Disuasión, como parte destacada de la Ciberdefensa, debería ser objeto de estudio e investigación en las Escuelas Superiores de Guerra de las Fuerzas Armadas y aun con mayor énfasis en la Escuela Superior de Guerra Conjunta.

g. Ciber Disuasión debería ser motivo de permanente tratamiento entre las autoridades políticas de los Ministerios de Defensa y de Relaciones Exteriores asistidas por equipos técnicos de muy alto nivel.

5. Referencias

Chapple, Mike, Seidl, David, "Cyberwarfare: Information Operations in a Connected World, (Information Systems Security & Assurance)", Editor:
Jones & Bartlett Learning, agosto de 2014, Inglés, ISBN-10: 1284058484

Clarke, Richard, "Cyberwar: The Next Threat to National Security & What to Do About It", Publicado por Ecco; Reprint edition (August 5, 2011),
Inglés, ISBN-10: 9780061962240

Mazanec, Brian "The Evolution of Cyber War: International Norms for Emerging-Technology Weapons Hardcover", Potomac Books, inglés, noviembre de 2015, Publisher: Potomac Books, ISBN-10: 1612347630

NATO Cooperative Cyber Defence Centre of Excellence: "Tallinn Manual on the International Law Applicable to Cyber Warfare" https://ccdcoe.org/research.html

NATO Cooperative Cyber Defence Centre of Excellence: Peacetime Regime https://ccdcoe.org/publications/books/Peacetime-Regime.pdf

Ohlin, Jens David, "Cyber War: Law and Ethics for Virtual Conflicts",
Editores Kevin Govern y Claire Finkelstein, 1ra Edición

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