O FORTALECIMENTO DA CONTRAINTELIGÊNCIA NO ÂMBITO DO SISTEMA DE PROTEÇÃO AO PROGRAMA NUCLEAR BRASILEIRO (SIPRON)*

RENATO FERREIRA **JÁCOMO** DOS SANTOS**
Capitão de Fragata
VIVIANE DA SILVA SIMÕES***
Analista de Relações Internacionais

SUMÁRIO

INTRODUÇÃO

O Sistema de Proteção ao Programa Nuclear Brasileiro (Sipron) foi instituído originalmente em 1980, por meio do Decreto-Lei 1.809, para atender às necessidades de segurança do Programa Nuclear Brasileiro (PNB).

Em 2012, a Lei 12.731 reformulou as atribuições do Sipron com vistas a conferir-lhe a competência específica de coordenar as ações para proteger os conhecimentos e a tecnologia relativos àquele Programa.

Nesta nova competência identificamos a aplicação da Contrainteligência, definida como a "atividade que objetiva prevenir, detectar, obstruir e neutralizar a inteligência adversa e ações de qualquer natureza que constituam ameaça à salvaguarda de dados, informações e conhecimentos de interesse da segurança da sociedade e do Estado, bem como das áreas e dos meios que os retenham ou em que transitem" (BRASIL, 2002).

No desenvolvimento deste trabalho, pesquisando em fontes abertas, apreciaremos

* Adaptação do Trabalho de Aplicação de Curso apresentado pelos autores à Escola Superior de Guerra.
** Analista de Contrainteligência do Centro de Inteligência da Marinha (CIM).
*** Analista de Relações Internacionais da Comissão Nacional de Energia Nuclear (Cnen).

a prática da Espionagem como um recurso empregado, ou passível de o ser, pelos Estados na defesa de seus interesses, e como os alvos desta ação podem buscar se defender, mediante a Contraespionagem. Constataremos a relevância do PNB como um alvo do interesse estrangeiro – portanto demandante de medidas de proteção por parte do governo brasileiro – e as deficiências de mentalidade de Contrainteligência no Brasil para a proteção deste conhecimento.

Ao final, procuraremos apresentar propostas para o fortalecimento da Contrainteligência no âmbito do Sipron, na forma de subsídios para a sua regulamentação, e também conhecimentos que poderiam ser de utilidade para os seus órgãos integrantes.

Dois milênios e meio após Suntzu, a Espionagem continua viva como um instrumento à disposição dos Estados em todos os campos das relações internacionais

ESPIONAGEM E CONTRAESPIONAGEM

"Não há quaisquer áreas em que não se empreguem espiões" (SUN TZU e SUN PIN, 2002).

Na transcrição dos ditos do estrategista militar Sun Tzu, verifica-se um dos primeiros registros históricos a respeito da utilidade da Espionagem. Definimo-la[1], nos termos da proposta de Política Nacional de Inteligência (PNI) para o Estado brasileiro[2], como: "a ação que visa à obtenção de conhecimentos ou dados sensíveis para beneficiar Estados, grupos de países, organizações, facções, grupos de interesse, empresas ou indivíduos" (BRASIL, 2009b).

Por sua vez, Conhecimento Sensível é: "todo conhecimento, sigiloso ou estratégico, cujo acesso não autorizado pode comprometer a consecução dos objetivos nacionais e resultar em prejuízos ao País, necessitando de medidas especiais de proteção" (BRASIL, 2009a).

Quase dois milênios e meio após a citação que abre esta seção, percebemos que a Espionagem continua viva como um instrumento à disposição dos Estados nos conflitos ou disputas de interesses que se verificam em todos os campos das relações internacionais.

Na China de 1999, os igualmente estrategistas militares Qiao Liang e Wang Xiangsui apontaram que, a partir da Guerra do Golfo de 1990-1991, evidenciou-se no mundo um aumento na violência política, econômica e tecnológica, em contraste com uma relativa redução na violência militar. Isto levaria a uma reformulação dos princípios da guerra no sentido de que não prescreveriam mais "o emprego da força armada para compelir um inimigo a submeter-se a nossa vontade" (CLAUSEWITZ, 1984, p. 75), e sim "a utilização de todos os meios, militares e não militares, letais e não letais, para compelir um inimigo a submeter-se aos nossos interesses" (LIANG e XIANGSUI, 1999, p. 6). Assim, um Estado poderia desencadear "Operações de Guerra Não Militares", que incluiriam as seguintes modalidades: comercial, financeira, terrorista em redes, ecológica, psicológica, de contrabando, de mídia, de drogas, em redes interativas, tecnológica, de maquinação[3], de recursos,

1 Preferimos esta definição à constante do Glossário das Forças Armadas (BRASIL, 2007, p. 95).
2 Em 29 de junho de 2013, a proposta da PNI encontrava-se em tramitação no Poder Executivo/Congresso Nacional.
3 Criando uma falsa aparência de poder real aos olhos do inimigo.

de ajuda econômica, cultural, de legislação internacional, entre outras possibilidades (LIANG e XIANGSUI, 1999, p. 58-66). Nesse contexto, um Estado poderá adotar a definição de "guerra" que seja mais conveniente à sua Estratégia Nacional; e na mesma medida estaria propenso a utilizar-se de "quaisquer meios", entre os quais a Espionagem.

Hodiernamente também podemos constatar a formulação de legislações estatais que, em geral de forma velada, validam o emprego da Espionagem. Citamos aqui o exemplo dos Estados Unidos da América (EUA), ator internacional de prevalência global[4], cujo *National Security Act* de 1947 (EUA, 2010, p. 6) define "inteligência estrangeira" como o seguinte produto: "informações relativas às capacidades, intenções ou atividades de governos estrangeiros ou elementos equiparados, organizações ou pessoas estrangeiras, ou atividades terroristas internacionais". Também é relevante considerar o *Foreign Intelligence Surveillance Act* (Fisa) de 1978, que, em 2008 recebeu emenda incluindo, sob o Título VII, procedimentos de Inteligência adicionais concernentes à interceptação de dados de pessoas específicas fora dos EUA (EUA, 2008, p. 2438).

As ações de busca e violação de dados sigilosos em poder dos Estados vêm se desenvolvendo em paralelo com a exponencial evolução tecnológica e alargamento das áreas do conhecimento humano. A chamada Ciberespionagem, uma modalidade de Guerra Cibernética[5], segue na crista desta onda, viabilizando que tanto atores estatais como não estatais[6] furtem, adulterem ou destruam informações remotamente, com baixo custo e baixo risco de detecção ou captura, em escala industrial (REINO UNIDO, 2013).

As ações de busca e violação de dados sigilosos em poder dos Estados vêm se desenvolvendo em paralelo com a exponencial evolução tecnológica e alargamento das áreas do conhecimento humano

Explicitando essa tendência de acesso a dados negados em escala industrial, em 7 de junho de 2013 o jornal britânico *The Guardian* divulgou a existência de um programa oficial da Agência de Segurança Nacional dos EUA (NSA) denominado Prism/US-984XN (ou simplesmente "Prism")[7], que visaria à obtenção de dados (e-mail, conversas em vídeo e voz-sobre-IP, transferências e arquivos de imagem, áudio e vídeo, detalhes de redes sociais etc.) por meio de acesso direto aos servidores de internet das empresas Microsoft, Yahoo!, Google, Facebook, PalTalk, YouTube, Skype, AOL e Apple (GREENWALD e MACASKILL, 2013). Apesar de ter sua existência negada pelos executivos das empresas, no mesmo dia

4 A legislação estadunidense também é citada, de maneira específica, em razão da facilidade de acesso à informação oficial.

5 Guerra Cibernética – Conjunto de ações para uso ofensivo e defensivo de informações e sistemas de informações.

6 Em outubro de 2012, foi detectada uma rede de ciberespionagem, chamada Outubro Vermelho, que comprometia várias agências de serviços diplomáticos internacionais.

7 O responsável pelo vazamento do programa Prism para a imprensa foi Edward Snowden, um ex-funcionário de empresa terceirizada pela NSA. Por ocasião do fechamento deste artigo, em 30 de agosto, Snowden encontrava-se em asilo temporário na Rússia.

o programa foi admitido pelo Presidente dos EUA, Barack Obama, que enfatizou a aquiescência do Congresso e do Judiciário estadunidenses. E o diretor de Inteligência Nacional, James Clapper, além de confirmar, frisou que o programa seria direcionado exclusivamente à "inteligência estrangeira", e não aos cidadãos de seu Estado, estando em conformidade com a Seção 702, parte do Título VII do Fisa (ROBERTS e ACKERMAN, 2013).

Destaque-se que o caso supramencionado evidencia outro aspecto importante do problema que estudamos: a possibilidade de vazamento de Conhecimentos Sensíveis por funcionários dos órgãos que os detêm. É uma situação que se constata em nível mundial, inclusive no Brasil, onde pesquisa feita pela empresa Symantec entre outubro e novembro de 2012 apontou, entre outras constatações, que 62% dos colaboradores que mudaram de emprego mantêm dados corporativos confidenciais, e 56% planejam usá-los na nova companhia para a qual trabalharão (SYMANTEC, 2013). Voltaremos a este ponto quando tratarmos mais adiante dos desafios à implantação de uma mentalidade de Contrainteligência no Brasil.

Em que pese a conotação negativa que se pode perceber atribuída à Espionagem, como uma atividade antiética especialmente no campo empresarial, constatamos que no realismo das relações internacionais esta lógica não se aplica. Apesar do discurso politicamente correto[8], empresas podem se beneficiar da Espionagem estatal no limite da Inteligência Competitiva – aquela voltada para o mundo dos negócios, ou seja, que busca a manutenção ou o desenvolvimento de vantagem competitiva em relação aos concorrentes (ABRAIC, 2013). Além dos EUA[9], França, Rússia, China e Japão seriam Estados que empregariam Inteligência estatal em apoio a empresas nacionais (FILHO, 2000).

Em face do exposto, caberia a pergunta: seria o Brasil um alvo da espionagem estrangeira?

Em que pese a conotação negativa atribuída à Espionagem, e apesar do discurso politicamente correto, empresas podem se beneficiar da Espionagem estatal

Bem, se já não for centenária, essa atividade se verifica no Brasil (como alvo) há mais de 90 anos. Jeffrey M. Dorwart (1979, p. 137) apresenta que, em 1918, o Capitão de Mar e Guerra (da Marinha dos EUA) Frank K. Hill, oficial de Inteligência agindo sob cobertura diplomática de Adido Naval, operava a partir do Rio de Janeiro uma rede de informantes e agentes[10] engajada no levantamento de conhecimentos acerca das condições de trabalho nas minas de manganês de Minas Gerais, e de subsídios para que a companhia estadunidense Bethlehem Steel superasse a britânica Vickers and Armstrong na disputa pelo lucrativo contrato de modernização dos encoura-

8 "Sobre a espionagem, queremos acrescentar que, apesar do caráter totalmente antiético da atividade, as empresas que cogitam praticá-la correm riscos demasiadamente grandes que podem conduzir à morte da organização." (CÂMARA DE COMÉRCIO FRANÇA-BRASIL, 2007, p. 8)

9 O que impediria o Prism de ser um instrumento, entre outros?

10 Integrariam esta rede um censor postal, três agentes de campo, um assistente no porto do Recife, dois funcionários de escritório, um oficial de ligação com a Marinha do Brasil e representantes comerciais de empresas.

çados *São Paulo* e *Minas Gerais*, entre 1920 e 1922 (VIDIGAL, 1983, p. 92), entre outros conhecimentos. Eis aqui um exemplo cabal, conquanto já histórico, de envolvimento estatal em Inteligência Competitiva, e no Brasil.

Com efeito, a proposta da PNI aponta a Espionagem como a ameaça prioritária para efeito de balizamento das atividades dos diversos órgãos que integram o Sisbin (BRASIL, 2009b, p. 10).

Retornamos então à importância das medidas de Contrainteligência, que se dividem em dois segmentos: Segurança Orgânica e Segurança Ativa – esta de caráter proativo, aquela de caráter preventivo. No Glossário das Forças Armadas (BRASIL, 2007, p. 235-236), estão definidas da seguinte forma:

– A **Segurança Orgânica** visa obter um grau de proteção ideal, por meio da adoção eficaz e consciente de um conjunto de medidas destinadas a prevenir e obstruir as ações de qualquer natureza que ameacem a salvaguarda de dados, conhecimentos e seus suportes; e

– A **Segurança Ativa**, preconizando a adoção de medidas de caráter proativo, destina-se a detectar, identificar, avaliar e neutralizar as ações da Inteligência adversa e outras ações de qualquer natureza, dirigidas contra os interesses da sociedade e do Estado.

No segmento Segurança Orgânica, destacamos a existência, no Brasil, do Programa Nacional de Proteção ao Conhecimento (PNPC)[11] e do Programa Nacional de Integração Estado-Empresa na Área de Bens Sensíveis (Pronabens)[12].

Com relação à Segurança Ativa, limitaremos nossa apreciação ao seu desdobramento na Contraespionagem[13], ou seja, o conjunto de medidas voltado para detecção, identificação, avaliação e neutralização das ações adversas de busca de conhecimento e dados sigilosos.

Allen Welsh Dulles (1963, p. 175) sintetiza de maneira bastante apropriada a maneira como um serviço de Contraespionagem deve atuar eficientemente: "É claro que se um país pretende proteger-se contra a incessante invasão dos serviços de espionagem hostis, tem de fazer mais qualquer coisa que vigiar os viajantes estrangeiros que atravessam suas fronteiras, que colocar guardas em volta de áreas 'estratégicas', ou que averiguar a lealdade dos seus empregados em posições de destaque. Tem também de descobrir o que procuram os serviços de espionagem das nações hostis, como procedem, que espécie de agentes usam e quem são."

Disto depreendemos que uma proteção efetiva do Conhecimento Sensível não pode se dar somente com medidas de Segurança Orgânica nos limites do território nacional. As medidas de Segurança Ativa são igualmente fundamentais, e só terão êxito se calcadas em atividade de Inteligência no exterior. Shulsky e Schmitt reforçam esta assertiva, ao se referirem à Contraespionagem como "medidas que procuram entender como um serviço de Inteligência estrangeiro atua, a fim de frustrá-lo, impedir suas ações, ou, no extremo, volver tais ações em nossa própria vantagem" (2002, p. 108).

---

11 Para mais informações sobre a aplicação recente do PNPC, q.v. BALUÉ e NASCIMENTO, 2006, NOGUEIRA, 2012 e CRUZ, 2012.

12 Tendo em vista a adesão do Brasil aos principais regimes e às convenções internacionais estabelecidos pelos países comprometidos com o desarmamento e a não proliferação nucleares, o Ministério da Ciência, Tecnologia e Inovação (MCTI) e a Agência Brasileira de Inteligência (Abin) conceberam o Pronabens.

13 A Segurança Ativa desdobra-se didaticamente em contraespionagem, contraterrorismo, contrassabotagem e contrapropaganda.

Sob a perspectiva da ação da Ciberespionagem, vislumbramos também a necessidade do envolvimento de órgãos vocacionados para a Guerra Cibernética[14] com as medidas de Segurança Ativa.

A seguir, veremos que, em um quadro de continuidade do interesse estrangeiro na busca por dados nacionais sigilosos, o desenvolvimento do PNB representa um potencial alvo.

UM CONHECIMENTO NACIONAL A SER PROTEGIDO

O domínio da tecnologia nuclear é considerado estratégico[15] e objeto permanente de atenção das potências internacionais, principalmente em razão de presumir capacitação para desenvolvimento e produção de ADM, tanto pelo Estado desenvolvedor da tecnologia como por terceiros Estados que venham a ter acesso por seu intermédio, consentido ou não (EISENHOWER, 1953). A preocupação legítima com a proliferação nuclear, suscitando questões como a própria destruição da Humanidade, levou à criação da Agência Internacional de Energia Atômica (AIEA), órgão das Nações Unidas que objetiva a aceleração e a ampliação da contribuição da energia atômica para a paz, a saúde e a prosperidade pelo mundo, e assegurar, na medida do possível, que tal energia não seja usada para propósitos bélicos (AIEA, 2013).

O Brasil possui estatura de relevo neste setor de alto grau de especialização e sofisticação tecnológica, a nível mundial, sendo um país que detém o domínio tecnológico de todas as fases do ciclo do combustível nuclear

Neste sentido, compreendem-se as reações internacionais de oposição aos programas nucleares desenvolvidos por Irã e Coreia do Norte (ONU, 2013), como também ocorrera em 1990 em relação ao Iraque. No sentido oposto, encontram-se os próprios Estados interessados na obtenção de armamento nuclear, que lançam mão de Espionagem para sobrepujar os obstáculos internacionais impostos à proliferação, como foi o caso do Paquistão[16].

Contudo, além das nobres considerações quanto à paz e à segurança mundiais, a tecnologia nuclear também se coloca como uma variável relevante no equacionamento das matrizes energéticas dos Estados, carreando assim interesse econômico e, por conseguinte, da Inteligência estrangeira. Evidentemente, as atividades nucleares estão inseridas num mercado altamente competitivo. Os países competem por mercados para venda de reatores (de potência e de pesquisa), de radiofármacos, de urânio, de combustível nuclear, de serviços de enriquecimento de urânio, e de equipamentos pesados para o setor, entre outros itens. Então, surge o risco

14 A Estratégia Nacional de Defesa atribui ao Ministério da Defesa (MD) e ao MCT, por intermédio do Departamento de Ciência e Tecnologia do Exército, a promoção de ações que contemplem a multidisciplinaridade e a dualidade das aplicações no setor cibernético (BRASIL, 2012a).

15 Os setores cibernético, nuclear e espacial são considerados estratégicos e decisivos para a Defesa Nacional (BRASIL, 2012a).

16 O cientista nuclear Abdul Qadeer Khan, considerado o "Pai da Bomba Paquistanesa", furtou a tecnologia de enriquecimento de urânio da companhia Urenco, na Holanda, quando lá trabalhara entre 1972 e 1975, e a aplicou na instalação da Usina de Kahuta, Paquistão. Posteriormente, liderou uma rede clandestina de venda da tecnologia para Irã, Coreia do Norte e Líbia, que seria desmantelada em 2004 (OLIVEIRA, 2008, p. 4-5).

do aproveitamento de um discurso de não proliferação nuclear como cobertura para a obstrução de um programa de finalidade autenticamente não bélica.

O Brasil possui estatura de relevo neste setor de alto grau de especialização e sofisticação tecnológica, a nível mundial, sendo um país que detém o domínio tecnológico de todas as fases do ciclo do combustível nuclear, com destaque para a tecnologia própria de enriquecimento de urânio por ultracentrifugação.

A busca por esta tecnologia remonta a 1953, a partir dos entendimentos realizados pelo Almirante Álvaro Alberto da Mota e Silva com os cientistas alemães Wilhelm Groth, Konrad Beyerle e Otto Hahn, que culminaram na aquisição sigilosa de três ultracentrífugas. Estes equipamentos, entretanto, acabaram apreendidos na Alemanha Ocidental, por ordem do Alto Comissário dos EUA, em conformidade com uma política estadunidense de negação de transferência de tecnologias nucleares a países do Terceiro Mundo. Na superação destas barreiras, o Brasil desenvolveu, a partir de 1979, sua própria tecnologia de enriquecimento, inclusive com o recurso à Espionagem. Logrou sucesso em 1987, com a operação da ultracentrífuga projetada pelo então Capitão de Fragata engenheiro naval Othon Luís Pinheiro da Silva (MONIZ BANDEIRA, 2011).

Deparamo-nos no Brasil com óbices de ordem cultural que representam talvez as maiores resistências para a implantação da mentalidade de Inteligência nas instituições públicas

A esta conquista se acrescenta a decisão governamental de investir em projetos que projetarão ainda mais o País neste setor, dos quais podemos destacar: a retomada da construção da usina de Angra III, a construção de pelo menos quatro novas usinas nucleares em território nacional (com possibilidade de serem oito novas usinas) até 2030, desenvolvimento e construção de depósito definitivo de rejeitos radioativos de baixa e média atividades (GONÇALVES FILHO, 2011), desenvolvimento e construção de reator nuclear multipropósito (CORRÊA, 2013) e a produção de submarino movido a propulsão nuclear (BRASIL, 2012b).

Como se ainda precisássemos explicitar mais sobre o interesse adverso no PNB, destacamos dois exemplos concretos, primeiramente um de Espionagem humana, e outro de campanha de desinformação na mídia.

Entre 1992 e 1994, o já Almirante Othon, como coordenador da Coordenadoria de Projetos Especiais da Marinha em São Paulo (Copesp) teve um agente de Inteligência estadunidense como vizinho do apartamento em que residia (MONIZ BANDEIRA, 2011, p. 270-271), que o vigiou durante o período.

Em 2004, veículos de comunicação estadunidenses e argentinos polemizaram em torno da negativa brasileira de permitir acesso de inspetores da AIEA às ultracentrífugas instaladas nas Indústrias Nucleares Brasileiras (INB)[17], levantando suspeitas

17 "O Comando da Marinha, responsável pelas ultracentrífugas para enriquecimento de urânio, e as agências brasileiras do setor advertiram o governo de que por trás das pressões da AIEA, atrás das quais o Departamento de Estado [dos EUA] se movia, poderia existir o objetivo de espionagem da tecnologia de ponta desenvolvida pelo Brasil e considerada superior à americana e à francesa." (MONIZ BANDEIRA, 2005, p. 78) Os almirantes Othon Luiz Pinheiro da Silva (2004) e Tiudorico Leite Barboza (2005, p.73), ambos engenheiros navais, endossaram esta possibilidade.

de que o Brasil estaria envolvido com a proliferação nuclear.[18]

MENTALIDADE DE CONTRAINTELIGÊNCIA NO BRASIL

Deparamo-nos no Brasil com óbices de ordem cultural que representam talvez as maiores resistências para a implantação da mentalidade de Inteligência nas instituições públicas, a despeito da existência de alguma compreensão, em determinados setores, acerca dos interesses e da probabilidade de atuação de Inteligência estrangeira em nosso país.

Infelizmente, o que se vê como regra são tão somente reações após a ocorrência de um infortúnio ─ isto quando se toma conhecimento do infortúnio, muitas vezes catastrófico. Como diz o adágio popular, "depois da porta arrombada, põe a tranca na porta".

Carecemos ainda do fortalecimento de uma cultura democrático-cidadã, assim como de uma cultura capaz de ser sensível à percepção de ameaças à segurança da sociedade e do Estado

Especialistas, acadêmicos ou não, da área de Inteligência no Brasil reconhecem que há uma percepção distorcida, tanto por parte dos tomadores de decisão quanto por parte da sociedade em geral – incluída aí a mídia[19] – da atividade de Inteligência. Na verdade, tal incompreensão e preconceito se verificam mesmo no seio de instituições estatais, nos setores que não lidam com a atividade. De fato, persiste, mesmo após décadas de retorno à democracia, a associação dos serviços secretos com as arbitrariedades cometidas durante o regime militar que vigeu por 21 anos no Brasil[20].

Enquanto o crescimento econômico reposiciona o Brasil no mundo, no âmbito doméstico a classe política e a sociedade em geral não se mostram devidamente preparadas para reconhecer o papel que a atividade de Inteligência joga na qualificação do País como ator no cenário internacional. Verifica-se "desconhecimento generalizado da essência da atividade: ferramenta parcial e oportuna, pautada em evidências coletadas e analisadas com metodologia e racionalidade, cujo objetivo exclusivo é apoiar o processo decisório nacional, definidor do destino da sociedade e do Estado brasileiro" (REBELLO, 2006, p. 37).

A conformação da política de um país reflete a cultura do seu povo. Carecemos ainda do fortalecimento de uma cultura democrático-cidadã, assim como de uma cultura capaz de ser sensível à percepção de ameaças à segurança da sociedade e do Estado. Mesmo setores elitizados de nossa sociedade mostram-se incapazes de perceber que o Brasil é alvo do interesse, por exemplo, de comunidades científicas internacionais e das empresas que as financiam. Rebello (2006, p. 44) ilustra o descaso com a proteção do conhecimento

18 Lembramos que em 2004 ocorreu o desmonte da rede de contrabando tecnológico nuclear do Dr. Khan, já citada.

19 Vide a reportagem da revista *Veja* de 19 de junho de 2013 (MARQUES e RANGEL, 2013), que expõe a público, pejorativamente, a identidade de agentes e veículos da Abin empregados em missão de vigilância no porto de Suape, e que, no mínimo, não leva em consideração a segurança pessoal ou familiar dos citados servidores do Estado Brasileiro.

20 A atuação dos "órgãos de informações" militares naquele período, ao confundir a atividade de Inteligência com a de Segurança, seria a responsável pela repulsa de parte da sociedade brasileira aos serviços de Inteligência (ANTUNES, 2001, p. 193).

sensível nacional ao destacar dois casos. O primeiro é o do cupuaçu – fruta típica da Região Norte –, que teve seu nome patenteado por empresa japonesa. O segundo caso é o da rapadura – doce tipicamente brasileiro –, cuja tentativa de exportação por produtores cearenses foi inviabilizada, uma vez que empresa alemã já possuía a patente do nome.

Apesar dos sérios argumentos acima mencionados, há que se reconhecer que, desde 1980, o Brasil vem desenvolvendo atividades que visam à proteção do conhecimento sensível. Em 1983, a Escola Nacional de Informações desenvolveu o primeiro Estágio de Proteção da Informação Empresarial, com o propósito de oferecer instrumentos para auxiliar as instituições a protegerem informações empresariais sensíveis. Posteriormente, a partir da criação da Abin, e com base no artigo 4º da Lei 9.883/99, que atribui àquela Agência a competência de "planejar e executar a proteção de conhecimentos sensíveis, relativos aos interesses e à segurança do Estado e da sociedade", coube ao seu Departamento de Contrainteligência a responsabilidade de cumprir o disposto na lei, por meio da aplicação do PNPC.

É imperativo que seja amplamente disseminada, fortalecida e consolidada, nos âmbitos da administração pública, do setor privado e do meio acadêmico, a mentalidade da Contrainteligência, especialmente no seu aspecto de proteção do conhecimento sensível

Não resta dúvida de que esse é um desenvolvimento importante. No entanto, é forçoso reconhecer que, a despeito da existência do PNPC, há um longo caminho a ser percorrido, sobretudo no âmbito da administração pública federal, para a efetivação de uma mentalidade de Contrainteligência. Consideramos que o PNPC, como um instrumento demandante de cooperação das entidades nacionais, públicas ou privadas, que geram ou custodiam conhecimentos sensíveis para o Brasil, não tem sido suficiente para atingir o propósito de proteção destes conhecimentos.

Nossa assertiva respalda-se no levantamento feito pela Controladoria-Geral da União (CGU) até 14 de junho de 2013, sobre os órgãos públicos ligados à União que usaram a classificação para manter dados sob sigilo. Destacamos que, de todas as universidades federais, somente quatro[21] fizeram uso de classificação sigilosa. Ou seja, uma das medidas mais triviais de proteção de conhecimento sensível, que é a atribuição de classificação sigilosa[22], não estaria sendo observada por uma série de órgãos responsáveis[23].

Na área nuclear, entre alguns exemplos de vulnerabilidades que podem suscitar a

21 Fundação Universidade Federal de Ciências da Saúde de Porto Alegre - UFCSPA, Fundação Universidade Federal do ABC – UFABC, Universidade Federal de Itajubá – Unifei e Universidade Federal de Santa Catarina – UFSC (BRASIL, 2013b).

22 O artigo 23 da Lei 12.527/ 2011 relaciona as informações consideradas imprescindíveis à segurança da sociedade ou do Estado.

23 Um representante da comissão criada dentro da UFSC para analisar e classificar os dados em 2012 para que nenhum trabalho seja usado inadequadamente (FELLTHAUS, 2013).

perda de conhecimentos sensíveis podemos mencionar a internacionalização da comunidade científica, uma vez que há intensa interação entre os especialistas do setor, requerida pelo exercício de suas funções – troca de visitas técnicas, treinamentos, participação em congressos, cursos e reuniões internacionais etc. Surge, assim, a possibilidade de vazamento de dados sigilosos por parte de servidores motivados (ou desmotivados) por diferentes causas, brechas na segurança cibernética, publicações em periódicos internacionais sem prévia aprovação do órgão, e até recrutamento por serviço de Inteligência estrangeiro (de forma consciente ou não). Portanto, as ações a serem planejadas devem conter enfoque realista, aplicado às práticas usuais dos servidores e dirigentes do órgão em questão.

Diante do exposto, e na medida em que o Brasil capacita-se para ser, e manter-se, como um Estado-chave para as discussões no contexto das principais agendas temáticas do século XXI, é imperativo que seja amplamente disseminada, fortalecida e consolidada, nos âmbitos da administração pública, setor privado e meio acadêmico, a mentalidade da Contrainteligência, especialmente no seu aspecto de proteção do conhecimento sensível.

Em última instância, como se poderá depreender, a relevância do tema evidencia-se pela contribuição para o desenvolvimento e a manutenção dos seguintes Objetivos Fundamentais do Estado Brasileiro: Progresso e Soberania (ESCOLA SUPERIOR DE GUERRA, 2013, p. 24-25).

A OPERACIONALIZAÇÃO DA CONTRAINTELIGÊNCIA NO SIPRON

Na exposição de motivos do anteprojeto encaminhado pelo MCTI em 2003, que redundou na Lei 12.731/ 2012, constam, entre as preocupações elencadas:

c) a perfeita caracterização do Sipron como sistema responsável por garantir a prevenção e a pronta resposta às ocorrências que possam comprometer as atividades nucleares no País; e

d) o enquadramento das atividades relacionadas à área nuclear como assunto de interesse estratégico do Estado.

Como vimos, a cultura de Inteligência e Contrainteligência no Brasil é ainda bastante incipiente, seja por sua associação ao período de exceção dos governos militares, seja pela fraca percepção de ameaças, internas e externas, à segurança da sociedade e do Estado. Conforme temos procurado demonstrar, essas condições afetam sensivelmente a proteção dos conhecimentos sensíveis do setor nuclear nacional.

No contexto do Sipron original (1980), foi estabelecida, em 1998, no âmbito da Secretaria de Assuntos Estratégicos (SAE), a Norma Geral para o Planejamento e a Execução da Proteção ao Conhecimento Sigiloso (NG-08), com o objetivo de "orientar o planejamento da Proteção ao Conhecimento Sigiloso dos órgãos do Sipron, estabelecendo diretrizes quanto à forma de proteger os conhecimentos sigilosos considerados de interesse do Estado, particularmente aqueles relacionados aos projetos, às atividades e às instalações nucleares" (BRASIL, 1998).

Com efeito, a NG-08 significou um passo importante no sentido de aplicar, no contexto das instituições que integram o PNB, o conceito e as medidas de Contrainteligência. No entanto, a despeito de tal evolução à época, atualmente reconhecemos que seu cumprimento tem sido negligenciado por parte das instituições pelas quais deveria ser aplicada, como já demonstrado no levantamento realizado pela CGU em junho de 2013.

Nos últimos 15 anos (1998-2013), importantes transformações ocorreram nos

cenários nacional e internacional no que tange ao tema nuclear. Internamente, a usina Angra II entrou em operação (2000), o governo de Luís Inácio Lula da Silva (2003-2011) decidiu reativar os projetos estratégicos do setor e o País encarou desafiadoras negociações internacionais no campo das salvaguardas internacionais aplicadas pela AIEA (MONIZ BANDEIRA, 2011, p. 321, n. 3). Externamente, as mudanças climáticas ensejaram o reposicionamento da opção nuclear como efetiva contribuição à diminuição do aquecimento global. Com isso, deu-se o que se convencionou denominar "renascimento da energia nuclear" em nível global.

Assim, acreditamos que as significativas transformações ocorridas no âmbito doméstico – onde se destacam a construção de instalações para enriquecimento de urânio em escala industrial e a construção de submarino movido a propulsão nuclear – repercutiram em Brasília a ponto de fomentar a reformulação das atribuições do Sipron, formalizada em 2012.

Tomando por base as especificidades institucionais e culturais nas quais ocorrem os esforços para aplicação da Contrainteligência no âmbito dos organismos do PNB, advogamos que certas medidas podem ser observadas com vistas a tornar o Sipron, reformulado em 2012, mais operacional no que tange à proteção do conhecimento sensível nuclear. Deste modo, apresentaremos algumas propostas que estimamos possam ser aproveitadas quando da regulamentação da Lei Nº 12.731/2012.

A NG-08 de 1998 prevê como "ações a serem implementadas pelos órgãos do Sipron" as seguintes, que consideramos ainda passíveis de aproveitamento no decreto de regulamentação da nova lei, ao encontro da atribuição do Sipron de "coordenar as ações" que visem proteger os conhecimentos e a tecnologia da área nuclear:

a) elaboração dos Planos Diretores de Proteção ao Conhecimento Sigiloso;

b) supervisão da execução do Plano Diretor de Proteção ao Conhecimento Sigiloso; e

c) cumprimento, no que couber, das diretrizes contidas nos Planos Diretores de Proteção ao Conhecimento Sigiloso.

É importante observar que a NG-08 estabelece que os Planos Diretores devam contemplar a adoção de medidas de segurança adequadas às necessidades particulares de cada órgão. Diz ainda que tais planos, "e suas respectivas regulamentações, no âmbito do Sipron, deverão orientar os órgãos integrantes do Sistema no cumprimento das legislações especial e comum sobre a proteção dos assuntos sigilosos de interesse da sociedade e do Estado brasileiros, particularmente, quanto às responsabilidades de natureza civil, penal e administrativa".

Ou seja, enquanto a lei de 2012 se refere a "coordenar ações", não especifica quais seriam as tais "ações" a serem coordenadas. Propomos que sejam mantidas as ações que foram estabelecidas em 1998.

Adicionalmente, entendemos como necessária uma articulação formal mais efetiva entre o Sisbin e o Sipron. O distanciamento entre estes sistemas é uma situação curiosa, permitindo inferir que, até o momento, o fato de ambos se encontrarem sob a coordenação de um mesmo órgão, o Gabinete de Segurança Institucional da Presidência da República (GSI/PR), não estaria se concretizando como fator de força para o fortalecimento da Contrainteligência no PNB.

De acordo com o arcabouço jurídico em vigor, "o Sistema Brasileiro de Inteligência é responsável (...) pela salvaguarda de assuntos sigilosos de interesse nacional" (BRASIL, 2002). Desta forma, entende-se que são competências dos órgãos do Sisbin

tanto a discriminação dos elementos do PNB que sejam potenciais alvos do interesse de serviços de Inteligência estrangeiros como a adoção das correspondentes medidas de Segurança Ativa, em especial as de Contraespionagem.

Conforme evidenciado pela Tabela 1, essa articulação ainda carece de ser aperfeiçoada, uma vez que no Sipron ainda há vários órgãos que não se relacionam formalmente com o Sisbin[24]. Em outras palavras, apontamos a ocorrência de órgãos integrantes do Sipron não participantes do Sisbin como uma vulnerabilidade na proteção dos conhecimentos e tecnologia detidos por esses órgãos[25].

Para superar tal vulnerabilidade, propomos que, na regulamentação da Lei 12.731/2012, seja previsto o estabelecimento da figura do "oficial de Ligação de Contrainteligência" em cada órgão integrante do Sipron. Este "oficial de Ligação" deverá ser formalmente qualificado e designado, tendo como um dos requisitos de qualificação a realização, por exemplo, do Curso Superior de Inteligência Estratégica (CSIE), ministrado pela Escola Superior de Guerra, ou equivalente designado pelo Órgão Central do Sisbin (Abin) – que também vem a ser Órgão de Coordenação Setorial de Inteligência do Sipron. A realização de curso especializado é de crucial

TABELA 1 – Órgãos do Sipron que não integram o Sisbin[26]

ÓRGÃOS	FUNÇÃO NO SIPRON
Centrais Elétricas Brasileiras S.A. (Eletrobras)	Órgão de Execução Seccional
Eletrobras Termonuclear S.A. (Eletronuclear)	Órgão de Execução Seccional
Entidades de ensino e pesquisa científicas[27] (federais, estaduais ou privadas) que participem em projeto ou atividade nuclear ou, ainda, que possuam instalação nuclear no País	Órgãos de Execução Seccional
Ministério dos Transportes	Órgão de Apoio
Ministério do Planejamento, Orçamento e Gestão	Órgão de Apoio
Ministério das Comunicações	Órgão de Apoio
Prefeituras Municipais em cujos territórios se desenvolvam projetos ou atividades do Programa Nuclear Brasileiro	Órgãos de Apoio
Empresas ou entidades do setor privado que, por contrato ou outro documento hábil, prestam serviços relacionados com a segurança de projetos e atividades do Programa Nuclear Brasileiro	Órgãos de Apoio

Fontes: BRASIL, 2002 e 2013.

24 No Apêndice, a Tabela 2 explicita os órgãos do Sipron que integram o Sisbin.

25 O Ministério das Minas e Energia, apesar do envolvimento com a mineração de urânio e geração de energia nucleoelétrica, não figura como participante nem do Sipron nem do Sisbin. Contundo, figura na composição da Comissão de Coordenação da Proteção ao Programa Nuclear Brasileiro (Copron) (BRASIL, 2012e).

26 Consideramos que as INB, Órgão de Execução Seccional do Sipron, estariam ligadas ao Sisbin via MCTI (BRASIL, 2013).

27 Exceto os institutos militares – CTMSP, CTEx e IEAv do Departamento de Ciência e Tecnologia Aeroespacial.

importância para o exercício da função institucional, a qual guarda estreita relação com o caráter estratégico das atividades nucleares desenvolvidas no País. Com tal iniciativa, espera-se consolidar, gradativa e regularmente, a formação de quadros especializados em Contrainteligência no âmbito do setor nuclear.

Outra proposta seria a instituição de duas reuniões anuais de coordenação do Sipron. A primeira reunião seria interna de cada órgão, conduzida pelo "oficial de Ligação do Sipron" e tendo como público-alvo a Alta Direção (diretores e vice-diretores, ou DAS 6 e 5) e os gestores de média gerência (chefes de departamento ou DAS 4), com vistas à sensibilização sobre o tema Contrainteligência e formulação de subsídios para discussão com os demais órgãos do sistema, e também do Sisbin. Esta seria uma forma direta de promover o efetivo envolvimento dos tomadores de decisão e respectivos assessores do setor nuclear no tema "Inteligência de Estado." Cremos que a persistência do hiato de conhecimento entre o nível de tomada de decisão e o nível operacional nesta área tão sensível implicará a impossibilidade do cumprimento do previsto na lei.

A segunda reunião, decorrente da primeira, envolveria todos os órgãos integrantes do Sipron que participam do Sisbin, com os propósitos de discutir o próprio fortalecimento da Contrainteligência no Sipron e, principalmente, de superar barreiras burocráticas e de confiança existentes entre os órgãos.

Com base no que precede, acreditamos ser possível tornar mais operacional o Sipron, estimulando tanto a realização de ações eficazes, eficientes e efetivas pelos órgãos que o integram quanto gerando insumos para uma coordenação perene das ações de Contrainteligência no PNB.

CONCLUSÃO

Como procuramos demonstrar, a Espionagem continua sendo, nos dias de hoje, um recurso utilizado pelos Estados na defesa de seus interesses, sendo forçoso reconhecer que o PNB é um potencial alvo do interesse da Inteligência estrangeira.

Desse modo, identificamos a regulamentação da Lei 12.731/2012 como um momento por demais oportuno para promover o aperfeiçoamento da Contrainteligência nos órgãos que integram o Sipron, estabelecendo efetivos mecanismos de operacionalização do sistema e levando em consideração a modernidade das ameaças que se figuram, notadamente a Ciberespionagem.

A institucionalização da Contrainteligência, aproximando mais o Sipron do Sisbin, é requisito básico para subsidiar e robustecer o caráter estratégico das atividades nucleares do País. No entanto, o estabelecimento formal da Contrainteligência no âmbito do setor nuclear por meio da lei não é, isoladamente, suficiente. O comprometimento da Alta Direção das instituições nucleares é crucial.

No eixo operacional, a formalização da figura dos oficiais de Ligação de Contrainteligência poderá contribuir para:

– a formação de quadros especializados em atividades de Inteligência em nível estratégico nos órgãos do setor nuclear;

– um maior engajamento de seus órgãos no Sipron, notadamente no que tange à proteção do conhecimento sensível da área nuclear; e

– apoiar, de maneira mais eficiente e racional, as medidas de Segurança Ativa do Sisbin.

Vislumbramos, assim, uma maneira eminentemente prática de contribuir para a criação paulatina de uma mentalidade proativa e sinergética de Contrainteligência no

País, experiência que poderia no futuro até ser replicada, após a obtenção de resultados consistentes, em outros setores estratégicos do governo.

Enfim, esperamos que este artigo seja mais um incentivo à ruptura do paradigma brasileiro da "porta arrombada", neste caso com relação ao PNB.

🗁 CLASSIFICAÇÃO PARA ÍNDICE REMISSIVO:
<INFORMAÇÃO>; Inteligência; Espionagem; Sistema de informação; Segurança da informação; Programa nuclear;

REFERÊNCIAS

As referências relativas a este artigo podem ser consultadas com os autores.

APÊNDICE

TABELA 2 – Órgãos do Sipron que integram o Sisbin

ÓRGÃO	FUNÇÃO NO SIPRON	COMO SE INTEGRA AO SISBIN
Gabinete de Segurança Institucional da Presidência da República (GSI/PR)	Órgão Central	Órgão de coordenação das atividades de Inteligência federal
Agência Brasileira de Inteligência (Abin)	Órgão de Coordenação Setorial	Órgão Central
Ministério da Ciência e Tecnologia (MCT)	Órgão de Coordenação Setorial, por meio da Comissão Nacional de Energia Nuclear (CNEN)	por meio do Gabinete do Ministro de Estado
Ministério do Trabalho e Emprego (MTE)	Órgão de Coordenação Setorial, por meio do Departamento de Segurança e Saúde no Trabalho	por meio da Secretaria Executiva
Ministério da Integração Nacional	Órgão de Coordenação Setorial	por meio da Secretaria Nacional de Defesa Civil
Ministério do Meio Ambiente	Órgão de Coordenação Setorial, por meio do Instituto Brasileiro do Meio Ambiente e dos Recursos Naturais Renováveis (Ibama)	por meio do Ibama e da Secretaria Executiva
Ministério da Justiça	Órgão de Apoio	por meio da Secretaria Nacional de Segurança Pública, da Diretoria de Inteligência Policial do Departamento de Polícia Federal, do Departamento de Polícia Rodoviária Federal, do Departamento Penitenciário Nacional e do Departamento de Recuperação de Ativos e Cooperação Jurídica Internacional da Secretaria Nacional de Justiça
Ministério das Relações Exteriores (MRE)	Órgão de Apoio	por meio da Secretaria-Geral de Relações Exteriores e da Coordenação-Geral de Combate aos Ilícitos Transnacionais
Ministério da Defesa	Órgão de Apoio	por meio da Subchefia de Inteligência Estratégica, da Assessoria de Inteligência Operacional, da Divisão de Inteligência Estratégico-Militar da Subchefia de Estratégia do Estado-Maior da Armada, do Centro de Inteligência da Marinha (CIM)[28], do Centro de Inteligência do Exército (CIE), do Centro de Inteligência da Aeronáutica (CIAer) e do Centro Gestor e Operacional do Sistema de Proteção da Amazônia
Ministério da Fazenda	Órgão de Apoio	por meio da Secretaria Executiva do Conselho de Controle de Atividades Financeiras (Coaf), da Secretaria da Receita Federal do Brasil (SRF) e do Banco Central do Brasil
Ministério da Saúde	Órgão de Apoio	por meio do Gabinete do Ministro de Estado e da Agência Nacional de Vigilância Sanitária (Anvisa)
Governos estaduais em cujos territórios se desenvolvam projetos ou atividades do PNB	Órgãos de Apoio	poderão integrar mediante ajustes específicos e convênios

Fontes: BRASIL, 2002 e 2013

28 Na MB, o CIM é o órgão responsável pela centralização e coordenação da produção de conhecimentos de Contrainteligência, bem como pela coordenação e supervisão da Segurança Ativa (BRASIL, 2012c).