A RELAÇÃO ENTRE POLÍTICAS PÚBLICAS NAS ÁREAS DE INTELIGÊNCIA E DE INDÚSTRIA DE DEFESA NO BRASIL: um debate necessário

Peterson Ferreira da Silva*

> "I suppose that if we in intelligence were one day given three wishes, they would be to know everything, to be believed when we spoke, and in such a way to exercise an influence to the good in the matter of policy"
>
> **Sherman Kent**[1]

Resumo

O objetivo deste artigo é discutir a relação entre as políticas públicas delineadas para as áreas de inteligência de Estado e de indústria de defesa no Brasil. Nas últimas décadas, o acelerado avanço tecnológico das Tecnologias de Informação e de Comunicação (TICs) suscitou diversas consequências para a atividade de inteligência de uma forma geral. Contudo, embora o fortalecimento doméstico de determinados campos tecnológicos seja de fundamental importância não só para a área de defesa nacional, mas também para a de inteligência de Estado, observa-se que o debate sobre essa relação tem se desenvolvido ainda de forma incipiente no Brasil.

O acelerado avanço tecnológico e a atividade de inteligência na atualidade

Atualmente, são visíveis as consequências do acelerado avanço tecnológico para a atividade de inteligência[2] em vários países, especialmente no que se refere às Tecnologias de Informação e Comunicação (TICs). Hoje, satélites e plataformas aéreas, por exemplo, fornecem diversos tipos de dados geoespaciais, assim como possibilitam comunicações em tempo real. Tais informações

* Doutor em Relações Internacionais (IRI-USP) e, atualmente, pesquisador associado ao Laboratório de Estudos das Indústrias Aeroespaciais e de Defesa (LabA&D/UNICAMP) e ao Centro de Estudos Estratégicos do Exército Brasileiro (CEEEx/EME).

1 *'Sherman Kent and the Board of National Estimates: Collected Essays' – 'Estimates and influence'. Studies of Intelligence*, Summer 1968. Disponível em: <https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/sherman-kent-and-the-board-of-national-estimates-collected-essays/4estimates.html >. Acesso em: 09 jul. 2016.

2 Neste artigo, atividade de inteligência será entendida como o *"exercício permanente de ações especializadas, voltadas para a produção e difusão de conhecimentos, com vistas ao assessoramento das autoridades governamentais nos respectivos níveis e áreas de atribuição, para o planejamento, a execução, o acompanhamento e a avaliação das políticas de Estado"* (Decreto nº 8.793, de 29 de junho de 2016, o qual fixa a Política Nacional de Inteligência – PNI), em suas acepções estratégica, tática e operacional.

podem ser utilizadas nas mais distintas atividades militares e civis, como vigilância de fronteiras, monitoramento agrícola, planejamento territorial e atuação contra crimes ambientais, constituindo-se um campo em expansão inclusive no Brasil.[3]

Outro fator importante é a diversidade de soluções tecnológicas disponíveis no mercado internacional para os segmentos de segurança e defesa, como sistemas de radiocomunicação criptografados, de videomonitoramento e de geo-informação (ex. georreferenciamento de ocorrências e de viaturas), além de serviços de processamento como sintetizadores para análise de filmagens, de mineração de dados (data mining), de segurança de redes e de extração de informações de câmeras, computadores e celulares.

Incrementos tecnológicos, no entanto, também podem gerar novas vulnerabilidades e ameaças. O emprego de Veículos Aéreos Não Tripulados (VANTs), por exemplo, ganhou notoriedade pelo seu papel nos conflitos no Iraque e no Afeganistão e pela polêmica envolvendo o assassinato seletivo de indivíduos associados ao terrorismo. Cabe destacar que o emprego dessa plataforma também exigiu mudanças conceituais e organizacionais importantes, como maior cooperação interagências entre as atividades militares (ex. operações especiais) e as de inteligência (ex. *targeting officers*).[4] Contudo, conforme os VANTs vão cada vez mais se difundindo para atividades comerciais civis variadas (ex. entretenimento), multiplicam-se tentativas não só de se contrapor a tal tecnologia,[5] mas também de empregá-los, por exemplo, em atividades ilegais e em atentados (BOYLE, 2015; OGURA, 2015).

No mesmo sentido, a profusão dos *smartphones* vem transformando o cotidiano de pessoas em todo o mundo, propagando fotos e vídeos por redes sociais, descortinando novas formas de desenvolvimento de aplicativos e oferecendo produtos e serviços personalizados via dados coletados sobre localização, rede de amizades, preferências e hábitos (MAOR, 2013). No entanto, ainda não estão claros os limites de coleta de

[3] Consultar, por exemplo, Vasconcelos (2016) e as informações disponibilizadas pelo Instituto Nacional de Pesquisas Espaciais (INPE) sobre o Programa do Satélite Sino-Brasileiro de Recursos Terrestres (CBERS) < http://www.cbers.inpe.br/sobre_satelite/introducao.php >. Acesso em: 06 jul. 2016.

[4] O ataque bem sucedido, realizado em 2016, no Paquistão contra o líder do Taliban, Mullah Akhtar Mansour, ilustra como a interceptação de comunicações, o uso de *drones* e a combinação de outras fontes de inteligência são capazes, atualmente, de alimentar operações militares. Ver, por exemplo, Entous e Donati (2016).

[5] As interceptações de vídeos gerados por *drones* no Iraque (GORMAN; DREAZEN; COLE, 2009) e as tentativas dos cartéis de drogas mexicanos de interferir em *drones* utilizados pela agência norte-americana *Customs and Border Protection* (CBP) podem ser vistas como interessantes exemplos nesse contexto (TUCKER, 2015).

dados dos usuários por parte das empresas, levantando toda uma série de questões sobre privacidade e sobre como tais informações podem ser utilizadas por companhias e, nesse contexto, qual seria o papel dos governos (SINGER, 2016).

Assim, por um lado, o avanço tecnológico beneficiou aparatos dedicados especificamente à inteligência de sinais (SIGINT) de países como os EUA (ex. *National Security Agency* – NSA) e o Reino Unido (ex. *The Government Communications Headquarters* – GCHQ), expandindo o alcance dos serviços de inteligência das grandes potências ocidentais praticamente para todo o mundo (ex. "*Five Eyes*": Estados Unidos, Reino Unido, Austrália, Canadá e Nova Zelândia) (BAMFORD, 2008). Dado o aperfeiçoamento das ferramentas de análise de grandes volumes de informações *online*, o Pentágono, por exemplo, estuda substituir os regulares levantamentos de segurança em seus funcionários por avaliações contínuas executadas por meio de buscas automáticas em diversas fontes, incluindo redes sociais (STERNSTEIN, 2016). Por outro lado, as mesmas condições que conferem vantagens frente a inimigos e oportunidades na cena internacional também ensejam vulnerabilidades que tornaram possíveis os vazamentos perpetrados, por exemplo, por Bradley Manning (LEIGH, 2010) e Edward Snowden (GREENWALD; POITRAS; MACASKILL, 2013). Além disso, há crescentes possibilidades de que a disseminação de tecnologias mais modernas ligadas à biometria (ex. reconhecimento facial e de íris) contribua, por exemplo, para o comprometimento de agentes encobertos (STEIN, 2012).

Alguns dos desafios atuais

Por trás desses desdobramentos conceituais e organizacionais está toda uma gama de financiamentos governamentais e segmentos do setor privado de base tecnológica. Paradigmático nesse sentido é o trabalho realizado pela norte-americana *Intelligence Advanced Research Projects Activity* (IARPA),[6] responsável por pesquisas de fronteira tecnológica de alto risco e de alto impacto no campo da inteligência. Outro fator importante é a diversidade de soluções tecnológicas disponíveis no mercado internacional para os segmentos de segurança e defesa, como sistemas de radiocomunicação criptografados, de videomonitoramento e de geo-informação (ex. georreferenciamento de ocorrências e de viaturas), além de serviços de processamento como sintetizadores para análise de filmagens, de mineração de dados (*data mining*), de segurança de redes e de extração de informações de câmeras, computadores e celulares. Combinadas, essas tecnologias podem compor, por exemplo, "sistemas de sistemas" integrados voltados à vigilância de fronteiras, ao monitoramento de sistemas de transporte, ao comando e controle no campo da segurança pública, à prevenção e mitigação de desastres (ex. enchentes e deslizamentos de terra) e à atividade de inteligência. Estima-se que somente o mercado global de cibersegurança, por exemplo, alcançará US$170 bilhões até 2020 (MORGAN, 2015).

[6] Cf. IARPA <https://www.iarpa.gov/index.php/about-iarpa>. Acesso em: 17 jul. 2016.

A relativa baixa capacidade estatal do país, em termos de políticas públicas, observada entre o final da década de 90 e o início dos anos 2000 também pode ser apontada como um fator importante para se compreender o delineamento das estruturas de inteligência e de defesa ocorridas nesse período.

Esses desdobramentos do desenvolvimento tecnológico no nível global certamente não ocorrem sem tensões políticas. Nos EUA, por exemplo, o escândalo promovido por Edward Snowden atraiu a atenção para o debate sobre liberdades civis, fomentando pressões a favor de um maior controle sobre as práticas de vigilância e de monitoramento empreendidas por seus órgãos de inteligência (LANDLER; SAVAGE, 2014). Os EUA também foram palco, em 2016, de uma intensa discussão envolvendo o dilema entre segurança e privacidade, tendo como objeto a tentativa do *Federal Bureau of Investigation* (FBI) de acessar as informações de um celular, produzido pela empresa norte-americana *Apple*, que pertencia à Syed Farook, o atirador do episódio ocorrido, em dezembro de 2015, em San Bernadino, Califórnia. Diante da recusa da *Apple* de prover o acesso às informações do celular (o que poderia abrir precedentes e brechas para outros acessos), o FBI teria optado por pagar US$1.3 milhões para uma empresa ainda não identificada para realizar o desbloqueio (YADRON, 2016).

Ademais, questões organizacionais também fazem parte das consequências do avanço da tecnologia para a atividade de inteligência. No Reino Unido, por exemplo, há mais indicativos de que seu serviço de inteligência interno, o MI5, estaria coletando mais informações (seja por meios próprios ou por parceiros) do que sua capacidade de análise pode plenamente acompanhar – deixando espaços para possíveis "falhas de inteligência" (GALLAGHER, 2016). Na França, são apontados fatores burocráticos e a falta de compartilhamento de informações entre suas organizações de inteligência como explicações para a incapacidade de detecção dos preparativos da série de ataques que assolaram o país entre 2015 e 2016 (SIMCOX, 2016).

"A revolução análoga"

De certa forma, os desafios trazidos para a atividade de inteligência pelo incremento e pela difusão das Tecnologias de Comunicação e Informação não são uma novidade em termos históricos. De acordo com Warner (2012), por exemplo, o conjunto de transformações vivenciado hoje nesse campo, definido por ele como uma "revolução digital", pode ser comparado ao que a invenção do rádio e a utilização sistemática do reconhecimento aéreo promoveram no contexto da I Guerra Mundial – o que Warner denominou de "revolução análoga" à atual.[7] Essas duas invenções, seus graduais

[7] "*World War I precipitated what might be called the 'analog revolution' in intelligence. Before the invention of radio and aerial photography, intelligence could still be conducted in ways essentially unchanged since the beginning of history.*" (WARNER, 2012, p. 138).

aperfeiçoamentos e suas absorções conceituais e organizacionais deram origem às disciplinas mais comumente conhecidas como inteligência de sinais (*signals intelligence* – SIGINT) e de imagens (*imagery intelligence* – IMINT), as quais foram expandidas e aprofundadas ao longo da Guerra Fria, impactando sobremaneira a atividade de inteligência como um todo. Assim:

> Transformações tecnológicas modelam e remodelam tanto as ameaças a um Estado quanto as oportunidades apresentadas para este na arena internacional e, portanto, desempenham um papel na determinação dos alvos de inteligência e dos meios que a inteligência emprega (WARNER, 2012, p. 135 – tradução minha)[8]

Ainda segundo Warner (2012, p. 152-153), a assim denominada "revolução digital" em andamento beneficiaria os sistemas de inteligência[9] que se adaptarem mais rapidamente a essas mudanças e, mais especificamente, aqueles que melhor conseguirem explorar todas as fontes possíveis de inteligência ("*all-source analysis*"), ou seja, tendo êxito em separar informações significativas e importantes em meio a um imenso volume de dados e informações coletados.

Nesse contexto, de acordo com Wirtz e Rosenwasser (2010), tornam-se cada vez mais importantes os esforços dedicados à combinação das variadas disciplinas de inteligência do modo mais efetivo possível, contemplando inteligência de imagens/geoespacial (IMINT/GEOINT), de sinais (SIGINT), de interpretação de assinaturas (*measures & signals intelligence* – MASINT), humana (HUMINT) e de fontes abertas (*open source intelligence* – OSINT).

O caso brasileiro: as áreas de inteligência e defesa na agenda política

De uma forma geral, as áreas de Inteligência de Estado e de defesa nacional no Brasil, desde a Constituição de 1988, não estiveram entre as prioridades na agenda política. Contribuem para tal quadro o histórico de atuação do extinto Serviço Nacional de Informações (SNI), criado na Ditadura Militar brasileira (1964-1985), e a ausência de ameaças interestatais claras, com destaque para o fim das tensões entre Brasil e Argentina na década de 80.

A relativa baixa capacidade estatal do país, em termos de políticas públicas,[10] observada entre o final da década de 90 e o início dos anos 2000 também pode ser apontada como um fator importante para se compreender o delineamento das estruturas de inteligência e de defesa ocorridas nesse período (CEPIK, 2005). Afinal, após se arrastarem na agenda política praticamente por toda a década de 90, somente em 1999 esses dois campos fundamentais para a segurança

8 "*Technological change shapes and reshapes both the threats to a state as well as the opportunities available to it in the international arena, and thus it plays a role in determining the targets of intelligence and the means that intelligence employs*."

9 Entendidos como "*the collective authorities, resources, personnel, and tasks that a nation allocates to using secret means against real and potential opponents*" (WARNER, 2012, p. 135).

10 Compreendidas neste trabalho tanto como diretrizes estruturantes, de nível estratégico, quanto diretrizes de nível intermediário e operacional (SECCHI, 2013, p. 2-10).

da sociedade e do Estado receberam novo impulso. Assim, foi sancionada a Lei Complementar nº 97, de 9 de junho de 1999, criando o Ministério da Defesa e estabelecendo a direção superior das Forças Armadas ao seu ministro. Poucos meses depois, a Lei nº 9.883, de 7 de dezembro de 1999, instituiu o Sistema Brasileiro de Inteligência (SISBIN) e criou seu órgão central, a Agência Brasileira de Inteligência (ABIN). Ambos os campos, a partir de então, foram institucional e paulatinamente amadurecidos, embora carecessem de direcionamentos políticos mais claros.

Defesa: a primeira END e a emergência dos "projetos estratégicos"

Sem dúvida o principal marco do debate sobre defesa nacional após a Constituição de 1988 ocorreu no contexto do lançamento, em 2008, da primeira Estratégia Nacional de Defesa (END).[11] Esse documento foi elaborado focando em ações de médio e longo prazos, com o objetivo de modernizar toda a estrutura nacional de defesa. Para tanto, foram estruturados três eixos: (1) reorganização das Forças Armadas, (2) reestruturação da indústria de defesa e (3) composição dos efetivos das Forças Armadas e, consequentemente, a definição do futuro do serviço militar obrigatório. Ademais, foram selecionados três setores decisivos para a defesa nacional: o cibernético, o espacial e o nuclear. A primeira END abriu caminho para um debate público substancial sobre a modernização das Forças Armadas e, sobretudo, para o aperfeiçoamento institucional do Ministério da Defesa. A Lei Complementar nº 136, de 25 de agosto de 2010, por exemplo, entre outras medidas, fortaleceu a figura do ministro da Defesa e criou o Estado-Maior Conjunto das Forças Armadas (EMCFA). Além disso, em 2012 ocorreu a atualização da Política Nacional de Defesa (PND) e da END, assim como o lançamento do primeiro Livro Branco de Defesa Nacional (LBDN), o qual definiu, em seu anexo II, o Plano de Articulação e Equipamento de Defesa (PAED) (BRASIL, 2012, p. 246-253).

O PAED reuniu basicamente todas as principais demandas por produtos de defesa (bens e serviços) das três Forças Singulares (Marinha, Exército e Aeronáutica), originando um conjunto ambicioso de projetos considerados estratégicos para o país. Entre eles, encontravam-se grandes "sistemas de sistemas", isto é, complexos e bilionários projetos articulando diferentes equipamentos (ex. radares e torres de comunicação) e plataformas (ex. aeronaves, veículos e embarcações). Esses grandes projetos foram colocados sob a responsabilidade de Forças distintas, como o Sistema de Gerenciamento da Amazônia Azul (SisGAAz – Marinha do Brasil), a Defesa Cibernética (Exército Brasileiro), o Sistema Integrado de Proteção de Estruturas Estratégicas Terrestres (PROTEGER – Exército Brasileiro), o Sistema Integrado de Monitoramento de Fronteiras (SISFRON – Exército Brasileiro) e o Desenvolvimento e Construção de Engenhos Aeroespaciais (Aeronáutica), o qual, por sua vez, abrange a construção de satélites geoestacionários.

[11] Decreto nº 6.703, de 18 de dezembro de 2008.

Certamente, um dos fatores em jogo é a distância entre o debate, no Brasil, sobre políticas públicas voltadas para a indústria de "defesa" e aquelas direcionadas à atividade de inteligência.

Os problemas da abordagem escolhida para a implementação desses "sistemas de sistemas" podem ser sintetizados e separados em dois níveis. Em primeiro lugar, considerando apenas o âmbito da defesa nacional, observa-se que a falta de um tratamento sistêmico e integrado desses projetos complexos contribuiu para a manutenção da duplicação de mobilizações tecnológicas, a falta de clareza no que se refere a priorizações (e, consequentemente, a falta de previsão de liberação de recursos no longo prazo) e a persistência de dificuldades no que tange à interoperabilidade entre as três Forças. Não por acaso, atualmente, o SisGAAz se encontra suspenso, o PROTEGER permanece aguardando maiores definições e o SISFRON teve seus prazos estendidos significativamente.[12] Desse modo, em vez de, por exemplo, esses projetos terem sido concebidos desde o início como uma "capacidade militar" integrada, situada no nível interforças (ex. *Intelligence, Surveillance, Reconnaissance, Electronic warfare, Space & Cyber*), o que há de fato são estruturas descentralizadas de ciclos de vida e de gestão de projetos em cada uma das Forças, com claros impactos no que se refere à gestão e à interoperabilidade.

Em segundo lugar, focando o aspecto da dinâmica interagências e compreendendo mais especificamente as áreas de inteligência, defesa e segurança pública, essa mesma fragmentação de concepção e implementação desses "sistemas de sistemas" também pode significar perdas de oportunidades para a otimização de esforços (e recursos). O SISFRON, por exemplo, pode se configurar em um importante instrumento de inteligência não só para o Exército Brasileiro, mas também para órgãos e agências, como a Polícia Federal, a Receita Federal e a própria ABIN, contra, por exemplo, os desdobramentos do crime organizado transnacional ao longo das fronteiras brasileiras. Já o PROTEGER pode se tornar um relevante aliado ao Sistema de Proteção ao Programa Nuclear Brasileiro (SIPRON).[13] Para tanto, as diferentes necessidades dos diversos órgãos e agências devem ser levados em conta, desde o começo, na própria concepção desses projetos, a fim de explorar possibilidades tecnológicas e de contribuir para o fortalecimento da cultura de cooperação e integração interagências.

Assim, apesar de as Forças Armadas exercerem uma forte participação no SISBIN (podendo, portanto, compartilhar dados e informações coletados por variados meios, incluindo a Defesa Cibernética do Exército ou, futuramente, por exemplo, o SisGAAz da Marinha), não há como deixar de questionar os possíveis benefícios caso esses grandes projetos tivessem sido coadunados, desde o início, para obter diversos dados e informações de inteligência de forma mais integrada

12 Mais detalhes em Silva (2015 e 2016).

13 Instituído, na forma atual, pela Lei nº 12.731, de 21 de novembro de 2012.

e compartilhada. Tal abordagem representaria, sem dúvida, um importante reforço das capacidades, por exemplo, de GEOINT, SIGINT e MASINT existentes no SISBIN.

Certamente, um dos fatores em jogo é a distância entre o debate, no Brasil, sobre políticas públicas voltadas para a indústria de "defesa" e aquelas direcionadas à atividade de inteligência. Sob um exame mais atento, observa-se que há um conjunto de empresas capazes de atender demandas não só de "defesa", mas também de inteligência e de segurança pública, perpassando inclusive outras políticas públicas, como as voltadas para as relações exteriores (ex. exportação de produtos de defesa); o desenvolvimento industrial (ex. geração de empregos); a Ciência, Tecnologia e Inovação (CT&I); a segurança pública (ex. armamentos e sistemas de comunicações) e a inteligência (ex. aplicações em SIGINT, MASINT e GEOINT).

No contexto desse distanciamento, é simbólico que a área de defesa nacional tenha sido contemplada com um Regime Especial Tributário para a Indústria de Defesa (RETID),[14] embora desafios similares em relação a licitações sejam também constatados na área de inteligência (ex. buscar preenchimento das necessidades, com qualidade, menor preço/melhor técnica e observando a promoção do desenvolvimento nacional):

> "Se eu for comprar um sistema de segurança para a Abin e tiver de publicar um edital, no dia em que ele for divulgado eu perco a segurança. Se eu tiver de comprar um software ou um hardware, é a mesma situação: há pessoas que vão saber. Quando construímos um centro de inteligência para os Jogos Pan-Americanos de 2007, tivemos de licitar a construção. O cara que se interessa pela licitação tem de saber qual é planta, qual é a metragem, o que vai funcionar em cada área. Isso tudo vai para a licitação." (Depoimento atribuído ao diretor-geral da ABIN, Wilson Trezza, em reportagem de Peduzzi, 2015, da Agência Brasil - EBC).

Inteligência: desafios e perspectivas após a Política Nacional de Inteligência

É possível afirmar que, ao contrário, por exemplo, da área de defesa nacional, a inteligência de Estado não ganhou mais espaço na agenda política brasileira. Essa leitura pode ser reforçada por, resumidamente, duas observações. Primeiro, o fato de que, enquanto a defesa nacional, por exemplo, foi beneficiada com importantes incrementos institucionais nos últimos dez anos (ex. PDN de 2005,[15] PNID de 2005,[16] END de 2008, criação do EMCFA,[17] RETID,[18] e PND, END e LBDN de 2012), observa-se que a área de inteligência somente obteve um arcabouço mais claro

[14] Lei nº 12.598, de 21 de março de 2012, a qual estabelece "normas especiais para as compras, as contratações e o desenvolvimento de produtos e de sistemas de defesa e dispõe sobre regras de incentivo à área estratégica de defesa".

[15] Política de Defesa Nacional - Decreto nº 5.484, de 30 de junho de 2005.

[16] Política Nacional da Indústria de Defesa – Portaria Normativa nº 899/MD, de 19 de julho de 2005.

[17] Lei Complementar nº 136, de 25 de agosto de 2010.

[18] Lei nº 12.598, de 21 de março de 2012.

de atuação no período 2013-2016 (ex. Regimento Interno da Comissão Mista de Controle das Atividades de Inteligência,[19] "Lei Antiterrorismo"[20] e Política Nacional de Inteligência[21]).

O acelerado desenvolvimento tecnológico em escala global observado nas últimas décadas, em especial no que tange às Tecnologias de Comunicação e Informação (TICs), não só abre mais possibilidades e oportunidades para a atividade de inteligência, como também amplia riscos e cria novas vulnerabilidades e ameaças.

Em segundo lugar, mesmo quando a polêmica mundial envolvendo vazamentos promovidos por Edward Snowden alcançou, em 2013, a presidente Dilma Rousseff e a Petrobras, configurando-se um quadro propício para o fortalecimento da atividade de inteligência no Brasil, observa-se que as atenções foram concentradas, por exemplo, na implementação do Centro de Defesa Cibernética do Exército Brasileiro (CDCiber) (MORAES, 2013) e no pedido do Ministério das Comunicações para que os Correios desenvolvessem um sistema de e-mail nacional no "intuito" de tornar mais difícil a espionagem e o acesso a dados de comunicação eletrônica de brasileiros (G1, 2013).

De toda forma, o rol amplo e complexo de ameaças priorizadas pela Política Nacional de Inteligência (PNI) (ex. espionagem, sabotagem, interferência externa, ataques cibernéticos, terrorismo, ADMs[22] e criminalidade organizada) indica a necessidade de investimentos em estruturas, equipamentos e recursos humanos, com objetivo de ao menos buscar acompanhar o rápido passo do desenvolvimento tecnológico mundial, o qual possibilita, por exemplo, um vasto leque de opções (ex. difusão de meios de comunicações criptografados) para aqueles indivíduos e organizações, no Brasil e no exterior, que almejem ocultar ou mascarar ações adversas (ex. espionagem e terrorismo). Para tanto, torna-se fundamental o debate democrático, amplo e plural sobre a questão abrangendo a viabilidade de expansão da capacidade da Inteligência brasileira em áreas como SIGINT e MASINT, com, obviamente, a inserção, no ordenamento jurídico nacional, dos devidos instrumentos de amparo às suas atividades.

Considerações finais

O acelerado desenvolvimento tecnológico em escala global observado nas últimas décadas, em especial no que tange às Tecnologias de Comunicação e Informação (TICs), não só abre mais possibilidades e oportunidades para a atividade de inteligência, como também amplia riscos e cria novas vulnerabilidades e ameaças.

[19] Resolução nº 2, de 2013-CN.

[20] Lei nº 13.260, de 16 de março de 2016.

[21] Decreto nº 8.793, de 29 de junho de 2016.

[22] Armas de Destruição em Massa (ex. química, biológicas e nucleares).

Nesse quadro, é possível vislumbrar vantagens de uma maior intersetorialidade entre políticas públicas delineadas para a inteligência de Estado e para a indústria de defesa brasileira. Tal movimento pode compreender uma aproximação institucional, por exemplo, entre iniciativas como o Programa Nacional de Proteção do Conhecimento Sensível (PNPC) e indústrias de defesa contempladas por auxílios da Agência Brasileira de Promoção de Exportações e Investimentos (Apex-Brasil) para participarem de exposições no exterior. No mesmo contexto, grandes projetos gestados no âmbito do Ministério da Defesa poderiam contemplar, desde o início, funcionalidades pensadas para a obtenção e o compartilhamento de determinados dados e informações, visando a atender a necessidades de inteligência de forma mais integrada.

Assim, é possível afirmar que um dos legados significativos das experiências com os Grandes Eventos, como a Copa do Mundo 2014 e as Olimpíadas 2016, é justamente o fortalecimento de uma cultura de cooperação e integração interagências, por meio de iniciativas como o Plano Estratégico de Segurança Integrada (PESI) e a criação do Comitê Integrado de Enfrentamento ao Terrorismo (CIET), os quais, certamente, apontarão demandas por novos equipamentos, protocolos e soluções tecnológicas.[23] Afinal, um efetivo aparato de inteligência de Estado depende dos contínuos esforços de se adaptar aos desafios e às oportunidades proporcionados pelo desenvolvimento tecnológico global.

[23] Com o objetivo de enfrentar possibilidades de atentados terroristas nas Olimpíadas 2016 realizadas no Brasil, por exemplo, a Polícia Federal e a Secretaria Extraordinária de Segurança para Grandes Eventos (SESGE) disponibilizaram para funcionários de hotéis, restaurantes, entre outros, um aplicativo para celulares denominado "Vigia", possibilitando ao usuário relatar de forma georreferenciada suspeitas, assim como enviar fotos às autoridades competentes (PUFF, 2016).

Referências

BAMFORD, James. *The Shadow factory*. The Anchor books: NY, 2008.

BOYLE, Danny. Strangeways prison smugglers crash drone delivering drugs and mobile phones. *The Telegraph*, 09/11/2015. Disponível em: <http://www.telegraph.co.uk/news/uknews/law-and-order/11983257/Strangeways-prison-smugglers-crash-drone-at-HMP-Manchester.html>. Acesso em: 15 jul. 2016.

BRASIL. Ministério da Defesa. *Livro Branco de Defesa Nacional*. Brasília-DF, 2012. Disponível em: <www.defesa.gov.br/arquivos/2012/mes07/lbdn.pdf>. Acesso em: 18/02/2016.

CEPIK, Marco. Regime político e sistema de Inteligência no Brasil: legitimidade e efetividade como desafios institucionais. *Dados – Revista de Ciências Sociais, v. 48, n. 1, Rio de Janeiro, p. 67-113*, 2005.

ENTOUS, Adam; DONATI, Jessica. How the U.S tracked and killed the leader of the Taliban. *The Wall Street Journal*, 25/05/2016. Disponível em: <http://www.wsj.com/articles/u-s-tracked-taliban-leader--before-drone-strike-1464109562>. Acesso em: 15 jul. 2016.

G1. Contra espionagem, governo quer sistema de e-mail nacional. Brasília, 02/09/2013. Disponível em: <http://g1.globo.com/politica/noticia/2013/09/contra-espionagem-governo-quer-sistema-de-e--mail-nacional.html>. Acesso em: 17 jul. 2016.

GALLAGHER, Ryan. Facing data deluge, secret U.K. spying report warned of intelligence failure. *The Intercept*, 07/06/2016. Disponível em: <https://theintercept.com/2016/06/07/mi5-gchq-digint-surveillance-data-deluge/>. Acesso em: 17 jul. 2016.

GORMAN, Siobhan; DREAZEN, Yochi J.; COLE, August. Insurgents hack U.S. drones. *The Wall Street Journal*, 17/12/2009. Disponível em: <http://www.wsj.com/articles/SB126102247889095011>. Acesso em: 15 jul. 2016.

GREENWALD, Glenn; POITRAS, Laura; MACASKILL, Ewen. NSA shares raw intelligence including Americans' data with Israel. *The Guardian*, 11/09/2013. Disponível em: <https://www.theguardian.com/world/2013/sep/11/nsa-americans-personal-data-israel-documents>. Acesso em: 15 jul. 2016.

LANDLER, Mark; SAVAGE, Charlie. Obama outlines calibrated curbs on phone spying. *The New York Times*, Politics, 17/01/2014. Disponível em: <http://www.nytimes.com/2014/01/18/us/politics/obama-nsa.html>. Acesso em: 17 jul. 2016.

LEIGH, David. How 250,000 US embassy cables were leaked. *The Guardian*, 28/11/2010. Disponível em: <https://www.theguardian.com/world/2010/nov/28/how-us-embassy-cables-leaked>. Acesso em: 15 jul. 2016.

MAOR, Amir. The app market's Big Data challenge. *Wired*, Partner Content, abril/2013. Disponível em: <http://www.wired.com/insights/2013/04/the-app-markets-big-data-challenge/>. Acesso em: 15 jul. 2016.

MORAES, Maurício. Espionagem abre discussão sobre preparo do Brasil para uma guerra cibernética. *BBC Brasil*, 14/10/2013, São Paulo. Disponível em: <http://www.bbc.com/portuguese/celular/noticias/2013/10/131011_defesa_seguranca_cibernetica_brasil_mm.shtml>. Acesso em: 17 jul. 2016.

MORGAN, Steve. Cibersecurity market reaches $ 75 bilhões in 2015; expected to reach $170 billion by 2020. *Forbes* (Tech), 20/12/2015. Disponível em: <http://www.forbes.com/sites/stevemorgan/2015/12/20/cybersecurity%E2%80%8B-%E2%80%8Bmarket-reaches-75--billion-in-2015%E2%80%8B%E2%80%8B-%E2%80%8Bexpected-to-reach-170-billion--by-2020/#1743201d2191>. Acesso em: 17 jul. 2016.

OGURA, Junko. Arrest after drone with radioactive material lands on Japan PM's rooftop. *CNN*, 25/04/2015. Disponível em: <http://edition.cnn.com/2015/04/24/asia/japan-prime-minister-radioaction-drone-arrest/>. Acesso em: 15 jul. 2016.

PEDUZZI, Pedro. Diretor da Abin pede lei que garanta sigilo da identidade de agentes. *EBC – Agência Brasil*, Geral, Brasília, 05/09/2015. Disponível em: <http://agenciabrasil.ebc.com.br/geral/noticia/2015-09/abin-defende-mudancas-na-lei-que-garantam-preservacao-da-identidade-de-agentes>. Acesso em: 17 jul. 2016.

PUFF, Jefferson. Como aplicativo ajudará a evitar ataques terroristas na Rio 2016. BBC, 18 de junho de 2016. Disponível em: <http://www.bbc.com/portuguese/brasil-36812614>. Acesso em: 18 jul. 2016.

SECCHI, Leonardo. *Políticas públicas*. Trilha/Cengage Learning, 2ª edição, 2013.

SILVA, Peterson F. da. *A política industrial de defesa no Brasil* (1999-2014): intersetorialidade e dinâmica de seus principais atores. 2015. Tese (Doutorado em Relações Internacionais) – Instituto de Relações Internacionais, Universidade de São Paulo, São Paulo, 2015. Disponível em: <http://www.teses.usp.br/teses/disponiveis/101/101131/tde-15092015-113930/>. Acesso em: 17 jul. 2016.

_____. Política Industrial de Defesa brasileira em tempos de crise: os principais desafios para o PAED 2016. *Mundorama - Revista de Divulgação Científica em Relações Internacionais*. Disponível em: <http://www.mundorama.net/2016/03/17/politica-industrial-de-defesa-brasileira-em-tempos-de-crise--os-principais-desafios-para-o-paed-2016-por-peterson-silva/>. Acesso em: 17 jul. 2016.

SIMCOX, Robin. French Intelligence reform - the counterterrorism commission won't prevent the next attack. *Foreign Affairs*, 17/07/2016. Disponível em: <https://www.foreignaffairs.com/articles/france/2016-07-17/french-intelligence-reform>. Acesso em: 17 jul. 2016.

SINGER, Natasha. Why a push for online privacy is bogged down in Washington. *The New York Times*, Technology, 28/02/2016. Disponível em: <http://www.nytimes.com/2016/02/29/technology/obamas--effort-on-consumer-privacy-falls-short-critics-say.html?_r=0>. Acesso em: 15 jul. 2016.

STEIN, Jeff. CIA's secret fear: high-tech border checks will blow spies' cover. *Wired*, Security, 04/12/2012. Disponível em: <https://www.wired.com/2012/04/cia-spies-biometric-tech/>. Acesso em: 17 jul. 2016.

STERNSTEIN, Aliya. Pentagon wants to automate social-media checks on clearance holders. *Defense One*, 20/07/2016. Disponível em: <http://www.defenseone.com/technology/2016/07/pentagon--wants-automate-social-media-checks-clearance-holders/130062/?oref=site-defenseone-flyin-sail-thru>. Acesso em: 21 jul. 2016.

TUCKER, Patrick. DHS: Drug Traffickers are spoofing border drones. *Defense One*, 17/12/2015. Disponível em: <http://www.defenseone.com/technology/2015/12/DHS-Drug-Traffickers-Spoofing-Border-Drones/124613/>. Acesso em: 15 jul. 2016.

VASCONCELOS, Yuri. Um satélite brasileiro – Amazônia 1 desenvolvido no país vai monitorar recursos naturais e ajudar no combate ao desmatamento. *Revista Pesquisa FAPESP*, Ed.239, Jan. 2016. Disponível em: <http://revistapesquisa.fapesp.br/2016/01/12/um-satelite-brasileiro/>. Acesso em: 15 jul. 2016.

WARNER, Michael. Reflections on Technology and Intelligence Systems. *Intelligence and National Security*, v 27, n. 1, p. 133-153, 2012.

WIRTZ, James J.; ROSENWASSER, Jon J. From combined arms to combined intelligence: philosophy, doctrine and operations. *Intelligence and National Security*, v. 25, n. 6, p. 725-743, 2010.

YADRON, Danny. FBI confirms it won't tell Apple how it hacked San Bernardino shooter's iPhone. *The Guardian*, 28/04/2016. Disponível em: <https://www.theguardian.com/technology/2016/apr/27/fbi--apple-iphone-secret-hack-san-bernardino>. Acesso em: 17 jul. 2016.