11 de Setembro de 2001: as falhas da inteligência americana e as lições aprendidas para a inteligência brasileira

Cel Inf QEMA Roberto Pereira Angrizani*

Introdução

Na história da humanidade, a sociedade jamais havia testemunhado um período com transformação tão intensa e veloz como a ocorrida a partir da última década do século XX. Pode-se afirmar que o mundo hoje é mais complexo. Na verdade, vive-se em um mundo VUCA – *Volatile, Uncertain, Complex e Ambiguous*. Em português, VICA – Volátil, Incerto, Complexo e Ambíguo. Estudiosos afirmam, na verdade, que o mundo VUCA evoluiu para o atual mundo BANI – *Brittle, Anxious, Nonlinear and Incomprehensible*, ou, em português, FANI – Frágil, Ansioso, Não linear e Incompreensível. E o Estado, diante desse ambiente, enfrenta desafios enormes.

Em virtude da revolução da informação, um dos grandes desafios que se apresenta é o gerenciamento do enorme volume de informações disponíveis ao Estado. Dessa forma, o Estado deve ser capaz de processar, analisar e transformar as informações disponíveis em conhecimento para que seja útil no processo de tomada de decisão. Assim, faz-se necessário produzir inteligência.

Em que pese seu destacado e positivo desempenho ao longo da história, em muitas ocasiões a inteligência também assumiu o papel de vilã. Tem sido uma constante histórica responsabilizar aqueles que trabalham na inteligência sempre que houve falhas nos processos decisórios, em todos os níveis, ocasionando eventos catastróficos ou de comoção mundial. Na história recente, entretanto, nenhum fato teve maior repercussão e foi alvo de tantos estudos e análises quanto os atentados terroristas de 11 de setembro de 2001, nos Estados Unidos da América (EUA), perpetrados pela rede terrorista Al Qaeda.

Os atentados terroristas de 11 de setembro de 2001, que, por sua notoriedade, dispensam maiores esclarecimentos, constituíram-se em um evento disruptivo que impactou o Sistema Internacional (SI). A surpresa obtida pelos terroristas deixou perplexa toda a sociedade norte-americana e global.

Após o choque inicial, em 12 de setembro, o mundo se perguntava: o que aconteceu? Como e por que aconteceu? Quem eram os autores dos ataques? Qual o objetivo? Era possível prevenir e evitar os ataques? Quem deveria ter agido e não o fez? Por último, e não menos importante, por que a inteligência norte-americana falhou em proteger os cidadãos do país?

Como é da cultura organizacional das instituições norte-americanas, intensa investigação foi conduzida no sentido de identificar as possíveis falhas da inteligência do país. O Comitê de Inteligência do Senado e o Comitê Permanente de Inteligência da Câmara dos Representantes foram os primeiros a instituir uma comissão de investigação para analisar as causas que conduziram aos ataques de 2001.

Ao final, relatórios apontaram falhas das agências de segurança e inteligência, particularmente organizacionais, culturais, sistêmicas, além de falhas humanas. Desde então, os EUA têm buscado aperfeiçoar seu sistema de inteligência na prevenção de acidentes daquela natureza e de ações de outras ameaças à segurança nacional.

E o Brasil? Estaria nosso SISBIN preparado para evitar que ameaças à segurança nacional tenham sucesso em seus objetivos? Assim, é extremamente relevante identificar as falhas da inteligência norte-americana e analisar quais dessas falhas podem se constituir em lições aprendidas para o SISBIN,

* Cel Inf QEMA (AMAN/1996, EsAO/2004, ECEME/2014). Possui o Curso Avançado de Inteligência para Oficiais e integrou o Centro de Inteligência do Exército. Atualmente, serve no Comando Militar da Amazônia.

aperfeiçoando o sistema e a atuação da inteligência brasileira.

Dessa forma, este trabalho buscou, em geral, analisar a atuação da inteligência dos EUA nos atentados terroristas de 2001, destacando as falhas ocorridas e elencando possíveis lições aprendidas para a inteligência brasileira. Para atingir o objetivo maior da pesquisa, buscou-se caracterizar o Sistema de Inteligência Norte-Americano e o SISBIN. Como *core* do trabalho de pesquisa, foram apontadas as principais falhas da comunidade de inteligência norte-americana e apresentadas as lições aprendidas para o SISBIN.

A comunidade de inteligência dos Estados Unidos da América e o Sistema Brasileiro de Inteligência

Os EUA têm conduzido atividades de inteligência desde sua guerra de independência em 1775. Há relatos de que o líder da revolução, George Washington, que viria a ser o primeiro presidente do país, era um entusiasta da atividade e recrutou agentes de inteligência durante o conflito com os ingleses (FEDERATION, 1996).

Somente após a Segunda Guerra Mundial, entretanto, quando o então presidente Harry Truman promulgou a Lei de Segurança Nacional de 1947, que reformulou toda a estrutura de defesa do país, foi organizado, pela primeira vez, o Sistema de Inteligência dos EUA, conhecido por Comunidade de Inteligência. Foi criada a Central Intelligence Agency (CIA, sigla em inglês), responsável por coordenar as atividades de inteligência do país, relacionar, avaliar e disseminar todos os tipos de dados que poderiam ser críticos para a segurança americana. A CIA passou a ser o órgão central da comunidade de inteligência dos EUA, e o diretor central de inteligência, chefe da agência, foi designado como o coordenador da atividade de inteligência do país (BADER, 2019).

Desde sua criação, a CIA enfrentou uma série de obstáculos para exercer a função de órgão central da comunidade de inteligência. Não havia uma hierarquização, e a integração e o compartilhamento das informações entre as agências situavam-se no nível da cooperação, e não da subordinação ou da obrigatoriedade. A comunidade era, a bem da verdade, um conglomerado de agências, atuando isoladamente, sem uma autoridade central que pudesse agir como orientadora do processo e integradora do conhecimento produzido. Contribuindo para agravar o quadro, havia grande rivalidade entre a agência e os serviços de inteligência das Forças Armadas e o FBI.

Esse era o panorama da comunidade de inteligência norte-americana por ocasião dos atentados terroristas de 2001, que tornaram públicas as deficiências do sistema. Como consequência dos aten tados e após minuciosa análise das causas que motivaram as falhas da inteligência, em 17 de dezembro de 2004, o presidente George W. Bush assinou a Lei de Reforma da Inteligência e Prevenção do Terrorismo, que reestruturou a comunidade de inteligência (BADER, 2019).

A Lei de Reforma da Inteligência extinguiu o cargo de diretor central de inteligência. Entretanto, buscando fortalecer a centralização da comunidade de inteligência e facilitar a integração entre as agências, foi criado o Escritório do Diretor de Inteligência Nacional (ODNI, sigla em inglês), órgão central do sistema de inteligência norte-americano. Segundo Bader (2019), o diretor de inteligência nacional é o chefe da comunidade de inteligência, supervisionando e dirigindo a implementação do programa nacional de inteligência, ao mesmo tempo em que atua como principal conselheiro do presidente e do conselho de segurança nacional.

O diretor de inteligência nacional é, ainda, o responsável por delinear a estratégia de inteligência nacional, com base na estratégia de segurança nacional e que fornece à comunidade de inteligência a direção estratégica para um período de quatro anos (OFFICE, 2019). Observa-se, assim, que o outrora ambiente descentralizado e dependente da iniciativa das agências para a integração, colaboração e compartilhamento de informações agora se constitui em uma estrutura mais hierarquizada, com menos liberdade de ação para as agências e com um órgão central com claras e definidas responsabilidades.

De acordo com Office (2022), atualmente, a comunidade de inteligência dos EUA compreende 18 organizações e agências do poder executivo. O ODNI e a CIA são consideradas agências independentes e respondem somente ao presidente da República e ao Conselho de Segurança Nacional e aos mecanismos de controle externo do Congresso Nacional.

No Brasil, as origens da atividade de inteligência remontam a 1927, com a criação do Conselho de Defesa Nacional, órgão de assessoramento do Poder Executivo (BADER, 2019). Desde então, a atividade tem evoluído e acompanhado o cenário nacional, sem deixar de refletir, entretanto, as grandes questões geopolíticas mundiais. Levando em consideração esse aspecto e a evolução dos diversos órgãos que compõem o SISBIN, a Agência Brasileira de Inteligência (ABIN) – (2020b) propõe uma divisão didática e cronológica das fases da atividade de inteligência no Brasil: fase embrionária (1927-1964); fase da bipolaridade (1964-1985); fase de transição (1985-1999); e fase contemporânea (1999 até os dias atuais).

O SISBIN foi instituído por intermédio da Lei nº 9.883, de 7 de dezembro de 1999. De acordo com a Estratégia Nacional de Inteligência, o SISBIN

> tem por objetivo integrar ações de planejamento e execução das atividades de inteligência no país, com a finalidade de fornecer subsídios ao presidente da República nos assuntos de interesse nacional. (BRASIL, 2017)

Atualmente, o SISBIN é composto por 48 órgãos, englobando agências de diversos ministérios e das Forças Armadas brasileiras.

Os mesmos instrumentos jurídicos que criaram o SISBIN estabeleceram a ABIN como órgão central do sistema, com a "responsabilidade de planejar, executar, coordenar, supervisionar e controlar as atividades de inteligência do país" (BRASIL, 1999, 2002). Recentemente, foi criado o Centro de Inteligência Nacional (CIN), estrutura da ABIN responsável por

> coordenar o fluxo de dados e informações oportunas e de interesse da atividade de inteligência de Estado, com a finalidade de subsidiar a tomada de decisão do presidente da República. (BRASIL, 2002)

A ABIN afirma que as operações conjuntas e a atuação do CIN e dos Centros de Inteligência Regionais (CIR) nos grandes eventos esportivos exemplificam o processo de cooperação entre os órgãos do SISBIN. O CIN e os CIR também são ativados em eventos políticos e sociais de relevância nacional, como posse presidencial, reuniões de cúpula, dentre outros (ABIN, 2020c).

Segundo a ABIN, em âmbito nacional, ocorrem reuniões semestrais em que são estabelecidas diretrizes e necessidades gerais de conhecimento de inteligência. Ademais, reuniões periódicas acontecem para tratar de temas específicos, quando são compartilhados conhecimentos, analisam-se conjuntamente cenários e se estabelecem necessidades pontuais de informações para a produção de relatórios. Reuniões semelhantes ocorrem, também, em âmbito estadual (ABIN, 2020a).

As falhas da inteligência dos Estados Unidos da América nos atentados terroristas de 11 de setembro de 2001

A fim de investigar os fatos ocorridos em 2001, foi estabelecida uma comissão conjunta composta pelo Comitê de Inteligência do Senado e pelo Comitê Permanente de Inteligência da Câmara dos Representantes. Em dezembro de 2002, a comissão conjunta apresentou o relatório final das investigações, o *Joint Inquiry into Intelligence Community Activities before and after the Terrorist Attacks of September 11, 2001 (the House Permanent Select Committee on Inteligence and the Senate Select Committee on Intelligence, 2002).*

Além da comissão conjunta, o então presidente George Bush determinou, em novembro de 2002, a criação da Comissão Nacional de Inquérito sobre Ataques Terroristas contra os Estados Unidos, composta por 10 congressistas norte-americanos. A comissão, conhecida por *9/11 Commission*, apresentou o relatório final em julho de 2004 (NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES, 2004).

Sobre as comissões relatadas, ainda que afirmassem estar realizando um trabalho independente, pode-se inferir que, muito provavelmente, sofreram influência do componente político. Dessa forma, as falhas da comunidade de inteligência que serão apresentadas a seguir são uma compilação dos principais pontos abordados nos relatórios das duas comissões oficiais, mas também de relatos, artigos e críticas de especialistas independentes e membros da comunidade acadêmica.

Deficiência na integração entre os órgãos da comunidade de inteligência

Esta é, provavelmente, a principal falha apontada por todos aqueles que analisaram a atuação da inteligência nos ataques terroristas de 2001. Não havia integração entre os órgãos da comunidade de inteligência, agravada pelo fato de não se compartilhar as informações entre os diversos órgãos, gerando uma compartimentação excessiva, também conhecida como *stovepipe system*. Segundo Melvin Goodman, durante o período de janeiro a março de 2000, entre 50 e 60 analistas e agentes da comunidade de inteligência obtiveram acesso às informações da presença de jihadistas da Al Qaeda em território norte-americano, mas não compartilharam nenhuma informação (GOODMAN, 2008).

O diretor central de inteligência e a CIA, órgão central da comunidade, não tinham força política para exercer o papel de coordenadores da política nacional de inteligência. Ademais, cada instituição possuía uma cultura organizacional fortemente arraigada, além da existência de rivalidades pueris, especialmente entre a CIA, o FBI e os órgãos das Forças Armadas. Além do compartilhamento dentro da comunidade de inteligência, também houve falhas em compartilhar informações com outros serviços do governo federal e mesmo órgãos de segurança pública.

Cabe destacar, ainda, que, mesmo internamente, nas agências da comunidade, não ocorria o compartilhamento de informações essenciais que poderiam ter evitado os atentados, sempre sob o escudo dos princípios da compartimentação das informações e da necessidade de conhecer (RAMÍREZ, 2010; THE HOUSE, 2002). Amy Zegart afirma que a CIA apresentava uma crença excessiva na importância da segurança, resumida pela frase *need to know* (necessidade de conhecer), que, segundo a escritora, opunha-se ao princípio *need to share* (necessidade de compartilhar) – (ZEGART, 2005).

Problemas de organização e coordenação dentro da comunidade de inteligência

Em que pese a CIA e o FBI possuírem grande volume de informações sobre a possibilidade de ataques terroristas, os órgãos não foram capazes de analisar essas informações e prover assessoramento oportuno aos decisores. Ambos falharam em realizar o acompanhamento de terroristas que, sabidamente, já se encontravam nos EUA e realizavam atividades suspeitas. Por outro lado, como não havia coordenação dentro da comunidade de inteligência, os aspectos a conhecer não eram compartilhados, o que contribuiria para a diminuição das lacunas de informação existentes (RAMÍREZ, 2010; THE HOUSE, 2002).

Limitações do papel do diretor central de inteligência

O diretor central de inteligência, George Tenet, não possuía todas as ferramentas para exercer o papel de coordenador da atividade de inteligência no país. Não havia uma hierarquização, e a integração e o compartilhamento das informações entre as agências situavam-se no nível da cooperação, e não da subordinação ou obrigatoriedade. A situação foi agravada pela não existência de uma estratégia abrangente de contraterrorismo que pudesse envolver toda a comunidade de inteligência (RAMÍREZ, 2010; THE HOUSE, 2002).

Falhas da cultura organizacional da comunidade de inteligência

Especialistas e acadêmicos discordaram dos relatórios oficiais, que, segundo eles, buscaram isentar as instituições e focaram mais em falhas humanas dos profissionais de inteligência. Para os estudiosos, a principal causa das falhas identificadas no 11 de

Setembro repousam na cultura organizacional da comunidade de inteligência. Zegart (2005) sustenta que as falhas ocorreram devido à natureza burocrática das organizações e à aversão às mudanças. A autora afirma que oficiais de inteligência e políticos sabiam da gravidade da ameaça terrorista da Al Qaeda, e entenderam que mudanças organizacionais tinham que ser feitas para conter a ameaça, mas não o fizeram. Bruce Berkowitz, ex-analista da CIA, ressalta que a falha da inteligência no 11 de Setembro resultou da falta de agilidade organizacional da comunidade, ainda presa a procedimentos do período da Guerra Fria, lenta e inflexível para enfrentar novas ameaças (BERKOWITZ, 2003).

Falhas na política contraterrorista

O governo dos EUA subestimou a ameaça terrorista, e a comunidade de inteligência não deu a devida importância ou prioridade à Al Qaeda. Segundo Johnson (2006), devido à falta de comunicação entre o nível político e as agências de inteligência, não foram definidas as necessidades de inteligência para a comunidade e, sem objetivos claramente definidos, os analistas não focaram na ameaça terrorista. Johnson critica, ainda, a postura dos governantes, que não deram a devida atenção às análises de inteligência, ainda que estas demandassem recursos financeiros vultosos.

Capacidades insuficientes para lidar com a ameaça terrorista

Segundo a *National Comission* (2004), a comunidade de inteligência norte-americana buscou conter a ameaça terrorista empregando as mesmas capacidades, doutrina, *modus operandi* e meios da Guerra Fria. A CIA não possuía as capacidades necessárias para realizar ações encobertas contra Bin Laden, ao mesmo tempo em que não havia vontade política para fazê-las, tendo em vista questões legais envolvendo agentes do órgão no passado. Para a chefia da CIA, as ações diretas deveriam ser realizadas pelas Forças Armadas. Os militares, no entanto, acreditavam que o uso de bombardeiros e mísseis não estava sendo eficiente para eliminar a ameaça terrorista.

Falhas de inteligência humana (HUMINT)

A HUMINT foi relegada a segundo plano no acompanhamento da atividade terrorista. Em que pese a dificuldade de infiltração de agentes norte-americanos nas organizações terroristas, observou-se que não ocorreu recrutamento de colaboradores com afinidades religiosas e culturais que facilitariam a obtenção de informações confiáveis. Da mesma forma, concluiu-se que os EUA estavam excessivamente dependentes das informações fornecidas pelos serviços de inteligência estrangeiros, nem sempre confiáveis (RAMÍREZ, 2010; THE HOUSE, 2002). Ademais, a partir da revolução da informação, as fontes tecnológicas passaram a ter prioridade na comunidade de inteligência (CILLUFFO, 2002). Como resultado, a prioridade nacional para a coleta de informações passou para satélites e outros meios de coleta eletrônica, longe da inteligência tradicional baseada em agentes humanos (CARAFANO, 2004).

Uso ineficiente da enorme apacidade tecnológica americana para o combate terrorista

A indiscutível capacidade tecnológica dos EUA não foi capaz de superar a falta de compartilhamento de informações entre as agências, particularmente entre o FBI e a NSA. Ademais, não havia um banco de dados centralizado sobre o terrorismo. Verificou-se, ainda, que as agências operavam sistemas obsoletos e insuficientes para gerenciar seus bancos de dados. A NSA, responsável pela inteligência de sinais (SIGINT), pouco contribuiu para detectar as conexões entre os terroristas e prover alerta oportuno do ataque. Além disso, a agência apresentou deficiências na busca e coleta de informações empregando alta tecnologia de forma excessivamente cautelosa (RAMÍREZ, 2010; THE HOUSE, 2002).

Análise estratégica deficiente

As análises estratégicas produzidas pela comunidade de inteligência eram deficientes, pouco criativas e incapazes de integrar os conhecimentos e formular quadros abrangentes da ameaça terrorista. Por conseguinte, as análises não permitiram o asses-

soramento preciso aos decisores no nível político. Constatou-se que a inexperiência, a incompetência e a falta de treinamento dos analistas e a falta de acesso às informações críticas foram os principais fatores que contribuíram para uma análise deficiente (RAMÍREZ, 2010; THE HOUSE, 2002).

Falhas na execução das medidas defensivas antiterroristas

A comunidade de inteligência possuía, desde 1998, conhecimento de que a Al Qaeda tinha a intenção e planejava realizar um ataque terrorista em território norte-americano. Apesar disso, não foram planejadas ou executadas quaisquer medidas preventivas ou mesmo ações defensivas no campo do antiterrorismo, objetivando neutralizar a ameaça (RAMÍREZ, 2010; THE HOUSE, 2002). O relatório da comissão conjunta do Congresso Nacional concluiu, ainda, que, mesmo sabendo da possibilidade de ocorrer um ataque em solo norte-americano, o governo e a comunidade de inteligência falharam em não alertar, antecipadamente, a população norte-americana sobre a realidade e a gravidade da ameaça, o que poderia ter aumentado o estado de alerta e evitado os atentados (THE HOUSE, 2002).

Deficiências no uso de serviços de inteligência de outros países

Havia uma excessiva dependência da comunidade de inteligência norte-americana em relação aos órgãos de inteligência de outros países, especialmente para a coleta de informações e condução de outras atividades contraterroristas. Esses órgãos, no entanto, apresentaram capacidades muito heterogêneas, entregando produtos com diferentes níveis de confiabilidade, o que contribuiu para a existência de lacunas na consciência situacional da comunidade dos EUA. O relatório do Congresso Nacional apontou, ainda, falhas da comunidade de inteligência e do governo em coordenar os esforços com outros países (THE HOUSE, 2002).

Falta de rastreamento das atividades financeiras das organizações terroristas

Em que pese ser de conhecimento da comunidade de inteligência que as organizações terroristas eram altamente dependentes de financiamento externo, não havia, nos EUA, estrutura voltada para o rastreamento dos recursos destinados aos sequestradores já baseados em território norte-americano. Ademais,

> não havia coordenação entre agências governamentais para rastrear os fundos dos terroristas e cortar suas redes de apoio financeiro. Isso teria ajudado a interromper e desorganizar o planejamento dos atentados. (RAMÍREZ, 2010)

O paradigma de inteligência de Sherman Kent

Sherman Kent é considerado o pai da análise de inteligência, e suas teorias e métodos orientaram os trabalhos da comunidade de inteligência dos EUA por décadas. Resumidamente, sua metodologia baseava-se nos princípios positivistas, em princípios científicos. Para Sherman, os analistas não deviam assumir riscos, deviam basear suas análises apenas em fatos e deveriam manter distância dos decisores políticos. Essas eram as premissas por ocasião dos ataques de 11 de setembro de 2001 (RAMÍREZ, 2010). especialistas acreditam, entretanto, que a aversão ao risco impede a produção de análises criativas, tão necessárias à época dos atentados terroristas, e que o paradigma de Kent não acompanhou a revolução tecnológica e da informação, e pode ter contribuído para análises deficientes em relação à ameaça terrorista (MEDINA, 2002; SCHMITT, 2006).

As lições aprendidas para a inteligência brasileira

Como se pode observar nas análises feitas até o momento, investigações oficiais e estudos independentes identificaram inúmeras falhas cometidas pela comunidade de inteligência norte-americana por ocasião dos atentados terroristas de 11 de setembro de 2001. Entender como essas falhas podem

se constituir em lições aprendidas para o SISBIN é um dos principais objetivos desse trabalho. Cabe ressaltar, entretanto, que tais ensinamentos devem ser analisados considerando a estatura geopolítica do Brasil, assim como as idiossincrasias de suas expressões políticas, econômicas, psicossociais, militares e científico-tecnológicas.

A principal falha apontada por todos aqueles que analisaram a atuação da inteligência dos EUA nos ataques terroristas de 2001 foi a deficiência na integração entre os órgãos da comunidade de inteligência e no compartilhamento de informações, interna e externamente. Observa-se que o SISBIN apresenta deficiências semelhantes à comunidade de inteligência norte-americana à época do 11 de Setembro. Ainda que haja um marco jurídico regulando o sistema e determinando aos diversos órgãos o compartilhamento das informações com o órgão central, a ABIN, observa-se que a estrutura ainda carece de aperfeiçoamento e que não há uma total integração entre os diversos componentes do SISBIN.

A legislação vigente não deixa clara a existência de uma hierarquização dentro do sistema, o que induz concluir que as relações entre as agências se encontrem no nível colaborativo, muitas vezes dependente mais da iniciativa individual do que de uma relação institucional. Colabora para esse fato o enorme número de integrantes do SISBIN, 48 órgãos, que, antes de facilitar a produção do conhecimento, dificulta o estabelecimento de objetivos comuns e de uma relação de confiança entre as instituições.

Ainda em relação ao compartilhamento de informações, pode-se inferir que, no sistema brasileiro, há uma excessiva compartimentação da informação, com base na necessidade de conhecer (*need to know*) em detrimento da necessidade de compartilhar (*need to share*), ocasionando o fenômeno *stovepipe*. Ou seja, há uma cultura organizacional em não compartilhar as informações com outros órgãos ou mesmo internamente, dentro de divisões de uma determinada agência.

Observou-se também que ocorreram problemas de organização e coordenação dentro da comunidade de inteligência dos EUA. Para a inteligência nacional, fica o ensinamento da necessidade de definição clara das responsabilidades de cada órgão do SISBIN no acompanhamento das ameaças. Ademais, destaca-se a importância de dotar os órgãos de inteligência com estruturas de análise com capacidade de produzir assessoramento oportuno e preciso aos decisores de mais alto nível.

Em relação aos órgãos externos à comunidade de inteligência, foi observado que falhas no rastreamento das atividades financeiras das organizações terroristas poderiam ser mitigadas, caso houvesse compartilhamento de informações. Assim, o trabalho de órgãos do governo de monitoramento financeiro de ameaças pode contribuir para o SISBIN na produção de evidências e na atuação preventiva de combate às ameaças.

Outra questão apontada pelas comissões e especialistas foi a falta de coordenação entre o nível político e a comunidade de inteligência. Para a inteligência brasileira, destaca-se o ensinamento da necessidade de perfeita simbiose entre o nível político e o SISBIN. Ressalta-se a importância de documentos de alto nível estabelecendo as diretrizes e as prioridades de inteligência para os integrantes do SISBIN, como a Política Nacional e Estratégia Nacional de Inteligência e, especialmente, o Plano Nacional de Inteligência.

Em relação às fontes de inteligência, observaram-se falhas no emprego da inteligência humana (HUMINT) por parte da comunidade de inteligência. Em que pese o elevado repertório de fontes sendo empregadas atualmente, o SISBIN deve entender que a HUMINT é a espinha dorsal de qualquer organismo de inteligência. Dessa forma, destacam-se a necessidade de haver uma seleção adequada dos recursos humanos, qualificação de qualidade e contínuo aperfeiçoamento do pessoal no emprego das diversas técnicas operacionais.

A experiência brasileira por ocasião dos grandes eventos esportivos demonstrou a importância do intercâmbio de informações com outros países, especialmente na contenção da ameaça terrorista. Há que se estabelecer, todavia, mecanismos seguros de compartilhamento de informações. Por outro lado, ainda que seja extremamente interessante o intercâmbio de informações com serviços de inteligência de outros países, a inteligência nacional não pode se tornar excessivamente dependente desses órgãos.

A variada disponibilidade de fontes tecnológicas não foi eficazmente empregada pela comunidade de inteligência norte-americana no acompanhamento da ameaça terrorista. O SISBIN deve trabalhar no sentido de prover seus órgãos com meios tecnológicos capacitados. Entretanto, há necessidade, também, de formação de recursos humanos qualificados, que possam empregar a tecnologia disponível nas diversas fases do ciclo de inteligência. Há que se buscar, ainda, a constante integração da inteligência cibernética com as demais disciplinas de inteligência.

Nos relatórios pós-11 de Setembro, muito se falou sobre a falta de criatividade dos analistas de inteligência e a produção de análises estratégicas deficientes, em virtude de inexperiência, incompetência e falta de treinamento. Nesse campo, identifica-se como lição aprendida a importância da qualificação dos recursos humanos, fornecendo as ferramentas necessárias para a produção de análises de qualidade. Outro aspecto que pode contribuir para análises mais robustas e precisas é uma maior permanência do especialista em sua área de acompanhamento.

Ainda no campo da análise, torna-se necessária a constante avaliação da doutrina em vigor, especialmente quanto às técnicas de análises e aos procedimentos adotados pelos analistas. Como foi observado por especialistas norte-americanos, o ideário de Sherman Kent foi concebido em outro contexto histórico e sua reavaliação pode ensejar mudanças necessárias ao atual mundo BANI. O analista deve agregar valor às suas análises e usar sua experiência e intuição para compreender a complexidade das ameaças atuais. Por fim, com o achatamento dos níveis de decisão, em todos as esferas de poder, o analista deve ter em mente o contexto político em que está inserido, além de entender as necessidades dos usuários e decisores.

Por fim, e não menos importante, destaca-se o que é de conhecimento notório de todo profissional de inteligência: a importância da contrainteligência. A comunidade de inteligência possuía, desde 1998, conhecimento de que a Al Qaeda tinha a intenção e planejava realizar um ataque terrorista em território norte-americano. Apesar disso, não foram planejadas quaisquer medidas preventivas ou mesmo ações defensivas, no campo do antiterrorismo, objetivando neutralizar a ameaça.

Conclusão

Os atentados terroristas em território norte-americano, em 11 de setembro de 2001, constituíram-se em eventos disruptivos que marcaram a história mundial. Suas consequências e efeitos ultrapassaram as fronteiras do grande país ao norte e transformaram profundamente a ordem mundial. Sobre a comunidade de inteligência dos EUA, entretanto, recaíram as principais acusações de responsabilidade pelas falhas em evitar os ataques.

A atividade de inteligência ganhou grande impulso pós-Segunda Guerra Mundial, com a Lei de Segurança Nacional de 1947, mas não foi capaz de evitar os ataques de 11 de setembro. A comunidade de inteligência era marcada, à época dos atentados de 2001, por deficiências na integração entre os diversos componentes do sistema. Havia uma profunda deficiência na organização e coordenação dos trabalhos dentro da comunidade, muitas vezes por falta de clara definição do papel de cada agência. Além disso, as agências possuíam cultura organizacional burocrática e lenta, que não estimulava a criatividade, a aversão ao risco e à integração com outros órgãos. Ademais, a falta de diretrizes políticas priorizando o esforço de inteligência revelou a falta de comunicação entre o nível político e a comunidade de inteligência.

No que diz respeito às falhas humanas, concluiu-se que a análise estratégica produzida sobre a ameaça terrorista era deficiente e sem criatividade. Da mesma forma, a inteligência humana não foi empregada em sua plenitude, gerando lacunas de conhecimento que outras disciplinas de inteligência não foram capazes de suprir. Houve, ainda, excesso de confiança na inteligência produzida por serviços estrangeiros. Mesmo o emprego das fontes tecnológicas não produziu a inteligência necessária para evitar os atentados. Não foi realizado, também, o rastreamento das atividades financeiras das organizações terroristas. Por fim, medidas de contrainteligência não foram adotadas para proteger os ativos do país.

Diante das falhas apresentadas, observou-se, nesse trabalho, aquelas que poderiam se constituir em lições aprendidas para a inteligência brasileira. Assim, lições indicam a necessidade de fortalecer a integração do SISBIN. Para a inteligência nacional, fica, ainda, a necessidade de definição clara das responsabilidades de

cada órgão do SISBIN no acompanhamento das ameaças. Além disso, destaca-se a importância de dotar os órgãos de inteligência com estruturas de análise com capacidade de produzir assessoramento oportuno e preciso aos decisores.

Faz-se necessário trabalhar a cultura organizacional dos diversos integrantes do sistema, buscando facilitar o rastreamento das atividades financeiras das ameaças, incrementar a já existente integração entre o SISBIN e outros órgãos do governo, assim como o compartilhamento de informações relevantes. Ressalta-se, ainda, a importância de documentos de alto nível estabelecendo as diretrizes e as prioridades de inteligência para os integrantes do SISBIN.

Em outro plano, a HUMINT deve ocupar papel de relevância no SISBIN, com preocupação constante com a qualificação dos recursos humanos. Importante buscar a integração das diversas fontes, especialmente as fontes tecnológicas, com destaque para a inteligência cibernética. A formação do analista deve ser reavaliada para que esteja sempre adequada à conjuntura do momento. Por fim, a contrainteligência deve ser enfatizada com suas medidas preventivas e preditivas.

Ao final deste trabalho, pode-se inferir a pertinência da realização de estudos visando levantar as falhas cometidas pela comunidade de inteligência dos EUA por ocasião dos atentados terroristas de 2001. Tão relevante quanto isso, entretanto, foi identificar em que medida os erros apontados podem se constituir em lições aprendidas para a inteligência brasileira, contribuindo para tão importante atividade de Estado, fundamental para a segurança nacional.

Referências

AGÊNCIA BRASILEIRA DE INTELIGÊNCIA (ABIN). **Atividades**. Gabinete de Segurança Institucional. Brasília, 2020a. Disponível em: https://www.gov.br/abin/pt-br/assuntos/sisbin/atividades. Acesso em: 21 abr 2022.

AGÊNCIA BRASILEIRA DE INTELIGÊNCIA (ABIN). **Histórico**. Gabinete de Segurança Institucional. Brasília, 2020b. Disponível em: https://www.gov.br/abin/pt-br/acesso-a-informacao/institucional/historico. Acesso em: 21 abr 2022.

AGÊNCIA BRASILEIRA DE INTELIGÊNCIA (ABIN). **Integração**. Gabinete de Segurança Institucional. Brasília, 2020c. Disponível em: https://www.gov.br/abin/pt-br/assuntos/sisbin/integracao. Acesso em: 21 abr 2022.

BADER, Juan Pablo. **Sistemas de inteligencia en la experiencia comparada**. Biblioteca del Congreso Nacional de Chile. Santiago, 2019. Disponível em: https://obtienearchivo.bcn.cl/obtienearchivo?id=repositorio/10221/26864/1/sistemas_de_inteligencia_en_la_experiencia_comparada.pdf. Acesso em: 20 abr 2022.

BERKOWITZ, Bruce. **Spying in the post-september 11 world**. Hoover digest, v. 4, p. 14-21, 2003.

BRASIL. Presidência da República. Lei n. 9.883, de 6 de dezembro de 1999. **Diário Oficial da União**, Brasília, 8 de dezembro de 1999, ano 1999, p. 1.

BRASIL. Presidência da República. Decreto n. 4.736, de 12 de setembro de 2002. **Diário Oficial da União**, Brasília, 16 de setembro de 2002, ano 2002, p. 4.

BRASIL. Agência Brasileira de Inteligência (ABIN). **Estratégia Nacional de Inteligência**. Brasília, 2017a. Disponível em: https://www.gov.br/abin/pt-br/centrais-de-conteudo/publicacoes/enint.pdf. Acesso em: 19 mar 2022.

BRASIL. Presidência da República. Decreto de 14 de dezembro de 2017b. **Diário Oficial da União**: seção 1, Brasília, 18 de dezembro de 2017, ano 2017, p. 36.

BRASIL. Ministério da Defesa. Exército Brasileiro. Estado-Maior do Exército. **Manual de Fundamentos EB20-MF-03.109**: Glossário de termos e expressões para uso no Exército. 5. ed. Brasília, DF, 2018.

BRASIL. Presidência da República. Lei n. 13.844, de 18 de junho de 2019. **Diário Oficial da União**, Brasília, 18 de junho de 2019, ano 2019, p. 4.

CARAFANO, James J. **The case for intelligence reform**: a primer on strategic intelligence and terrorism from the 1970's to today. Heritage Foundation, 2004.

CILLUFFO, Frank J.; MARKS, Ronald A.; SALMOIRAGHI, George C. **The use and limits of US intelligence**. Washington Quarterly, v. 25, n. 1, p. 61-74, 2002.

GOODMAN, Melvin. **Intelligence Failure**. The decline and fall of the CIA. Rowman & Littlefield publishers inc. New York, 2008.

FEDERATION OF AMERICAN SCIENTISTS (FAS). **The evolution of the US intelligence community** – a historical overview. Intelligence Resource Program. Washington, 1996. Disponível em: https://govinfo.library.unt.edu/npr/library/reports/intelexe.html. Acesso em: 20 abr 2022.

JOHNSON, Loch K. **A framework for strengthening US intelligence**. Yale J. Int'l aff., v. 1, p. 116, 2006.

MEDINA, Carmen A. **The coming revolution in intelligence analysis**: what to do when traditional models fail. Studies in intelligence, v. 46, n. 3, p. 24-26, 2002.

NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES. **The 9/11 Commission Report**. Washington, 2004.

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE (ODNI). **Intel.gov**. Washington, 2019. Disponível em: https://www.intelligence.gov/. Acesso em: 20 abr 2022.

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE (ODNI). **Office of the Director of National Intelligence**. Washington, 2022. Disponível em: https://www.dni.gov/index.php. Acesso em: 20 abr 2022.

RAMÍREZ, Franklin Barrientos. **El fracaso de la comunidad de inteligencia de Estados Unidos el 11 de septiembre de 2001**:¿ fallas humanas o sistémicas?. Revista Política y Estrategia, n. 116, p. 43-85, 2010.

SCHMITT, Gary J. **Truth to power?** Rethinking intelligence analysis. In Peter Berkowitz (editor): The future of intelligence. Hoover Press, 2006.

THE HOUSE PERMANENT SELECT COMMITTEE ON INTELLIGENCE AND THE SENATE SELECT COMMITTEE ON INTELLIGENCE. **Report of the joint inquiry into the terrorist attacks of September 11, 2001**. Washington, 2002.

ZEGART, Amy B. **September 11 and the adaptation failure of US intelligence agencies**. International Security, v. 29, n. 4, p. 78-111, 2005.