RBI

Revista Brasileira de Inteligência

Número 13, dezembro 2018, ISSN 2595-4717

PRESIDÊNCIA DA REPÚBLICA
GABINETE DE SEGURANÇA INSTITUCIONAL
AGÊNCIA BRASILEIRA DE INTELIGÊNCIA

Revista Brasileira de Inteligência

ISSN 1809-2632 versão impressa
ISSN 2595-4717 versão online

Pareceristas
Ana Maria Bezerra Pina, Bruno Seixas de Noronha, Delanne Novaes de Souza, Edson de Moura Lima, Eduardo Castello, Eduardo Henrique Pereira de Oliveira, Fábio Nogueira de Miranda Filho, Gills Vilar-Lopes, Pedro Nogueira Gonçalves Diogo, Ryan de Sousa Oliveira, Roniere Ribeiro do Amaral.

Capa
Helen Santos Rigaud.

Editoração Gráfica
Luciano Daniel da Silva.

Revisão
Caio Márcio Pereira Lyrio, Cláudia Suzano de Almeida e Eliete Maria de Paiva.

Catalogação bibliográfica internacional, normalização e editoração
Centro de Fontes Abertas - CFA/CGPAS/ESINT.

Disponível em
http://www.abin.gov.br

Contato
SPO Área 5, quadra 1, bloco D
CEP: 70610-905 – Brasília/DF
E-mail: revista@abin.gov.br

Tiragem desta edição
300 exemplares.

Impressão
Gráfica - Abin.

Dados Internacionais de Catalogação na Publicação (CIP)

Revista Brasileira de Inteligência / Agência Brasileira de Inteligência.
– n. 13 (dez. 2018) – Brasília: Abin, 2005 –
163 p.
Anual
ISSN 1809-2632 versão impressa
ISSN 2595-4717 versão online
1. Atividade de Inteligência – Periódicos 1. Agência Brasileira de Inteligência.

CDU: 355.40(81)(051)

SUMÁRIO

Editorial

Nos últimos dez anos, a Atividade de Inteligência do Brasil esteve envolvida com dois grandes processos, um de natureza histórica e outro de natureza política.

O processo de natureza histórica inicia-se em 2006, quando a Atividade de Inteligência engajou-se na primeira experiência de atuação integrada de órgãos em grandes eventos. Esse ciclo histórico inclui a série: Jogos Pan-Americanos (2007), Rio+20 (2012), Copa das Confederações (2013), Jornada Mundial da Juventude (2013), Copa do Mundo FIFA (2014) e Jogos Olímpicos e Paralímpicos (2016). Um ciclo que marca a história do país.

No seio da Agência Brasileira de Inteligência, isso inspirou a criação de um curso de pós-graduação *lato sensu* denominado "Curso de Gestão Integrada da Atividade de Inteligência", iniciado em 2018 e conduzido na Escola de Inteligência com a colaboração da Diretoria de Inteligência Policial do Departamento de Polícia Federal, do Instituto Rio Branco e da Escola de Inteligência Militar do Exército. Além disso, esse conjunto de grandes eventos condicionou outro grande processo: a publicação de atos normativos básicos para essa área da administração federal.

O outro processo, de natureza política, inicia-se em 2009, com o trabalho de elaboração dos marcos normativos da Atividade. O primeiro documento a ser concebido foi a Política Nacional de Inteligência. Contingências políticas adiaram sua publicação, o que ocorreu em junho de 2016. Esse documento foi complementado, em dezembro de 2017, pela Estratégia Nacional de Inteligência. Juntamente com a Estratégia, em maio de 2018, um Plano Nacional de Inteligência veio a detalhar a Política. Esses documentos de normatização da Atividade de Inteligência consolidam o intenso esforço de legitimação e racionalização desse segmento estatal.

O que se vê nesses processos é a prática e a gestão pública, em procedimentos paralelos e entrelaçados, determinando o aperfeiçoamento da Atividade de Inteligência. A extensão desses processos por governos distintos também evidencia o aspecto técnico desse setor da administração pública do Estado, lastreada em lei e políticas públicas.

A Revista Brasileira de Inteligência (RBI) é produto da Abin que contribui para a consistência dessa condição técnica. A RBI reúne o pensamento de profissionais, do Sistema Brasileiro de Inteligência e de outros campos, interessados em contribuir para a reflexão e, consequentemente, para o desenvolvimento dessa atividade.

Na RBI, vale o juízo corroborado em evidências e em argumentação racional. Ela é veículo público (na internet, exposto ao escrutínio do leitor) e republicano. Ela promove também o debate e, assim, exercita a democracia.

Participe dessa experiência: boa leitura!

Comissão editorial

O IMPACTO DE VIESES COGNITIVOS SOBRE A IMPARCIALIDADE DO CONTEÚDO DE INTELIGÊNCIA

André Mendonça Machado *

Resumo

Pesquisas em Psicologia Cognitiva demonstram que a mente humana está sujeita a uma variada sorte de condicionantes que limitam sua racionalidade e interferem na capacidade do homem de fazer escolhas e julgamentos lógicos. Na origem desse processo estão os vieses cognitivos, erros de raciocínio causados pela simplificação da representação do mundo pelo intelecto. O estudo desse fenômeno interessa aos profissionais de Inteligência pelo risco que representa para o processo de produção do conhecimento e, consequentemente, para o assessoramento no processo decisório nacional. Uma das características distintivas do conteúdo de Inteligência, a imparcialidade, é particularmente vulnerável à incidência desses vieses, o que exige controle por parte das organizações de Inteligência como premissa para garantir a utilidade de seu produto para a sociedade e o Estado. O objetivo do trabalho é assinalar o risco do impacto dos vieses cognitivos sobre a imparcialidade e indicar possibilidades de aperfeiçoamento da gestão do processo de produção do conhecimento. Ações de capacitação profissional e de aprimoramento nos controles dos processos de trabalho contribuem para a melhoria da qualidade do produto final das agências de Inteligência e para o fortalecimento da Atividade de Inteligência como instrumento de defesa dos interesses nacionais.

Palavras-chaves: Viés cognitivo, viés de confirmação, princípio da imparcialidade, processo decisório, assessoramento de Inteligência.

THE IMPACT OF COGNITIVE BIASES ON THE IMPARTIALITY OF INTELLIGENCE CONTENT

Abstract

Research in Cognitive Psychology shows that the human mind is subject to a variety of constraints, which curb its rationality and interfere with man's ability to make logical choices and judgments. Errors of reasoning caused by the simplification of the representation of the world by the intellect, that is to say the cognitive biases, are at the origin of this process. The study of such phenomenon draws the attention of Intelligence professionals, since cognitive biases pose a risk for the knowledge production process and, therefore, for the proper advising to the national decision-making process. One of the distinctive attributes of Intelligence, impartiality, is particularly vulnerable to the occurrence of cognitive biases, thus requiring control by Intelligence organizations as a premise to ensure the usefulness of their product to society and the state. The objective of this work is to point out the risk of the impact of cognitive biases on impartiality and indicate opportunities for improving the management of the knowledge production process. Professional training and improvement in the control of work processes, with focus in cognitive biases, may contribute to the enhancement of the final product of Intelligence agencies and to the strengthening of the Intelligence activity.

Keywords: *Cognitive bias, confirmation bias, decision-making process, Intelligence advisory role.*

---

* Oficial de Inteligência da Agência Brasileira de Inteligência.

Artigo recebido em julho/2018
Aprovado em setembro/2018

Introdução

O sociólogo e filósofo polonês Zygmunt Bauman cunhou a expressão Modernidade Líquida para referir-se à forma fluida e efêmera das relações. Nesses tempos líquidos, os produtos são descartáveis, a economia é volátil, as instituições são instáveis e as certezas são passageiras. Desigualdade social, violência urbana, terrorismo e corrupção liquefizeram as ligações entre as pessoas e colocaram em xeque o papel do Estado. É nesse ambiente de indeterminação que as agências de Inteligência devem produzir conhecimento útil a fim de colaborarem na redução de incertezas no âmbito do processo decisório nacional. Uma questão com a qual os gestores dos processos de produção de conhecimento têm que lidar é a manutenção das qualidades intrínsecas de um conteúdo de Inteligência, entre elas a imparcialidade, característica que confere singularidade à Inteligência de Estado quando comparada com outras atividades.

O problema levantado neste trabalho é como uma organização de Inteligência pode preservar o atributo da isenção diante de uma ameaça específica: o impacto de vieses cognitivos sobre o conteúdo de Inteligência. Essa preocupação se justifica em virtude da pouca importância dada a esse controle na gestão do processo de produção de conhecimento. Tradicionalmente, são empreendidos esforços em uma diversa gama de iniciativas: refinamento da coleta em fontes abertas, aprimoramento da atividade de busca com fontes humanas e meios técnicos, intensificação do intercâmbio com órgãos congêneres nacionais e estrangeiros, contratação de mais pessoal e capacitação em temas, idiomas e escrita. Porém, analistas não são treinados para aprimorar sua forma de pensar. Para abordar essa temática, foram feitas uma revisão de literatura sobre vieses cognitivos e uma análise do instituto do princípio da imparcialidade em documentos estruturantes da Atividade de Inteligência. A combinação desses elementos permitiu proceder a um exame do atual estado do problema. O objetivo deste trabalho é especificar alguns vieses cognitivos, assinalar seu risco para a imparcialidade na produção do conhecimento e apontar iniciativas de gestão que ajudem a mitigar os efeitos indesejados desse fenômeno.

Modelos mentais e viés cognitivo: o limite da racionalidade

Segundo Heuer (1999, p. 3), a mente humana, em virtude de sua capacidade limitada, não consegue lidar diretamente com a complexidade do mundo. Por isso, ela constrói um modelo mental simplificado da realidade e usa essa representação como objeto de trabalho sobre o qual são feitas suas análises. Assim, reconhece Heuer, o entendimento humano do mundo é o retrato de uma escolha subjetiva. A cognição é ajustada de acordo com as limitações inerentes ao funcionamento mental, sujeito a diversos tipos de vieses, entre eles o viés cognitivo. Vieses cognitivos são erros de raciocínio causados por estratégias mentais de simplificação geradas no esforço de processamento de informações. Não se confundem com outros tipos de vieses, como os organizacionais e culturais ou ainda os intencionais com objetivos escusos. Davies (1999, p. 21) explica que a mente constrói sua própria versão de realidade

com base nas informações fornecidas pelos sentidos e que esta entrada sensorial é mediada por processos mentais complexos que determinam quais informações são selecionadas e o significado que lhes é atribuído. Segundo ele, o que e como as pessoas percebem é fortemente influenciado por experiências passadas, educação, valores culturais, exigências funcionais e normas organizacionais, tanto quanto pelas especificidades da informação recebida.

Para Kahneman quando um julgamento é feito, a mente não está necessariamente consciente de como esse processo ocorreu. Apenas a interpretação mais adequada dos fatos desponta e possíveis incertezas, obscuridades ou ambivalências são eliminadas. A mente contenta-se com o que foi captado e não sente necessidade de confrontar a representação elaborada no intelecto. Kahneman explica ainda que a quantidade e a qualidade dos dados em que a narrativa construída está baseada são irrelevantes. Quando a informação é escassa, a mente opera "como uma máquina tirando conclusões precipitadas". A consistência da história importa mais que sua completude. Na prática, um volume maior de informações torna mais difícil para o intelecto processar e ajustar tudo o que se sabe dentro de um padrão coerente. A mente constrói a melhor história a partir da informação disponível e é esta a versão que prevalece como representação do mundo real. "Nossa reconfortante convicção de que o mundo faz sentido repousa em um alicerce seguro: nossa capacidade quase ilimitada de ignorar nossa própria ignorância" (2012, p. 205 - 251).

As classificações e descrições dos tipos de vieses cognitivos variam entre os diferentes autores. O que eles têm em comum é a propriedade de impedir a ampliação da capacidade lógica de produzir julgamentos distantes do modelo mental a que o intelecto está habituado. Segundo Kahneman (2012, p. 126),

> [...] o estado normal de sua mente é que você dispõe de sentimentos e opiniões intuitivos sobre quase tudo que surge em seu caminho. Você simpatiza ou antipatiza com uma pessoa bem antes de saber muita coisa sobre ela; você mostra confiança ou desconfiança em relação a estranhos sem saber por quê; você sente que um empreendimento está fadado ao sucesso sem fazer uma análise. Quer você afirme, quer não, muitas vezes tem respostas para perguntas que não compreende completamente, apoiando-se em evidências que não é capaz de explicar nem de defender.

As avaliações básicas desempenham papel importante na formação de um julgamento, pois substituem avaliações mais profundas em questões mais difíceis. Esse processo mental é abordado pelos pesquisadores de heurísticas[1] e vieses. Eles explicam que se uma resposta satisfatória a uma pergunta difícil não é rapidamente encontrada, a mente buscará responder a uma pergunta relacionada que é mais fácil.

Como exemplo de viés cognitivo, Heuer descreve a "ancoragem", estratégia mental intuitiva e inconsciente para simplificar a tarefa de fazer julgamentos (1999, p. 150). Um ponto de partida qualquer –

1 A definição de heurística é "um procedimento simples que ajuda a encontrar respostas adequadas, ainda que geralmente imperfeitas, para perguntas difíceis" (KAHNEMAN, 2012, p. 127).

por exemplo, certa avaliação anterior do mesmo objeto por outra pessoa – é usado como primeira aproximação do problema, à qual novas informações são adicionadas. A partir daí, será elaborada uma análise com o objetivo de ajustar o julgamento anterior à nova realidade. Entretanto, o que ocorre na prática é que o ponto de partida serve como uma âncora que reduz o volume de ajustamento e assim a estimativa final permanece mais perto do ponto de partida do que poderia estar. Tversky e Kahneman explicam que diferentes pontos de partida produzem diferentes estimativas finais, enviesadas na direção dos valores iniciais (2012, p. 533).

Kahneman descreve um fenômeno semelhante denominado "efeito halo" (2012, p. 107). Ele explica que a ordem com que uma pessoa observa uma série de eventos vai influenciar o julgamento final a respeito dessa sequência. O efeito halo aumenta o peso das primeiras impressões em relação às seguintes, às vezes a tal ponto que a informação subsequente é em grande parte desperdiçada. Uma vez formada uma narrativa lógica e coerente, a mente começa a dispensar dados adicionais por considerá-los excessivos, em particular aqueles que possam trazer incertezas. Taleb chama essa limitação mental de "falácia narrativa". Para ele, a mente prefere as histórias compactas à interpretação profunda, o que a torna vulnerável a representações distorcidas do mundo. "Nós gostamos de histórias, gostamos de resumir e gostamos de simplificar, ou seja, de reduzir a dimensão das questões" (2008, p. 100).

Taleb explica ainda que, no esforço de atribuir coerência à história, a mente reconstrói relatos inconsistentes do passado, acreditando que são verdadeiros. Para ele, "tendemos a lembrar mais facilmente os fatos de nosso passado que se encaixam em uma narrativa, enquanto tendemos a negligenciar outros que não aparentam desempenhar um papel causal nessa narrativa" (2008, p. 109). Ao recordar não a sucessão real de eventos, mas uma reconstrução dela, a mente dá uma aparência de razoabilidade à história e assim a torna mais explicável do que ela é.

No mesmo sentido, Kahneman afirma: "a mente que formula narrativas sobre o passado é um órgão criador de sentido. Quando um evento imprevisto ocorre, imediatamente ajustamos nossa visão de mundo para acomodar a surpresa". Ele explica que, uma vez tendo adotado uma nova visão de mundo, a mente perde muito de sua capacidade de recordar em que costumava acreditar antes de mudar de ideia. Ao reconsiderar suas antigas crenças, "as pessoas lembram-se, em vez disso, de suas atuais – um caso de substituição – e muitas não conseguem acreditar que um dia acharam outra coisa. Kahneman chama esse processo de "viés retrospectivo" e alerta que ele "gera uma robusta ilusão cognitiva". "O mundo faz muito menos sentido do que você pensa. A coerência deriva principalmente do modo como sua mente funciona" (2012, p. 253, 254, 70).

Kahneman descreve também o efeito que ele chama de *"priming"*: a exposição a uma ideia facilita a evocação de outras ideias relacionadas. "Como marolas num lago, a ativação se difunde por uma pequena parte da vasta rede de ideias associadas, cujo mapeamento ainda não foi possível". Ele acrescenta ainda: "Ações e emoções podem

ser primadas por eventos dos quais nem sequer se tem consciência". Essas operações de memória associativa contribuem para um "viés de confirmação", isto é, a mente tende a buscar validação daquilo que já conhece. Diante de uma pergunta, a mente testa a hipótese mediante uma busca deliberada por evidência confirmadora, em uma espécie de "estratégia de teste de positivo". O viés confirmatório favorece a aceitação acrítica de sugestões e o exagero da probabilidade de eventos extremos e improváveis (2012, 69, 70, 109).

> Contrariamente às regras dos filósofos da ciência, que aconselham testar hipóteses tentando refutá-las, as pessoas (e os cientistas, às vezes), buscam dados que tenham maior probabilidade de se mostrarem compatíveis com as crenças que possuem no momento (2012, p. 106).

Outro fator de geração de erros sistemáticos, segundo Kahneman, é a "heurística da disponibilidade". As falhas ocorrem quando a mente recorre a lembranças afetivas e emocionais ao invés de pensar em ocorrências numéricas. A memória de eventos dramáticos recentes, como a queda de um avião, é mais disponível para influenciar o julgamento das pessoas sobre segurança do transporte aéreo do que estatísticas, por exemplo. "Um erro judicial que o afete vai minar sua fé na justiça mais do que um incidente similar sobre o qual você tenha lido em um jornal" (2012, p. 167). A mente elabora julgamentos baseados em emoções muito mais que em avaliação de dados. O viés da disponibilidade está na origem do fenômeno que os cientistas chamam de "cascata de disponibilidade", uma cadeia de eventos autossustentável que começa com a divulgação de um fato menor pela imprensa que leva pânico ao público, o que obriga o governo a tomar ações de larga escala. Essas ações causam ainda mais alarde e a reação pública torna-se um evento em si mesmo, o que gera mais cobertura midiática, mais preocupação e mais envolvimento, num ciclo que pode ser acelerado por organizações interessadas em manter um fluxo contínuo de notícias preocupantes. Nesse caso, ações concretas de interesse público têm de ser relegadas a segundo plano para dar lugar à atenção política sobre o sentimento coletivo de insegurança.

Vieses cognitivos: um risco para a Inteligência Estratégica

Pesquisas em Psicologia Cognitiva sobre percepção, memória e raciocínio demonstram limitações relacionadas à interferência de vieses cognitivos e subsidiam estudos na área de Inteligência sobre falhas de análise de diversos profissionais e serviços de Inteligência. O foco das pesquisas é entender o papel do analista ao coletar e processar material. Tversky e Kahneman (2012, p. 536) afirmam que "a confiança nas heurísticas e a prevalência de vieses não estão restritas aos leigos. Pesquisadores experientes também são propensos aos mesmos vieses – quando pensam intuitivamente". Segundo eles, mesmo que pessoas "estatisticamente sofisticadas" evitem erros de julgamento em questões elementares, elas estão sujeitas a falácias em problemas mais intrincados e menos transparentes. Para Kahneman (2012, p. 65), inteligência elevada é diferente de racionalidade e não torna as pessoas imunes a vieses.

Heuer (1999, p. 52) afirma que, tendo estabelecido determinada programação mental em torno de um tema específico, o profissional de Inteligência tende a acoplar toda nova informação ao fortalecimento de uma argumentação lógica antiga. Uma vez que o analista disponha de informação suficiente para formar julgamento sobre um fato de interesse da Inteligência, a obtenção de mais dados geralmente não melhora a precisão da análise. Ao contrário, mais informação o torna mais seguro sobre seu juízo e o leva a se sentir excessivamente confiante e confinar a busca de dados em torno de uma operação de confirmatória. Além disso, o profissional tende a valer-se sempre das mesmas fontes, com as quais tem familiaridade e que acabam por reforçar seu modelo mental. Heuer acrescenta que analistas têm um entendimento imperfeito de qual informação realmente utilizam ao fazer seu julgamento. Eles não seriam, portanto, capazes de perceber até que ponto suas análises são determinadas por apenas alguns elementos dominantes, e não pela integração sistemática de todos os fatores acessíveis. Ao final, sua interpretação sobre os elementos integrados parecerá coesa, coerente e congruente, ainda que tenha sido fundamentada em frações incompletas e insuficientes. Em outras palavras, os analistas não são conscientes do enviesamento de seus produtos.

Heuer exemplifica o efeito de ancoragem com o evento típico do analista que se muda para nova área de análise e assume a produção de conhecimentos já iniciada por seus antecessores. O que acontece é que mesmo quando o analista recém-chegado faz seu próprio julgamento e tenta revisá-lo com base em novas informações ou análise mais profunda, normalmente ele não muda sua avaliação inicial suficientemente. A iniciativa do analista anterior serve como uma âncora a qual o profissional prende suas primeiras impressões. Para Heuer, o simples esforço de tomar consciência do problema de ancoragem não é um antídoto adequado. Em testes, os vieses cognitivos persistem mesmo depois que o sujeito é informado deles e instruído a evitá-los ou compensá-los (1999, p.151, 152).

Lowenthal explica que a ancoragem de modelos mentais dificulta a extrapolação para uma nova forma de enxergar um tema familiar. Ele apresenta um exemplo para ilustrar como a limitação crítica afeta a análise: durante os anos 1980, alguns analistas estadunidenses trabalhando sobre o Irã falavam de iranianos "extremistas" e "moderados". Quando pressionados por seus colegas céticos a respeito das evidências sobre a existência de moderados, os analistas argumentavam que, se há extremistas, então devem haver moderados, numa aproximação ao padrão político reconhecível em seu próprio país. Lowenthal usa a expressão "clientismo" para descrever falha que ocorre quando os analistas se tornam tão imersos em seus temas a ponto de perder a capacidade de enxergar as questões com a criticidade necessária (2003, p. 93).

Herman partilha da mesma visão. Ele afirma que a Inteligência nunca vai entender países estrangeiros completamente e prever todas as suas ações. Há muitas falhas em antecipar um ataque iminente, mesmo quando há evidência suficiente. Isso seria explicado como uma rigidez cognitiva, isto é, a tendência humana de interpretar qualquer evidência à luz de preconceitos e de resistir

a explicações alternativas (2006, p. 239).

Jones usa o caso dos erros do relatório da Comunidade de Inteligência estadunidense sobre a existência de armas de destruição em massa no Iraque, em 2002, para exemplificar o efeito da ancoragem. Para ele, o ponto de partida das análises foi o histórico de uso daquelas armas e a ocultação do desenvolvimento de novos programas relacionados ao assunto nos anos 1990, o que levou as agências de Inteligência à noção de que o Iraque ainda possuía armas químicas e biológicas e que pretendia expandir sua produção (2005, p. 47). O enviesamento cognitivo tornou os analistas resistentes a evidências contrárias e reativos a perspectivas alternativas à ideia de que o Iraque ainda era uma ameaça, indispostos a concederem atenção a fatos que desafiassem suas premissas lógicas ancoradas no passado. Para Jones, outros fatores, como pressão política, dificuldade de acesso a fontes confiáveis e urgência também contribuíram para o erro; no entanto, nenhum organismo envolvido no processo foi capaz de reconhecer a influência do viés cognitivo nos erros de julgamento que levaram a uma guerra (2005, p. 34).

Esse exemplo ilustra o viés de confirmação descrito por Kahneman. Dados compatíveis são imediatamente integrados, independentemente de sua confiabilidade. Toda informação que contribuía para fortalecer o julgamento de que o Iraque possuía armas de destruição em massa, por mais frágil que fosse, encontrava encaixe em uma figura concebida de antemão na mente dos analistas. Kahneman prognosticou: "A essência da mensagem é a história, que está baseada em qualquer informação disponível, mesmo se a quantidade de informação é mínima e sua qualidade é ruim" (2012, p. 163). Não interessa se a história é verdadeira, o importante é que tenha coerência.

Como exemplo de impacto do viés de disponibilidade na área de Inteligência estratégica, Miranda Filho cita o exemplo da formação discursiva e ideológica criada pelos Estados Unidos da América (EUA) após os atentados de 11 de Setembro,

> [...]em que se divulgou a noção de que o terrorismo era a nova ameaça global e que todos os países deveriam se juntar aos EUA nessa cruzada. Os discursos foram lançados por meio de artigos acadêmicos, principalmente nos temas Ciência Política, Defesa e Inteligência, na imprensa de forma massiva e generalizada, nos discursos oficiais de autoridades, enfim, a partir de qualquer comunicação que tratava da segurança dos países. [...] Praticamente não houve vozes dissidentes. Houve aqui o que se chama de cascatas de disponibilidade, ou seja, um evento é exagerado pela imprensa e pelo público a ponto de se tornar a única coisa sobre a qual se fala, influenciando a definição de políticas públicas (2016, p. 62).

Vieses cognitivos na produção do conhecimento de Inteligência: a imparcialidade no assessoramento ao processo decisório

Segundo Heuer, os vieses cognitivos são considerados intratáveis, isto é, o ser humano não tem como se desfazer deles por se constituírem em ferramenta para que a mente consiga interagir com grandes volumes de informações. É esse mecanismo

mental que permite ao profissional de Inteligência selecionar e classificar de forma rápida e sistemática as informações de interesse de seu campo de análise. No entanto, Heuer explica, diferentemente do que se pensa, o analista não constrói uma imagem como quem monta um quebra-cabeças, coletando e encaixando as pequenas peças de informações. O que ocorre é que ele encontra peças variadas que caberiam em diferentes figuras e, ao invés de montar uma figura com as peças encontradas, forma primeiro uma imagem e depois seleciona as peças que podem completá-la. Assim, informações relevantes são descartadas por não se encaixarem no modelo mental. Preconceitos e presunções determinam a forma de perceber e processar as novas informações (1999. p. 170, 62).

Platt descreve a produção de conhecimentos, núcleo da Atividade de Inteligência, como um processo essencialmente intelectual e cita "um famoso mestre de Oxford" que dizia que "fatos nada significam" (1974, p. 309). Com isso, ele quer explicar que um fato não tem valor para a Inteligência "a não ser relacionado com outros fatos, ou posto em destaque o seu significado" (1974, p. 78). Portanto, em razão de sua natureza fundamentalmente representativa e analítica, esse processo está sujeito à interferência de vieses cognitivos. Segundo a Doutrina Nacional da Atividade de Inteligência (DNAI), o processo do conhecimento:

> [...] indica a passagem da sensibilidade para as representações mentais, que se desenvolvem das sensíveis para as conceituais, em um movimento de formas sensíveis ou empíricas para formas racionais ou abstratas de conhecimento. A representação sensível conecta a sensibilidade à abstração (BRASIL, 2016, p. 51).

Ainda segundo a Doutrina (BRASIL, 2016), processamento é a fase da produção em que "os conhecimentos e dados obtidos são submetidos a métodos analíticos que permitem selecionar suas partes, relacioná-las, integrá-las e produzir inferências". A "passagem da sensibilidade para as representações mentais", na qual "os conhecimentos e dados obtidos" são submetidos a "métodos analíticos", corresponde, na prática, aos procedimentos mentais que atribuem significado a fatos de interesse da Atividade de Inteligência e deles extraem conclusões, para transformá-los em conteúdo de Inteligência a ser difundido aos decisores. Portanto, o cerne da produção de conhecimento – a construção de uma representação racional – é um processo mental do qual resultará o produto final da Inteligência sujeito à interferência de vieses cognitivos. A Doutrina engendra também um "ciclo do conhecimento", onde "a Atividade condiciona o pensamento, que elabora o conhecimento, o qual, por sua vez, orienta o pensamento, que dirige a ação". O processo de construção do conhecimento encadeia-se em formas racionais que incluem a ideia, o juízo e o raciocínio, cuja articulação pode gerar formas ainda mais sofisticadas como a hipótese, a tese e a teoria. Assim, como elemento intermediário do ciclo e gerador do conhecimento de Inteligência, o pensamento racional ameaçado por vieses cognitivos torna ainda mais imperioso o tratamento desse risco.

Verifica-se também que a Doutrina idealiza a produção de um conteúdo de Inteligência neutro e livre de direcionamentos tendenciosos (BRASIL, 2016, p. 55),

condição para a entrega de um produto isento e objetivo ao usuário final. Rosito (2006, p. 24) lembra-nos, no entanto, de que a abordagem da realidade pelo analista de Inteligência pode ser descrita como o tipo de experiência vivida por esse profissional no contato com o fenômeno acompanhado.

> Assim sendo, os fatos analisados não podem ser dissociados daquele que produz o conhecimento. Quando a mente posiciona-se perante a verdade, o que de fato ocorre é um processo ativo de autorregulação entre uma pessoa, seus conhecimentos pré-existentes (*a priori*) e um novo fato que se apresenta. O quanto essa pessoa conhece, o que já viveu, o que sente, e o vocabulário de que dispõe, estão entre as variáveis inerentes ao processo de produção de um Conhecimento acerca desse novo fato. O Relatório de Inteligência traz consigo o dado, agregando a este as experiências distintas do observador (a fonte, o agente operacional) e do analista, transferindo-as para o processo decisório do usuário final.

Segundo a Doutrina Nacional da Atividade de Inteligência (DNAI), a imparcialidade "consiste em abordar o assunto sem interesses e ideias preconcebidas que possam distorcer os resultados dos trabalhos" (BRASIL, 2016). O Planejamento Institucional da Abin (BRASIL, 2018) explica a imparcialidade como "isenção, no exercício da Atividade de Inteligência, de juízos de valor decorrentes de interesses ou convicções pessoais de caráter filosófico, ideológico, religioso, político, societário ou corporativo". Essas formulações objetivam advertir para a necessidade de que o produto final do processo de produção do conhecimento de Inteligência esteja livre de vieses de qualquer natureza. A DNAI demonstra preocupação com interferências externas quando afirma que "o produtor deve proceder de tal maneira que os conhecimentos produzidos sejam úteis e confiáveis ao usuário, sem, no entanto, descurar do princípio da imparcialidade" (BRASIL, 2016, p. 34). Nessa passagem, a Doutrina alerta para o fato de que há um risco, para a organização, no esforço de atingir um lugar de prestígio no assessoramento: tentar cativar o usuário pode comprometer a isenção do conteúdo de Inteligência. Em outras palavras, há um limite de proximidade entre produtor e usuário de Inteligência que deve ser obedecido a fim de que a atividade de assessoramento atenda não a interesses organizacionais ou políticos, mas seja direcionada ao Estado "e apenas para os propósitos legitimados democraticamente". "Rejeita-se o uso da Atividade de Inteligência como instrumento de particulares organizados em classes e grupos".

Kent (1967, p. 173) afirma que "não há nada mais importante nas informações do que as relações adequadas entre o seu pessoal e as pessoas que utilizam o produto de seu trabalho". Ele adverte que essas relações não ocorrem naturalmente, mas "são estabelecidas por meio de um grande esforço consciente e persistente, e é provável que desapareçam se esse esforço for relaxado". Por relações adequadas, o autor explica ainda que as informações "devem estar suficientemente próximas da política, planejamento e operações para obter o máximo de orientação, mas não tão próximas a ponto de perderem sua objetividade e integridade de julgamento". Isto é, a proximidade excessiva com o usuário final tende a comprometer o princípio da imparcialidade do conteúdo de

Inteligência. Em 1949, Kent já antecipava o que pesquisadores da psicologia analítica e da produção do conhecimento viriam a chamar, décadas mais tarde, de viés cognitivo:

> Uma equipe de informações habituada a esforçar-se para uma análise raciocinada e imparcial, para produzir algo de valor, tem suas dificuldades com os pontos de vista, posições, opiniões pessoais e linhas. Acima de tudo, ela é constituída de homens cujos padrões de raciocínio provavelmente colorirão suas hipóteses, e cujas hipóteses coloridas, provavelmente se tornarão uma conclusão mais atraente do que o demonstram as evidências. (...) O policiamento de suas inevitáveis irracionalidades é uma tarefa que lhes ocupa as vinte e quatro horas do dia. Mesmo assim nem sempre são bem sucedidos (p. 189).

Kent demonstra preocupação com a parcialidade quando o produtor do conhecimento se torna tão próximo do utilizador que passa a ser controlado por este. Nesse caso, ocorre uma modelagem cognitiva: a produção de conhecimento começa a ancorar-se nas expectativas do usuário em ver sua linha política executiva ser apoiada pela organização de Inteligência.

> [...] se as informações aparecem sempre com novidades em desacordo com a política do órgão de execução, não posso imaginar como contarão com seu apoio indefinidamente. Não posso deixar de pensar que [...] as informações serão diretamente envolvidas pela política e que tornar-se-ão fanáticos apologistas de uma dada política, em lugar de serem seu analista imparcial e objetivo (p.190).

No mesmo sentido, Afonso destaca que "a proximidade exacerbada entre analista e decisor pode criar distorções analíticas "[...] caso *[o oficial de Inteligência]* troque a imparcialidade inerente ao seu trabalho pela admiração por seu interlocutor". A ancoragem na ideologia do usuário gera um viés confirmatório crônico na mente do profissional e a elaboração de conhecimento redunda em um emparelhamento empírico de produção.

> A falta de eventuais contraposições entre usuário e produtores cria uma barreira que simplifica o ciclo de Inteligência de uma maneira tão perversa que pode inspirar o *policymaker* a cometer erros graves. Devido à poderosa confiança que se origina da similaridade entre os argumentos dos decisores e da Inteligência, potenciais questionamentos às análises, contra ou a favor de informações que fundamentam uma argumentação, permanecerão indefinidamente latentes. Nesse contexto, informações que necessitem de agregação de valor (confirmação) carecerão de atenção, o que comprometerá todo o resultado final da confecção do produto de Inteligência. Criar-se-á um círculo vicioso difícil de ser quebrado (2006, p. 15).

Em sua ânsia de atender prontamente ao usuário, os analistas produzem conhecimento na contingência de um viés de expectativa e a organização corre o risco de incorrer em seu erro mais grave, o assessoramento com potencial de dano ao processo decisório nacional.

Mecanismos de controle da imparcialidade em face dos vieses cognitivos

Os vieses cognitivos levam o analista a incorrer em erro, seja aceitando como verdadeira uma informação falsa, seja descartando como falsa uma informação verdadeira. Esse erro é um tipo de risco operacional que incide sobre o conteúdo

de Inteligência tanto em razão de uma falha na geração desse conhecimento quanto em razão de uma omissão no controle do processo de produção. No esforço de atender ao princípio da imparcialidade, as agências de Inteligência dependem da adoção de mecanismos capazes de identificar e reduzir em seu produto final a incidência dos erros decorrentes de vieses cognitivos. É tarefa dos envolvidos no processo de produção de conhecimento priorizar e definir respostas aos riscos e monitorar as ações de tratamento escolhidas. Quando não detectado e tratado pelo gestor, o erro redunda ainda em um risco de imagem para a organização pela possibilidade de comprometimento da qualidade do assessoramento.

Um dos pilares do tratamento do risco inerente aos vieses cognitivos é a estruturação de capacitação voltada para o ato de pensar. Para os gestores das agências de Inteligência que querem lidar com as limitações inerentes do processo mental dos analistas, Davis assinala que é necessário estabelecer um ambiente organizacional que promova e recompense o tipo de raciocínio crítico que não se ampare apenas nas primeiras hipóteses cabíveis, mas que continuamente reconsidere a fundo um conjunto de hipóteses plausíveis não admitidas no início da interpretação (1999, p. 24). Esse ambiente deve começar pelo treinamento dos profissionais de Inteligência. Segundo Heuer (1999, p. 4), analistas de inteligência devem entender a si mesmos antes que possam entender os outros. O treinamento deve aumentar a autoconsciência sobre como os oficiais de Inteligência percebem o mundo e fazem julgamentos analíticos. Eles devem ser capacitados também na superação desses problemas. O que ocorre geralmente é que há alguma instrução em técnicas metodológicas ou tópicos temáticos, mas pouco treinamento dedicado ao ato mental de pensar ou analisar.

No diagnóstico de Heuer (1999, p. 5), as organizações assumem, incorretamente, que analistas sabem como analisar. Alguns gestores entendem que, uma vez que o profissional admitido na carreira de Inteligência já tem formação de nível superior, a organização de Inteligência não tem necessidade de ensiná-lo a escrever relatórios, mas deve apenas instruí-lo nos temas de interesse da atividade. No entanto, a questão a ser enfrentada não é ensinar a escrever, mas ensinar a pensar a Inteligência, uma vez que não há formação específica na academia ou atividade no mercado de trabalho que prepare um profissional para produzir relatórios de assessoramento em Inteligência Estratégica. Platt (1974) explica: "Talvez seja mais correto dizer-se que, da forma como praticamos hoje em dia, *a Inteligência tem o talhe de uma profissão ao invés de ser uma profissão*" (p. 286, grifos do autor). Teixeira acrescenta que uma característica essencial do profissional de Inteligência é a:

> [...] flexibilidade de raciocínio, pois, ao se ter em conta as transformações de toda natureza pelas quais o mundo está passando, é fundamental que o profissional tenha capacidade de reavaliar posturas, reconsiderar ideias pré-concebidas e ter um pensamento bem articulado com a realidade (2006, p. 33).

No mesmo sentido, Heuer aponta que o problema é como garantir que a mente permaneça aberta a interpretações alternativas em um mundo em rápida transformação. Para ele, os analistas que mais sabem sobre um assunto são os que mais

têm a desaprender. Como exemplo, ele cita a Queda do Muro de Berlim: especialistas alemães tiveram que ser estimulados a aceitar o significado das mudanças dramáticas na direção da reunificação da Alemanha Oriental com a Ocidental. A desvantagem de uma programação mental, explica Heuer, é que ela pode controlar a percepção até o ponto em que um especialista experiente pode estar entre os últimos a ver o que realmente está acontecendo quando confrontado com uma grande mudança de paradigma (1999, p. 5). Mas o que se verifica na prática é que os analistas mais imersos em um processo viciado por vieses cognitivos e mais resistentes a mudanças são, paradoxalmente, aqueles mais investidos de autoridade e, em geral, detentores da última palavra na produção do conteúdo de Inteligência. O problema torna-se mais grave quanto mais especializado for o analista, uma vez que a preocupação institucional com a qualidade de sua produção diminui.

Platt avalia que, quanto a conhecimento técnico e métodos, a Inteligência aproxima-se dos demais campos de estudo, mas qualidades específicas devem ser desenvolvidas internamente nas organizações (1974, p. 286). Essa visão corrige a ideia corrente de que o profissional aprende a produzir Inteligência à medida que a produz. O que ocorre na prática é justamente o oposto: o profissional que se inicia mal orientado tende a reforçar vícios, aprofundar erros e produzir conteúdos cada vez mais enviesados e distantes das necessidades do assessoramento. Assim, as agências devem desenvolver e aplicar sistematicamente treinamento que examine os processos de pensamento e raciocínio envolvidos na análise de Inteligência. O currículo básico obrigatório do profissional de Inteligência pode se beneficiar de iniciativas de aprimoramento como treinamento em técnicas de análise estruturada, verificação da qualidade dos dados e *brainstorming;* conhecimentos sobre efeitos da percepção sobre o julgamento e sobre avaliação e validação de premissas, argumentos e hipóteses; e estudos em Linguística Geral e Aplicada, Análise do Discurso, Interferência Externa e Contrapropaganda. Estudos de doutrina podem aprofundar pesquisas sobre a influência de vieses cognitivos em cada uma das fases da Metodologia da Produção do Conhecimento (Planejamento, Reunião, Análise, Síntese e Interpretação), uma vez que todo o processo está sujeito a esse risco. Esse conjunto de disciplinas compõe o acervo de treinamento básico a ser aplicado ao profissional de Inteligência antes que ele seja considerado apto a se engajar no processo de produção de conhecimento.

A gestão do processo de produção do conhecimento é outro importante pilar na construção de um modelo de proteção contra o risco do enviesamento cognitivo do conteúdo de Inteligência. Davies (1999, p. 24) pontua que é necessário promover o desenvolvimento de ferramentas para auxiliar os analistas na avaliação de informações: em questões complexas, eles precisam de ajuda para melhorar seus modelos mentais tanto quanto precisam de novas informações. Diversas ferramentas de trabalho são úteis à redução do risco tratado aqui. A adoção de modelos de trabalho em grupos horizontais, onde os conteúdos são processados e integrados em equipe antes de serem submetidos à revisão, auxiliaria na redução da incidência de enviesamento cognitivo na produção de conhecimento.

Em relação à revisão, uma técnica capaz de beneficiar a qualidade do produto final é a "revisão por pares". Nesse sistema de verificação, o conteúdo não é revisado apenas por chefias, em um modelo vertical, mas submetido à apreciação de colegas fora da equipe de produção, conhecedores ou não do tema tratado, cuja identidade pode ser ou não reciprocamente conhecida. Outro recurso de identificação de vieses cognitivos é a implantação de um sistema de armazenamento e busca que garanta a disponibilidade de informações processadas pela agência de Inteligência não utilizadas em seus produtos finais. Esse acesso permitiria ao analista confrontar sistematicamente o material aproveitado com o material descartado, a fim de detectar e reduzir a incidência de efeitos de ancoragem e vieses de confirmação. Considerando-se que essas medidas estão relacionadas às etapas da metodologia da produção de conhecimentos, iniciativas de reestruturação e normatização de procedimentos metodológicos tendem a repercutir de forma sistêmica nos produtos internos e externos da organização.

Mais uma forma de ajudar os oficiais de Inteligência a tomarem consciência do processo pelo qual fazem análise é a releitura periódica do conteúdo produzido em cada unidade organizacional ou área temática. Heuer (1999, p. 5) explica que até há pouco tempo prevalecia a noção de que para perceber eventos com precisão era necessário apenas olhar para os fatos e purificar-se de todos os prejulgamentos. No entanto, hoje, há uma compreensão mais ampla de que analistas não abordam suas tarefas com mentes vazias, mas com um conjunto de suposições sobre como os eventos normalmente acontecem na área pela qual são responsáveis. A análise retrospectiva dos registros de produção sobre determinado assunto acompanhado por um grupo de analistas ao longo de certo período permite reavaliar o processo de construção dos conhecimentos. Com distanciamento histórico, os modelos mentais dominantes e os vieses cognitivos incorporados ao conteúdo de Inteligência podem ser identificados e rastreados e os analistas podem ser confrontados com seus próprios preconceitos e pré-julgamentos.

Outro suporte à detecção e redução de vieses cognitivos é a gestão da independência das agências de Inteligência em relação aos decisores. Shulsky (2002, p. 139) adverte que algum mecanismo deve assegurar que toda informação relevante, positiva ou negativa, esteja disponível para o consumidor de Inteligência, mesmo que o conhecimento entregue contrarie uma visão preestabelecida ou uma política em curso empreendida pelo mandatário. O autor explica que o papel do gestor é garantir que os profissionais de Inteligência, individualmente considerados, sintam-se protegidos de constrangimentos ou ameaças que possam induzi-los a produzir conclusões mais palatáveis ao usuário final. A única salvaguarda dos analistas é o amparo das chefias.

"O que a Inteligência sabe sobre isso?" Essa é a pergunta que mais interessa à agência ver formulada no alto escalão do processo decisório nacional. Uma das características diferenciadoras do relatório de Inteligência em relação a outros produtos de assessoramento do poder decisório é seu objetivo de ser o único documento a buscar o interesse coletivo da sociedade e do Estado brasileiros, sem apoiar ou atacar

pontos de vista sectários defendidos por grupos econômicos, partidários, filosóficos, ideológicos, religiosos, políticos, societários ou corporativos. Diferentemente, por exemplo, de editoriais de jornais, discursos de autoridades, artigos acadêmicos e teses jurídicas e econômicas, só o conteúdo de Inteligência tem como objetivo apresentar uma perspectiva de isenção em relação aos temas estratégicos nacionais. A imparcialidade como elemento de excelência do produto também sugere ao decisor que apenas o conteúdo de Inteligência é capaz de auxiliá-lo a identificar tentativas de ingerência adversa no processo decisório, como interferência externa ou contrapropaganda.

Conclusão

A Psicologia Cognitiva tem se valido de avanços no estudo da mente para tentar explicar como o homem captura e processa informações, faz julgamentos e toma decisões. À Inteligência Estratégica cabe aplicar esses estudos para o aprimoramento de sua atividade. Uma contribuição fundamental foi dada pela Ciência no século XX ao demonstrar que o homem é bem menos racional do que se imaginava. Vieses cognitivos, muitos deles ainda escassamente descritos, interferem em funções até há pouco tempo consideradas lógicas e racionais. É tarefa do profissional de Inteligência verificar em que medida esse fenômeno afeta o assessoramento prestado ao processo decisório nacional e como lidar com ele. No atual tempo de incertezas, as agências de Inteligência devem ser capazes de elaborar essa reflexão. Quão imparcial é meu produto? Quanto pode o mandatário confiar em meu trabalho? Como tratar um velho problema com novas ferramentas?

Erradicar os vieses cognitivos é impossível, mas seus efeitos sobre a imparcialidade do conteúdo de Inteligência podem ser minimizados. Diversos instrumentos de gestão têm potencial para contribuir com boas respostas se o risco for tratado de forma direta e sistemática. Inicialmente, é necessário conhecer esses vieses e a forma como interferem na produção do conhecimento. É necessário também que o profissional de Inteligência tome consciência de seu lugar no mundo – sua história pessoal, inserção social, formação educacional e profissional, inclinações ideológicas e preferências políticas e filosóficas – e entenda como isso afeta seu trabalho. Finalmente, cabe à agência empregar procedimentos para opor-se a danos potenciais dos vieses sobre o conteúdo de Inteligência, tanto na formação dos profissionais quanto na gestão do processo de que resultarão os conhecimentos. O resultado desse investimento contribui para que o produto final da agência permaneça útil e para que a Inteligência se torne imprescindível ao processo de tomada de decisões nacional.

Referências

AFONSO, Leonardo S. Considerações sobre a relação entre a Inteligência e seus usuários. *Revista Brasileira de Inteligência. Brasília*, v. 5, p. 7-19, out. 2009.

BRASIL – Gabinete de Segurança Institucional. Agência Brasileira de Inteligência. *Doutrina Nacional da Atividade de Inteligência:* fundamentos doutrinários. Aprovada pela Portaria nº 244 - ABIN/GSI/PR, de 23 de agosto de 2016. Brasília: Abin, 2016.

_____. *Planejamento Institucional ABIN 2017-2021; Revisão 2018*. Brasília: Abin, 2018.

DAVIES, Jack. *Improving Intelligence analysis at CIA:* Dick Heuer's contribution to Intelligence analysis. In: HEUER JR, Richards. Psychology of intelligence analysis. Washington: Central Intelligence Agency, 1999.

HERMAN, Michael. *Intelligence power in peace and war*. Cambridge: Cambridge University Press, 2006.

HEUER JR, Richards. *Psychology of intelligence analysis*. Washington: Central Intelligence Agency, 1999.

JONES, Lloyd. *Patterns of error perceptual and cognitive bias in intelligence analysis and decision-making*. Tese. Naval Postgraduate School, Monterey, 2005. Disponível em: <hdl.handle.net/10945/1774>. Acesso em: 21 de maio de 2018.

KAHNEMAN, Daniel. *Rápido e devagar:* duas formas de pensar. Rio de Janeiro: Objetiva, 2012.

KENT, Sherman. *Informações estratégicas*. Rio de Janeiro: Biblioteca do Exército Editora, 1967.

LOWENTHAL, Mark M. *Intelligence:* from secrets to policy. Washington: CQ Press, 2003.

MIRANDA FILHO, Fábio N. Ferramentas de interpretação de textos para uso da Inteligência. *Revista Brasileira de Inteligência*. Brasília, v. 11, p. 47-66, dez. 2016.

PLATT, Washington. *A produção de informações estratégicas*. Rio de Janeiro: Biblioteca do Exército Editora, 1974.

ROSITO, Guilherme A. Abordagem Fenomenológica e Metodologia de Produção de Conhecimentos. *Revista Brasileira de Inteligência*. Brasília, v. 3, p. 23-28, set. 2006.

SHULSKY, Abram N. SCHMITT, Gary J. *Silent warfare*. Understanding the world of

intelligence. Washington: Potomac Books, 2002.

TALEB, Nassim N. *A lógica do cisne negro.* Rio de Janeiro: Best Seller, 2008.

TEIXEIRA, Michelle M. S. Perfil do Profissional de Inteligência. *Revista Brasileira de Inteligência.* Brasília, v. 3, p. 29-43, set. 2006.

TVERSKY, Amos; KAHNEMAN, Daniel. *Julgamento sob incerteza:* heurísticas e vieses. In: KAHNEMAN (2012).

O IMPACTO DE *BIG DATA* NA ATIVIDADE DE INTELIGÊNCIA

Paulo M. M. R. Alves *

Resumo

A rápida evolução tecnológica implica a produção de um volume massivo de dados *(big data)*. Essa realidade impõe à atividade de Inteligência a necessidade de aprimoramento contínuo de seus métodos e processos. O artigo discute o impacto de *big data* na Inteligência e analisa três aspectos do mundo de *big data* que afetam o ambiente de trabalho dessa atividade: o excesso de informação, o incremento na capacidade de predição fornecida pelos algoritmos e os riscos democráticos ensejados pela prevalência desses algoritmos. Esses três aspectos são discutidos e apresentados como evidências da imprescindibilidade de apropriação das técnicas e ferramentas de *big data* para que a Inteligência cumpra com eficácia as atribuições que recebe da sociedade. A Política Nacional de Inteligência é invocada como balizador da atividade e o investimento em tecnologias aplicadas para tratamento e análise de grandes quantidades de dados está em consonância com os preceitos preconizados no documento.

Palavras-chaves: *big data*; análise de Inteligência; inteligência artificial; capacidade de predição.

BIG DATA IMPACT IN THE INTELLIGENCE ACTIVITY

Abstract

A massive volume of data (big data) is produced as a result of the rapid technological evolution. This reality imposes on the intelligence activity the need for continuous enhancement of its methods and processes. This article discusses the impact of big data in Intelligence and analyses three aspects of the big data world which affect the working environment of this activity: the information overload, the algorithms increased prediction capability and the risks to democracy sparked by the prevalence of theses algorithms. It also debates the balance between the usage of human resources and artificial intelligence. These aspects are discussed and presented as evidence of the essential need for a solid grasp of the big data tools and techniques by the intelligence community in order to effectively carry out the mandate it receives from the society. The National Intelligence Policy is invoked as a guiding parameter of the intelligence activity and the investment in technologies applied to the treatment and analysis of big data abide by the principles stated in that legal document.

Keywords: *big data; intelligence analysis; artificial Intelligence; prediction capability.*

* Oficial de Inteligência

Artigo recebido em julho/2018
Aprovado em setembro/2018

Introdução

A sociedade contemporânea vive na chamada Era da Informação, caracterizada por uma quantidade de dados disponíveis não apenas descomunal, mas ainda continuamente crescente. A esse grande volume de dados existente convencionou-se chamar *big data*[1]. Trata-se de uma nova e irreversível realidade tecnológica que afeta a sociedade e o Estado de inúmeras formas. Esse novo paradigma de abundância informacional impacta diretamente a atuação de serviços de Inteligência, que têm a razão de sua existência fundada na necessidade de informação que os Estados nacionais apresentam para fins de tomada de decisão.

Segundo Jean-Francois Rischard (2003 apud STEELE, 2008), os Estados nacionais são os maiores empreendimentos constituídos pelo homem. Gerir estas estruturas implica uma quantidade incessante de tomada de decisões. A Atividade de Inteligência tem, na sua gênese, o propósito primário de auxiliar o processo decisório. Quando um Estado procura conhecer estratégias e planos militares ou comerciais de outro Estado ou uma empresa espiona uma concorrente em busca de informações antecipadas sobre um novo produto, ambos têm um objetivo em comum: buscar informações privilegiadas que auxiliem a tomada de decisão. A Doutrina Nacional da Atividade de Inteligência (DNAI) afirma que a Inteligência se destina a assessorar a autoridade governamental, no sentido de permitir-lhe formular opções para a tomada de decisão. Para que a Inteligência exerça adequadamente sua atribuição de assessorar, produzindo conhecimentos úteis, confiáveis e oportunos é necessário um processo estruturado de produção de conhecimentos.

A sociedade contemporânea, no entanto, impõe novos desafios à produção de conhecimentos e ao assessoramento ao Processo Decisório Nacional (PDN). O macroambiente da Inteligência é indelevelmente marcado pela emergência da sociedade do conhecimento no contexto da Era da Informação. O mundo moderno amplia o papel da Inteligência ao mesmo tempo em que impõe o desafio de reavaliação contínua, como reconhece a Política Nacional de Inteligência (PNI):

> No mundo contemporâneo, a gestão dos negócios de Estado ocorre no curso de uma crescente evolução tecnológica, social e gerencial. [...] Nessas condições, amplia-se o papel da Inteligência no assessoramento ao processo decisório nacional e, simultaneamente, impõe-se aos profissionais dessa atividade o desafio de reavaliar, de forma ininterrupta, sua contribuição àquele processo no contexto da denominada "era da informação". (BRASIL, 2016)

O presente artigo pretende abordar, sob

1 Há diversas definições possíveis para o termo, algumas enfatizando a quantidade massiva de dados, outras enfatizando técnicas e ferramentas de análise desses dados. Neste artigo, demos preferência a primeira abordagem, adotando a definição dada pelo Dicionário de Oxford: "conjunto de dados extremamente amplo que podem ser analisados computacionalmente para revelar padrões, tendências e associações, especialmente relacionados ao comportamento e as interações humanas". Disponível em: <//en.oxforddictionaries.com/definition/big_data>. Acesso em: 15 Nov 2017. Sobre *big data*, ver o artigo de Gil Press *12 big data Definitions: What's Yours?*. Disponível em: <www.forbes.com/sites/gilpress/2014/09/03/12-big-data-definitions-whats-yours/>. Acesso em: 15 Nov 2017.

uma perspectiva multidisciplinar e no plano estratégico, três aspectos do cenário contemporâneo de *big data* que afetam decisivamente os ambientes interno e externo dos serviços de Inteligência. Esses aspectos constituem evidências do que se pretende demonstrar: a imprescindibilidade do domínio de técnicas e ferramentas de *big data* para a eficácia da atividade de Inteligência no mundo atual. Para este fim, emprega uma revisão bibliográfica que proporciona abundantes exemplos que ilustram o impacto de *big data* na atividade de Inteligência. O primeiro aspecto a ressaltar é o vertiginoso crescimento da quantidade de informações disponível, fenômeno que implica sobrecarga de informações *(information overload)* para o analista e para o decisor, afetando diretamente o processo decisório. Um segundo aspecto que impacta a Atividade de Inteligência é a possibilidade de utilizar a enorme massa de dados disponível para identificar padrões e, possivelmente, antecipar tendências. Por fim, outro aspecto merecedor de atenção é a capacidade que as novas tecnologias dão a um pequeno número de empresas e Estados de manipular opiniões e, potencialmente, populações inteiras em direção a determinada ideia ou sentimento.

Excesso de informação

Alvin Toffler, em seu livro A Terceira Onda (1980), alerta para o advento de um período pós-industrial, iniciado ainda nos anos de 1950, chamado de Era da Informação. Mas foi com o surgimento da *World Wide Web* (origem do famoso acrônimo "www"), agregando o hipertexto à rede, no início da década de 1990, que a internet começou a popularizar-se e efetivamente deixar os meios militares e acadêmicos para conectar o mundo. Também nessa década surgem os primeiros buscadores e indexadores de páginas web – como o Google, em 1998 –, um primeiro indício de aceleração no ritmo de crescimento da quantidade de informações.

Em meados da década de 2000, alguns autores acreditavam que o crescimento das fontes abertas (OSINT – *Open Source Intelligence*) iria facilitar o trabalho dos órgãos responsáveis pela atividade e traria uma significativa redução de custos (AFONSO, 2006). Já se vislumbrava, à época, que a inundação de dados gerada pela "democratização da informação"f e pela popularização das tecnologias da comunicação aumentaria a carga sobre decisores (FARIAS apud. AFONSO, 2006).

A sobrecarga de informação (TOFFLER, 1970) tem ocasionado dificuldades aos órgãos de Inteligência. Eles são, frequentemente, acusados de possuírem os dados e não serem capazes de fazer as correlações necessárias para prevenir uma ação adversa. Essa foi a tônica das críticas à comunidade de Inteligência americana após os atentados de 11 de Setembro de 2001 no *World Trade Center,* em Nova Iorque (AFONSO, 2006). Kissinger (2004) afirma que a causa da maior parte das falhas da Inteligência não se encontra na inadequação da coleta ou coordenação entre os órgãos, mas na etapa de avaliação *(assessment)* das informações.

Na França, uma comissão parlamentar estabelecida para examinar as falhas de Inteligência do país identificou que as agências estavam coletando informação,

mas não conseguiam "ligar os pontos" (SIMCOX, 2016). No Reino Unido, documentos vazados por Edward Snowden mostraram que os oficiais de Inteligência britânicos estavam preocupados com o excesso de informações (GALLAGHER, 2016). Em relatório secreto, advertiram que o MI5 era capaz de coletar mais dados do que era capaz de analisar e que isso poderia levar a graves falhas de Inteligência que poderiam, potencialmente, colocar vidas em risco. Um estudo ultrassecreto de 2009 vazado sobre o programa de vigilância eletrônica PRESTON, do GCHQ *(Government Communications Headquarters)* britânico, mostrou que, em um período de 6 meses, apenas 3% dos dados interceptados foram revisados pelas autoridades (GALLAGHER, 2016). O número chamou a atenção dos profissionais porque o PRESTON não é um programa de interceptação em massa, mas focado apenas em suspeitos conhecidos. Se boa parte das comunicações de alvos já identificados estava sendo ignorada, muita informação crucial estava sendo perdida.

Com efeito, a quantidade de dados disponíveis aumenta em taxas superiores ao crescimento demográfico humano. O universo digital dobra a cada dois anos (EMC, 2014). Postula-se, portanto, que nenhuma organização será capaz de lidar com esse incremento no volume de dados por meio da contratação de novos profissionais para processá-los. Um serviço de Inteligência, assim como qualquer outra organização, que tentasse semelhante expediente estaria fadado a tamanho inchaço de seus quadros que o tornaria ingerenciável. Ademais, restrições orçamentárias impõem limites evidentes a esse hipotético curso de ação.

Essa realidade apresenta um grande desafio para a Atividade de Inteligência. Por um lado, há mais dados disponíveis do que seus analistas são capazes de processar e transformar em conhecimento relevante. Por outro, não considerar o conjunto inteiro de dados torna o produto de Inteligência menos completo, por não considerar todas as possibilidades diante de um determinado problema. Gallagher (2016) lembra que, nesse contexto, há real possibilidade de que um serviço de Inteligência não perceba indícios de uma ameaça à segurança nacional, por exemplo.

A tendência ao crescimento do volume de dados não deve arrefecer nos próximos anos. Ao contrário, o advento da Internet das Coisas (IOT, sigla em inglês para *Internet of Things*) tende a aumentar drasticamente o número de dados brutos disponíveis. Os equipamentos eletrônicos modernos – televisores, câmeras de segurança, geladeiras, alarmes e outros – estão migrando para um paradigma de conectividade no qual todos se tornaram sensores, produzem dados e estão conectados na internet.

Se o crescimento da quantidade de dados tende a continuar, mas não é possível aumentar na mesma medida a capacidade de processamento humano desses dados e o não processamento leva a um conhecimento menos completo, como os serviços de Inteligência podem lidar com isso e SE manterem relevantes nesse mundo dominado pelo *big data?* O relatório vazado do MI5 oferece o caminho: pessoas, processos e tecnologia.

Primeiramente é necessário mudar o perfil do profissional de Inteligência (BESSA,

2003; AFONSO, 2006). Afastando-se do estereótipo da cinedramaturgia hollywoodiana, as agências de Inteligência devem procurar selecionar e/ou formar verdadeiros trabalhadores do conhecimento *(knowledge workers)*. É necessário que esse profissional trabalhe pautado por processos claros e bem definidos. Ele deve, desde o início de sua formação, estar inserido em um contexto de *big data,* no qual conhece as ferramentas disponíveis, sabe qual o seu papel na produção do conhecimento e segue uma metodologia apropriada para a Atividade de Inteligência.

Navegar pelas quantidades crescentes de dados, separar a informação dos ruídos que a acompanham e filtrar as frações significativas das irrelevantes têm se tornado um desafio cada vez maior para esses órgãos. A solução parece estar em mudar o paradigma de "o analista encontrar o dado" para "o dado encontrar o analista" (IBM, 2013). A análise automatizada de grandes volumes de dados *(Big Data Analytics)* potencializa a capacidade do profissional de Inteligência liberando-o de tarefas repetitivas e direcionando seu trabalho para áreas em que a intervenção intelectual humana é realmente essencial (IBM, 2013).

Antes de elaborar uma análise sobre determinada conjuntura política, por exemplo, o analista irá comumente dispender enorme quantidade de tempo reunindo material e separando o que considera significativo para o relatório a ser desenvolvido. Se ele puder treinar uma ferramenta de inteligência artificial (IA) para coletar das fontes corretas e filtrar a relevância segundo critérios definidos, o trabalho inicial de reunião e catalogação de material será feito de forma automatizada e quase instantânea. Dessa forma, o profissional de Inteligência poderá aplicar mais do seu tempo escasso na fase de análise, sem desperdiçá-lo com leituras de baixa relevância.

Segundo Jani (2016), o emprego de ferramentas de inteligência artificial pode trazer ao menos três benefícios ao trabalho analítico da comunidade de Inteligência:

- Automação da coleta de dados
- Redução do tempo de processamento na análise de estruturas de dados complexas
- Refinamento dos resultados para apresentar apenas os principais pontos que conduzam a uma tomada de decisão efetiva

Reconhecendo esses benefícios e percebendo a necessidade de ampliar a pesquisa e o desenvolvimento tecnológico voltado às necessidades específicas da comunidade de Inteligência, os Estados Unidos estabeleceram, em 2006, a IARPA *(Intelligence Advanced, Research Projects Activity)*. A instituição lidera ou financia projetos de pesquisas tecnológicas inovadoras que atendam às necessidades dos órgãos de Inteligência do país. Apresenta quatro principais focos de pesquisa:

- Análise: maximizar o discernimento dos grandes volumes de dados coletados de modo oportuno;
- Inteligência antecipatória: desenvolver tecnologias que reduzam

a incerteza e provejam aos tomadores de decisão predições acuradas de eventos relevantes para a segurança nacional;

• Coleta: aprimorar o valor dos dados coletados de todas as fontes; e

• Computação: segurança em ambientes hostis, detecção de ameaças e computação quântica.

Observando os campos de pesquisa acima, fica patente a alta prioridade que a IARPA confere à área de *big data*. Para a elaboração de uma conclusão razoável ou uma de predição confiável, faz-se necessário analisar o máximo possível de variáveis de um problema. Não é possível analisar todas essas variáveis se fontes de dados forem ignoradas em função da incapacidade de processamento.

No mundo moderno, o investimento mais relevante que uma agência de Inteligência pode fazer é justamente em Inteligência, contudo, em sua vertente artificial. Além de aumentar a capacidade de processar dados, esse investimento, em longo prazo, reduz custos e melhora o produto da Inteligência. A fração operacional, à guisa de exemplo, não precisa ser acionada em certas situações para confirmar dados que possam ser inferidos a partir da IA aplicada em mídias sociais. A fração analítica, por sua vez, não precisa perder tempo navegando por milhares de páginas da internet, fóruns ou plataformas de mídias sociais se a inteligência artificial conhece o interesse específico do analista e já filtra e apresenta apenas os resultados relevantes de acordo com o momento e o assunto.

Os profissionais de Inteligência que não contarem com esses instrumentos serão soterrados pela avalanche de dados produzidos pela Sociedade da Informação. As agências que ignorarem essa realidade arriscam-se a entregar produtos incompletos e, assim, perder relevância. O que o governo estadunidense percebeu, ainda em 2006, é algo que ficará cada vez mais evidente: não haverá Inteligência relevante sem ferramentas analíticas de *big data*.

Capacidade Preditiva

Um dos principais aspectos da Atividade de Inteligência que a torna relevante ao tomador de decisões é seu caráter preventivo (BESSA, 2004, p. 62). Fatos consumados são rapidamente divulgados pela imprensa e, ao governante, interessa saber os fatos antes que eles sejam de conhecimento público. A sociedade espera respostas rápidas de seus dirigentes. Atenta a essa realidade, a PNI estabelece o assessoramento oportuno como um dos pressupostos da atividade de Inteligência: "O trabalho da Inteligência deve permitir que o Estado, **de forma antecipada**, mobilize os esforços necessários para fazer frente às adversidades futuras e para identificar oportunidades à ação governamental". (BRASIL, 2016) (grifo nosso)

A DNAI (2016) estabelece quatro tipos de conhecimentos de Inteligência, a saber: informe, informação, apreciação e estimativa. Os dois primeiros referem-se a fatos pretéritos ou presentes e têm sua relevância vinculada à oportunidade e rapidez da difusão. Os dois últimos, por sua vez, voltam-se não apenas para fatos passados, mas para cenários e tendências

futuras. Para a autoridade tomar uma decisão, muitas vezes é fundamental a capacidade de antever os possíveis desdobramentos de determinada situação de interesse nacional. Para inferir tendências, a instrumentação matemática mostra-se bastante útil.

Em 1976, o demógrafo Emmanuel Todd, em sua obra *"La chute finale: Essais sur la décomposition de la sphère Soviétique"* [2] previu o colapso da União Soviética (URSS). Ciente de que os dados econômicos oficiais internos do país contavam com pouca confiabilidade, Todd utilizou em sua análise dados demográficos e de comércio exterior (mais facilmente verificáveis). Baseou seu estudo em dados como o crescimento da mortalidade infantil, importações de maquinários e exportações de materiais primários, número de automóveis, quantidade de indivíduos empregados no aparato estatal de segurança e índices de alfabetização. Comparou os dados levantados com os de outras nações comunistas da periferia soviética e percebeu que países como Alemanha Oriental, Tchecoslováquia e Hungria pareciam mais prósperos que a URSS.

Todd parte da premissa de que uma população que conta com alto índice de alfabetização (como a da URSS) é mais suscetível a revoltar-se em longo prazo caso não perceba melhorias substantivas na sua qualidade de vida. A pujança militar soviética, sua força política e o desenvolvimento em certos campos científicos encobriam anomalias estruturais de sua sociedade. Uma análise mais cuidadosa dos poucos dados confiáveis disponíveis daquele país permitia inferir uma deterioração da situação do país e da população. O demógrafo concluiu que a União Soviética, da forma como estava estruturada, era insustentável em longo prazo.

Verifica-se, contudo, a necessidade de adotar certos cuidados no emprego de instrumentos estatísticos. Suponha-se, por exemplo, um sistema de inteligência artificial com acesso à dados do Departamento de Agricultura dos Estados Unidos e da Fundação Nacional de Saúde, do mesmo país. Seus algoritmos poderão detectar uma forte vinculação (correlação de Pearson[3] de 95.86%) entre o número de títulos de doutorado em engenharia civil concedidos entre 2000 e 2009 e o consumo per capita de queijo mozarela no mesmo período (VIGEN, 2015), conforme mostrado na figura 1. Esse sistema poderia emitir as seguintes conclusões:

- Se há um aumento no consumo de queijo, mais doutores serão formados

- Se no próximo ano espera-se um número maior de doutorandos, os fazendeiros deveriam aumentar a produção.

2 Trad. de John Waggoner: *"The final fall: an essay on the decomposition of the Soviet sphere"* (1979).

3 Segundo Dicionário Estatístico de Cambridge como "um índice que quantifica a relação linear entre um par de variáveis" (EVERITT; SKRONDAL, 2010, trad. nossa).

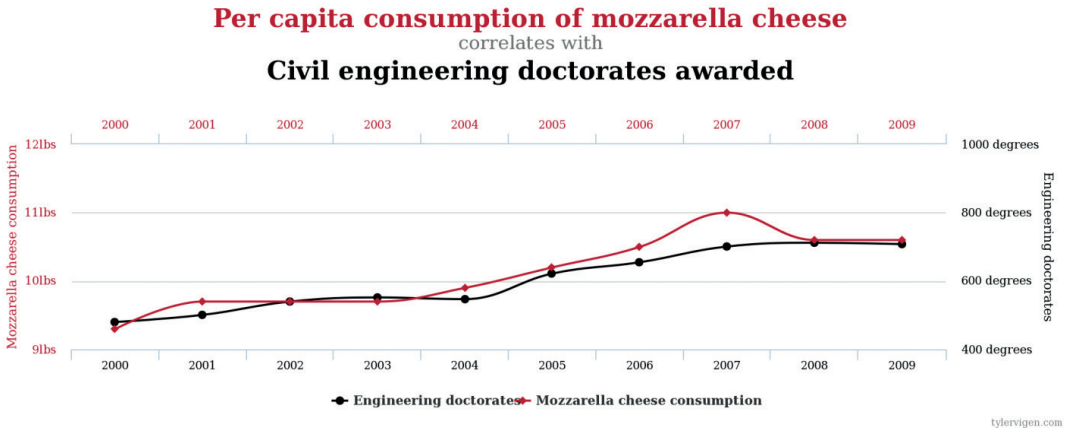


Figura 1 – correlação entre doutorados em engenharia civil e consumo de queijo mozarela (Fonte: www.tylervigen.com)

Um analista humano sensato perceberá, rapidamente, tratar-se de uma coincidência estatística. Uma máxima estatística preceitua que correlação não implica causalidade (CALUDE & LONGO, 2016, p. 05). Não se deve confundir simultaneidade com causalidade. Contudo, o fato de um sistema automatizado detectar essa correlação constitui um feito marcante, pois mostra a capacidade do sistema identificar padrões similares em uma grande massa de dados heterogêneos.

Alguns autores postulam que empregando poder de processamento suficiente em grandes volumes de dados, obtém-se considerável quantidade de correlações (FLETCHER, 2014; POPPELARS apud CALUDE & LONGO, 2016, p. 04-06). Correlações podem ser úteis por causa de seu potencial poder preditivo.

O investimento em análise por *big data* já é uma realidade no mundo da Inteligência estadunidense. Uma das quatro grandes linhas de pesquisa da IARPA, como mencionado anteriormente, é a Inteligência Antecipatória. Um de seus programas, o *Open Source Indicators* (OSI), financiou, a partir de 2012, o projeto EMBERS (Early Model Based Event Recognition using Surrogates). Esse sistema baseia-se em dados disponíveis publicamente para predição de eventos socialmente significativos na população, tais como protestos, focos de epidemias e resultados eleitorais (DOYLE et al, 2014, pg. 185).

O EMBERS foi modelado para permitir o emprego conjunto de cinco modelos preditivos distintos aplicados a fontes abertas de 10 países latino-americanos, a saber: Argentina, Brasil, Chile, Colômbia, Equador, El Salvador, México, Paraguai, Uruguai e Venezuela (RAMAKRISHNAN, 2014, p. 02-05). Iniciando em Novembro de 2012, o EMBERS gerava cerca de 50 predições diárias, enviando-as à IARPA em tempo real. Entre os principais resultados da pesquisa encontra-se a predição do crescimento e da posterior diminuição dos incidentes (eventos) relativos aos protestos populares de Junho de 2013 no Brasil e aos protestos estudantis de Fevereiro de 2014

na Venezuela (RAMAKRISHNAN, 2014, p. 14; DOYLE et al, 2014, p. 186). O artigo de Ramakrishnan (2014, p. 13-15) mostra que alguns modelos preditivos funcionam melhor em países com alto uso de mídias sociais (Brasil, Venezuela e México), como o Twitter, e no caso do Brasil, apresentou um tempo de antecipação[4] *(lead time)* médio de 11,82 dias.

Muitos analistas questionaram se teria sido possível prever a Primavera Árabe (RAMAKRISHNAN, 2014, p. 01) utilizando os dados abertos disponíveis. No ano de 2007, Courbage e Todd (2011) afirmam que as sociedades islâmicas estão em um processo de modernização evidenciado pelo aumento nas taxas de alfabetização. Os autores analisam ainda esse fator educacional em combinação com o papel das mulheres na sociedade e constatam quedas significativas nas taxas de fertilidade e tendências de natalidade nesses países. Concluem que as sociedades islâmicas se encontram em um caminho de modernização já trilhado pelas sociedades ocidentais desenvolvidas e que distúrbios sociais seriam consequências naturais desse processo.

Kalev Leetaru (2011), por sua vez, mostrou, em um estudo retrospectivo, que teria sido possível prever alguns eventos significativos para a Atividade de Inteligência utilizando ferramentas analíticas de *big data*. Foram utilizados como dados, mais de 30 anos de notícias traduzidas de serviços de monitoramento de fontes abertas do Reino Unido (SWB)[5] e dos Estados Unidos (FBIS)[6] . A pesquisa adotou uma abordagem focada no "tom[7] da notícia *(news tone)* e localização geográfica.

Quantificando o tom da notícia, Leetaru constatou que, no Egito, o tom negativo registrado em Janeiro de 2011 havia sido atingido, nos últimos 30 anos, apenas uma vez, por ocasião da Guerra do Golfo de 1991. Concluiu que essa elevada negatividade no tom das notícias seria indício de possível distúrbio social. Para Leetaru, essa Inteligência de fontes abertas funcionou melhor que a Inteligência de Estado, pois o presidente americano permaneceu apoiando o presidente egípcio Mubarak (BBC, 2011), que seria retirado do poder em pouco tempo. Resultados semelhantes foram encontrados para a Tunísia e para a Líbia (LEETARU, 2011). Analisando a Arábia Saudita, por outro lado, constatou que o tom negativo de Janeiro de 2011 já havia sido atingido diversas vezes nos últimos anos sem grandes perturbações sociais ou no sistema político, o que seria indicativo de maior estabilidade social e política. Com efeito, nesse último país, os impactos da Primavera Árabe foram inferiores aos de muitas outras nações da região.

Empregando as mesmas fontes, utilizando, porém, a dimensão geográfica das notícias,

4 Definida como a diferença entre a data que o evento é reportado pelos jornais (verificado por analistas humanos) e a data em que a previsão foi feita. Corresponde a ideia do número de dias pelos quais a predição "venceu a mídia" *(beat the news)* (RAMAKRISHNAN, 2014, p. 11).

5 *Summary of World Broadcasts*, da BBC.

6 Antigo *Foreign Broadcast Information Service*, atualmente *Open Source Center* da Agência Central de Inteligência (CIA)

7 Utiliza-se, mais comumente, a expressão "sentimento", ao invés de "tom".

Leetaru mapeou as citações a Osama Bin Laden nas notícias entre Janeiro de 1979 e Abril de 2011. Embora muitos acreditassem que o líder da Al Qaeda estivesse no Afeganistão (BBC, 2011), a análise de conteúdo de notícias proposta teria sugerido que Bin Laden estaria no norte do Paquistão, em um raio de 200 km envolvendo Islamabad e Peshawar – uma considerável redução de escopo, à época. Concluiu também que seria duas vezes mais provável que Bin Laden estivesse no Paquistão que no Afeganistão.

Ainda em relação à Primavera Árabe, pesquisadores do Centro de Combate ao Terrorismo de West Point e da Universidade de Princeton rastrearam, a partir de Janeiro de 2011, as pesquisas feitas no Google a partir do Egito e constataram que havia mais buscas por eventos relativos à Tunísia (estopim da Primavera Árabe) do que por estrelas de entretenimento egípcias (TEMPLE-RASTON, 2012). Também a partir de fontes abertas, a empresa Recorded Future previu, em janeiro de 2010, que uma combinação de enchentes, fome e terroristas islâmicos levaria o Iêmen ao desastre[8] (TEMPLE-RASTON, 2012).

Os exemplos de predições mencionados oferecem algumas lições para a atividade de Inteligência na era da Informação. Primeiramente, é preciso saber selecionar os dados relevantes de acordo com os objetivos da análise. Os dados de temperatura máxima e mínima em algum vilarejo dos montes Urais na Rússia, por exemplo, podem ter importância para algum estudo no campo da climatologia, mas não para o propósito do estudo de Todd que previu o colapso soviético. Também no mundo de *big data* é preciso saber filtrar os dados relevantes do ruído, isto é, separar as frações significativas da massa de dados irrelevantes que as acompanham.

Uma segunda lição diz respeito à importância do ser humano. A previsão da queda soviética foi possível porque um pesquisador humano selecionou as variáveis do problema (dados relevantes), estabeleceu premissas e critérios analíticos e inferiu conclusões a partir da análise dos dados coletados. Sistemas de inteligência artificial permitem o reconhecimento de padrões e tendências de forma mais rápida e a partir de uma quantidade consideravelmente maior de dados, contudo, se não for modelado corretamente por seu projetista, poderá levar a conclusões errôneas (como o exemplo anterior envolvendo o queijo mozzarela).

Tanto o homem quanto a máquina falham na tarefa preditiva. Por um lado, a inteligência artificial ainda não é capaz de interpretar com precisão a linguagem natural (FILHO, 2016). Também apresenta dificuldades em discernir coincidências estatísticas de outras correlações realmente significativas. Por outro lado, o ser humano possui capacidade limitada de coleta e armazenamento de dados. Afirmam Tetlock e Gardner (2016, p. 04) que a taxa humana de acerto em previsões de longo prazo é de 15% e seria, portanto, semelhante à de um chimpanzé arremessando dardos.

8 A Primavera árabe chega ao Iêmen em Janeiro de 2011. Disponível em: <www.bbc.com/news/world-middle-east-14704951>. Acesso em: 10 fe. 2018..

Para o diretor da IARPA, Jason Matheny, os melhores sistemas preditivos são aqueles que utilizam combinações homem-máquina (LAVINDER, 2016). Filho (2016) lembra que cumpre ao analista "estabelecer parâmetros corretos para que o *software* possa encontrar o padrão que mais interessa". Para Matheny, "o componente analítico humano é vital porque não há algoritmo que a máquina possa usar para predizer o comportamento humano" (LAVINDER, 2016). Portanto, na atividade de Inteligência, homem e máquina se complementam e se potencializam.

Convém observar também que os exemplos de predições mencionados cobrem temas particularmente relevantes para o PDN, como terrorismo, processo democrático e perturbações da ordem política e social. A PNI elenca entre suas ameaças o terrorismo e as ações contrárias ao Estado Democrático de Direito (BRASIL, 2016). Estabelece também como pressupostos da Atividade de Inteligência a abrangência e o assessoramento oportuno.

Para Bessa (2003, p.62), fornecer conhecimentos antecipados ao usuário é o mais importante papel da Inteligência. Segundo afirma Vidigal (2004, p. 14):

> [...] "para qualquer governo, é essencial a posse de informações que lhe permitam, no campo interno, identificar a existência de problemas que possam vir perturbar a ordem pública, a paz social ou prejudicar a economia, e, no campo externo, identificar as ameaças que possam se contrapor aos interesses nacionais".

Uma das possibilidades que a área de *big data* oferece e que a torna mais atrativa à Inteligência, portanto, consiste em utilizar a tecnologia para antecipar perturbações sociais e econômicas ou outras ameaças aos interesses nacionais. Uma correta combinação de recursos humanos e tecnológicos confere à atividade de Inteligência capacidade preditiva singular que a torna cada vez mais indispensável ao processo de tomada de decisões estratégicas.

Democracia em Risco

A Atividade de Inteligência deve permanecer atenta a ações, no ambiente cibernético, que possam obstar a consecução de interesses nacionais. Afirma a PNI que "os prejuízos das ações no espaço cibernético não advêm apenas do comprometimento de recursos da tecnologia da informação e comunicações. Decorrem, também, da manipulação de opiniões, mediante ações de propaganda ou de desinformação" (BRASIL, 2016). As primeiras ações, que comprometem diretamente os ativos tecnológicos, são mais facilmente observáveis e correspondem aos "ataques *hacker*" mais comuns. As últimas, no entanto, são mais sutis e envolvem o exercício de poder de influência e manobra sobre o conjunto da sociedade. Convém que a Inteligência de Estado compreenda como a área de *big data* atua nessa esfera de poder e como desenvolveu essa capacidade.

O norte-americano Norbert Wiener é creditado como o criador da cibernética (HELBING et al, 2017). O matemático mostrou, ainda na década de 1940, que o comportamento dos sistemas poderia ser controlado por meio de controles de retroalimentação *(feedbacks)* que corrigiriam as entradas (insumos) de um processo de

acordo com as saídas (resultados) obtidas. Logo pesquisadores começaram a imaginar que poderiam utilizar esse mesmo princípio para controlar a economia e a sociedade (HELBING et al, 2017).

À época de Wiener, a tecnologia digital ainda engatinhava e a internet e a conectividade não eram conceitos tão onipresentes na vida das pessoas. No mundo digital contemporâneo, estamos constantemente navegando online e quando o fazemos, nos deparamos continuamente com escolhas: o que comprar, o que ou quem seguir, o que ler, o que acreditar (CHATFIELD, 2016). Nesse contexto, as gigantes da economia digital parecem seguir o caminho de controle da sociedade previsto pelos pesquisadores do início da era cibernética. Google, Facebook, Amazon, Apple e Microsoft contam com uma gama de dados pessoais que permitem conhecer o que a pessoas querem, fazem, pensam ou sentem.

A esse respeito, um estudo apontou que os algoritmos têm melhor desempenho em uma tarefa cognitiva e social elementar: o julgamento de personalidades (YOUYOU et al, 2014). Utilizando como base questionários preenchidos por voluntários e por seus amigos e pessoas próximas e computando também o "rastro" digital (Likes do Facebook) dos voluntários, a pesquisa indica como uma de suas conclusões que as respostas previstas pelo algoritmo com base nos Likes do Facebook se aproximavam mais do auto-questionário que as respostas dos amigos. Por meio do Facebook, portanto, é possível saber mais sobre uma pessoa que seus conhecidos mais próximos.

O conhecimento que possui sobre os usuários é um dos principais insumos utilizados por Facebook, Google e outros gigantes tecnológicos para personalizar a experiência do usuário. A maioria das pessoas acredita que os resultados de pesquisa do Google são idênticos para qualquer internauta (PARISER, 2011, p. 01), mas Pariser (2011) lembra que duas pesquisas idênticas podem trazer resultados diferentes. Com efeito, a Google anunciou, em 4 de dezembro de 2009, que iria customizar os resultados das pesquisas em seu buscador (PARISER, 2011, p. 01). Isso implicou que os algoritmos da empresa começaram a fazer predições sobre quem o internauta é e que tipo de sites ele gostaria de ver e, em consequência, os resultados mostrados não mais seriam os considerados mais relevantes, mas sim os que o Google acreditava que haveria maiores chances de serem clicados pelo usuário (PARISER, 2011, p. 01).

Pariser (2011, p. 06) cunhou o termo "Bolha de Filtros" *(Filter Bubble)* para explicar como os algoritmos de personalização dos gigantes tecnológicos inserem os internautas em uma bolha de informações filtradas. Os serviços oferecidos por empresas como Google, Facebook, Amazon, Apple e Microsoft criam um universo único ("bolha") para cada indivíduo (PARISER, 2011, p. 06), no qual ele passa a ter acesso a notícias e informações que confirmam as opiniões e visões de mundo que já possui, tendo acesso limitado a conteúdos com opiniões diversas.

Como o filtro mostra informações baseadas em interesses pessoais e esconde

assuntos com os quais os indivíduos não tem familiaridade, as pessoas acabam aprendendo menos. Conforme Siva Vaidhuanathan (apud PARISER, 2011, p.91), "[...] o aprendizado é por definição um encontro com o que você não sabe, o que você não pensou, o que você não pôde conceber e o que você não entendeu ou acreditou ser possível"(trad. Nossa). Portanto, as pessoas mais educadas da era digital, isto é, aquelas que leem mais conteúdos fornecidos na "bolha", acabam, paradoxalmente, aprendendo menos, pois tem menos contato com informações previamente desconhecidas.

À época do Brexit (Plebiscito para decidir sobre a saída do Reino Unido da União Europeia), um usuário do Facebook explicou que teve muitas dificuldades para encontrar notícias sobre a vitória do "Deixo" no pleito. Identificando-o como partidário do "Fico", o sistema de notícias não permitia que ele visualizasse conteúdo da campanha vitoriosa do "Deixo" (NEJROTTI, 2016). Segundo Nejrotti (2016), "o Facebook está se tornando uma câmara de eco que nos previne de sermos confrontados por opiniões com as quais não concordamos". Dado que nos Estados Unidos, por exemplo, 62% das pessoas tem a rede de Mark Zuckerberg (fundador do Facebook) como uma das principais fontes de informação, os filtros do Facebook podem exercer considerável influência sobre a sociedade.

Richard Thaler, prêmio Nobel em Economia em 2017, introduz, juntamente com Cass Sunstein, o conceito de *"nudge"* [9] : "qualquer aspecto da arquitetura de escolhas que altera o comportamento das pessoas de maneira previsível sem proibir nenhuma opção nem mudar significativamente seus incentivos econômicos" (THALER; SUNSTEIN, 2009, p. 06). Em outras palavras, trata-se de um mecanismo de sugestão ("empurrão") que influencia a decisão do indivíduo.

Para exemplificar como pequenos "empurrões" podem influenciar decisões, o economista remete à pesquisa de Johnson e Goldstein (2003 apud. THALER; SUNSTEIN, 2009) acerca das decisões de doação de órgãos. Os pesquisadores comparam as abordagens de consentimento explícito (a pessoa precisa declarar por escrito o desejo de ser doador de órgãos) e consentimento presumido (a pessoa precisa declarar por escrito que não deseja doar). Países que adotam a primeira apresentam índices de doadores relativamente baixos, como Holanda (27,5% da população), Alemanha (12%) e Dinamarca (4,25%). Por outro lado, países que partem do pressuposto que todos são doadores salvo em caso de manifestação em contrário apresentam números significativamente mais favoráveis, como, por exemplo, Áustria (99,98%), França (99,91%), Portugal (99,64%) e Suécia (85,9%). Conclui-se que o simples fato de um governo adotar o consentimento presumido é uma medida que influencia positivamente o cadastro de doadores de órgãos. Governos e organizações podem apropriar-se do conceito de *"nudge"* para

9 O termo não possui uma tradução precisa para a língua portuguesa. A tradução brasileira (Elsevier Editora, 2009) do livro de Thaler e Sunstein utiliza os termos "empurrão", "cutucada" e "orientação". A tradução lusa (Academia do Livro, 2009), emprega os termos "estímulo", "empurrãozinho" e 'toque".

o interesse comum da sociedade ou para outros interesses espúrios.

A "Bolha de Filtros", caracteriza-se como um instrumento de *"nudging"*, pois trata-se de um mecanismo capaz de influenciar decisivamente as escolhas pessoais. Quanto maior a quantidade de decisões individuais influenciadas, maior a ingerência no conjunto da sociedade. Democracia e livre escolha, no entanto, são conceitos indissociáveis (ROSENFIELD, 2010). Quando a liberdade de escolha sofre alguma interferência, a própria democracia é abalada. A Inteligência de Estado deve estar atenta a essa questão, pois a PNI elenca as ações contrárias ao Estado Democrático de Direito como uma das ameaças que balizam as atividades do Sistema Brasileiro de Inteligência (Sisbin) (BRASIL, 2016).

No mundo digital, quanto mais se sabe sobre as pessoas, menos provável é que suas escolhas sejam livres (HELBING et al, 2017). Um experimento social conduzido na Índia, por ocasião das eleições para o Lok Sabha, a câmara baixa do Parlamento indiano, demonstrou a potencial influência que o Google pode ter sobre resultados eleitorais. Uma amostra de 2150 eleitores indecisos teve, no dia das eleições, a ordem dos 30 primeiros resultados de suas pesquisas no Google relativas às eleições alterada para favorecer um ou outro candidato. Essa simples mudança na ordem de apresentação dos resultados foi capaz de influenciar mais de 20%[10] dos indecisos em favor do candidato beneficiado pelo buscador (EPSTEIN; ROBERTSON, 2014, p. E4520). Para os pesquisadores, essa taxa pode ainda ser substancialmente melhorada se o experimento for realizado por semanas ou meses antes de um pleito.

Os resultados implicam que, se 80% dos votantes acessam a internet, e 10% deles forem indecisos, essa manipulação poderia levar cerca de 25% desses indecisos a apoiarem determinado candidato (EPSTEIN; ROBERTSON, 2014, p. E4520). Isso significa um ganho de 2% do eleitorado total. Como cerca de um quarto das eleições nacionais ao redor do mundo são ganhas por uma margem inferior a 3%, essa manipulação poderia impactar – ou, talvez, já esteja impactando – resultados de votações em diversos países (EPSTEIN; ROBERTSON, 2014, p. E4519-E4520).

O Brasil também têm sido palco da crescente influência das novas tecnologias no processo democrático. Ferramentas de *big data* nas mídias sociais têm sido cada vez mais empregadas em diversos eventos de porte nacional (como eleições ou protestos), conforme apontam estudos da Universidade de Oxford (ARNAUDO, 2017) e da Fundação Getúlio Vargas (RUEDIGER, 2017). Essa realidade começou a se tornar evidente na disputa presidencial de 2014, marcada por crescente acirramento político e que teve aproximadamente 11% das discussões no Twitter geradas por robôs *(bots)*. Na greve geral de 28 de Abril de 2017, esse percentual subiu para cerca de 20%.

Também significativo é o exemplo do uso de *fake news* (notícias falsas) na eleição presidencial americana de 2016.

10 Essa taxa foi chamada pelos pesquisadores de Poder de Manipulação de Voto.

Representantes do partido Democrata, da candidata derrotada Hillary Clinton, realizaram investigação nas redes sociais e alegam ter encontrado evidências de que as *fake news* disseminadas contra a candidata conseguiram mudar a posição de eleitores indecisos (CALABRESI, 2017). Relatório do governo americano indica que a Rússia empreendeu uma campanha multifacetada de propaganda e influência, com notório emprego de mídias sociais e atividades cibernéticas (DIRECTOR OF NATIONAL INTELLIGENCE, 2017). James Clapper, ex-Diretor de Inteligência Nacional (DNI), afirma que o episódio da campanha russa constitui ameaça à própria fundação do sistema político e democrático (CALABRESI, 2017).

O episódio da eleição americana demonstra o emprego intensivo de espionagem interestatal entre grandes atores do cenário político mundial. A prática não é nova, contudo ganhou contornos massivos com o crescimento da inteligência cibernética. Edward Snowden[11] já havia apresentado ao mundo os programas PRISM, XKeyscore, Fairview e outros empregados pela estrutura de Inteligência estadunidense na interceptação massiva das telecomunicações mundiais. Os documentos vazados por Snowden também mostram que o governo estadunidense havia espionado comunicações da Petrobrás, do Ministro das Minas e Energia e da própria Presidente da República (REVELATIONS, 2018). O conhecimento antecipado de planos e intenções das maiores autoridades e da maior empresa nacional confere a seu detentor vantagem estratégica considerável em negociações comerciais, diplomáticas ou políticas.

A PNI alerta para a ameaça das Ações Contrárias à Soberania Nacional, definindo-as como aquelas "que atentam contra a autodeterminação, a não-ingerência nos assuntos internos e o respeito incondicional à Constituição e às leis" (BRASIL, 2016). Elenca também entre as ameaças a Interferência Externa, entendida como "a atuação deliberada de governos, grupos de interesse, pessoas físicas ou jurídicas que possam influenciar os rumos políticos do País com o objetivo de favorecer interesses estrangeiros em detrimento dos nacionais" (BRASIL, 2016). Cita ainda como ameaças os Ataques Cibernéticos e as Ações Contrárias ao Estado Democrático de Direito (BRASIL, 2016). Entre as diretrizes da PNI está a determinação de "expandir a capacidade operacional da Inteligência no espaço cibernético", em cujo domínio torna-se "primordial acompanhar, avaliar tendências, prevenir e evitar ações prejudiciais à consecução dos objetivos nacionais" (BRASIL, 2016).

Analisando o balizamento fornecido pela PNI em conjunto com os exemplos anteriores, percebe-se a necessidade premente de investimento da Inteligência nacional em suas capacidades na área de *big data*, sob o risco de deixar o país à mercê de agentes adversos ao interesse nacional. A incapacidade de interagir nesse ambiente tecnológico e avaliar de modo preciso suas ameaças ensejam riscos aos valores

11 Edward Snowden é um ex-funcionário terceirizado da NSA que, em 2013, gravou grande quantidade de dados sobre os programas de interceptação daquela organização e tornou-se delator, entregando os dados para publicação por alguns jornalistas escolhidos.

democráticos e à autodeterminação do país.

Considerações Finais

A Era da Informação, caracterizada pelo constante incremento da quantidade de dados produzidos, está transformando o mundo. Indivíduos, organizações e nações precisam adaptar-se a esse novo paradigma tecnológico. Como observa a PNI, esse cenário de célere evolução amplia o papel da Inteligência e impõe aos seus profissionais uma constante reavaliação de sua contribuição. O domínio das técnicas e ferramentas de *big data* é essencial para que a Inteligência cumpra o que a sociedade espera dela, conforme os preceitos preconizados pela PNI.

Organizações e Estados com maior expertise na área de *big data* podem interferir decisivamente nos rumos de uma sociedade, muitas vezes em detrimento dos interesses nacionais. Para poder controlar seu destino, o país precisa ser capaz de avaliar as ameaças que o ambiente tecnológico enseja. Acompanhar e avaliar as conjunturas interna e externa, assessorando o processo decisório nacional e a ação governamental é um dos objetivos da Inteligência nacional (BRASIL, 2016).

Essa tarefa analítica, no entanto, é dificultada pela quantidade de dados disponíveis ao profissional de Inteligência. O emprego de ferramentas de IA na coleta e análise de dados auxilia grandemente o analista a compreender a complexidade crescente do mundo contemporâneo. Proporciona também capacidade preditiva que torna a Inteligência não apenas desejável, mas também essencial à estratégia nacional.

Dominando as ferramentas de *big data,* a atividade de Inteligência tem seu papel e importância amplificados no assessoramento oportuno do processo decisório. O conhecimento preciso, antecipado e, por vezes, preditivo proporciona vantagem competitiva ao país e permite reposicioná-lo no quadro das relações de poder do cenário mundial.

No mundo contemporâneo, tornaram-se essenciais aos órgãos de Inteligência o manejo adequado de ferramentas e tecnologias, a formação de profissionais capacitados e uma mudança de cultura institucional que permita que o analista tenha a percepção holística de que os cenários de Inteligência com que trabalha são também ambientes de *big data*. Para acompanhar a celeridade da evolução tecnológica, a atividade de Inteligência precisa estar continuamente se reinventando.

Os órgãos de Inteligência se deparam, portanto, com um desafio tecnológico que oferece riscos e oportunidades. Por um lado, aqueles que ignorarem a realidade de *big data* e continuarem a trabalhar exclusivamente com fontes humanas, como se ainda operassem nos tempos da Guerra Fria, se arriscam a apresentar um produto final anacrônico, incompleto e, quiçá, irrelevante. Por outro lado, os órgãos de Inteligência que se apropriarem do poder das ferramentas de *big data* podem se tornar imprescindíveis ao processo decisório e, dessa forma, participar da construção histórica de uma nação mais forte e soberana.

Referências

AFONSO, Leonardo S. Fontes abertas e Inteligência de Estado. *Revista Brasileira de Inteligência. Brasília,* DF, v. 2, n. 2, p. 49-62, abr. 2006.

ARNAUDO, Dan. *Computational Propaganda in Brazil: Social Bots during Elections.* Oxford: Eds. Working Paper. 2017.

BBC. *Supercomputer predicts revolution, 2011. Disponível em: <www.bbc.com/news/technology-14841018>. Acesso em: 15 nov. 2017*

BESSA, Jorge da S. A importância da Inteligência no processo decisório. In: *ENCONTRO DE ESTUDOS:* Desafios para a atividade de Inteligência no século XXI, 3., 2004. Brasília. *Anais* ... Brasília: Secretaria de Acompanhamento e Estudos Institucionais, 2004, p. 51-71

BIG DATA. English Oxford Living Dictionary. Disponível em: <en.oxforddictionaries.com/definition/big_data>. Acessado em: 28 abr. 2018.

BRASIL. *Decreto Nº 8.793, de 29 de junho de 2016*. Fixa a Política Nacional de Inteligência. Brasília, 2016. Disponível em: <www.planalto.gov.br/cciviL_03/_Ato2015-2018/2016/Decreto/D8793.htm> Acesso em: 10 fev. 2018.

CALABRESI, Massimo. *Inside Russia's Social Media War on America*. Disponível em: < time.com/ 4783932/inside-russia-social-media-war-america/>. Acesso em: 15 nov. 2017.

CALUDE, Cristian S.; LONGO, Giuseppe. *The Deluge of Spurious Correlations in big data. Foundations of Science*, [S.l.], v. 22, n. 3, p. 595-612, set. 2017.

CHATFIELD, Tom. *The invisible ways Facebook is affecting our choices*. Disponível em: <www.bbc.com/future/story/20160523-the-invisible-ways-facebook-is-affecting-our-choices>. Acesso em 15 nov. 2017.

COURBAGE, Youssef; TODD, Emmanuel. *A Convergence of Civilizations: The Transformation of Muslim Societies Around the World.* Translated by George Holoch Jr. 1 Ed. [S.l.]: Columbia University Press, 2011. 160 p.

DOYLE, Andy et al. Forecasting Significant Societal Events Using The Embers Streaming Predictive Analytics System. *big data*, [S.l.], v. 2, n. 4, p. 185-195, dez. 2014.

DIRECTOR OF NATIONAL INTELLIGENCE. *Assessing Russian Activities and Intentions in Recent US Elections.* [S.I.: s.n.], 2017.

DOUTRINA NACIONAL DE INTELIGÊNCIA: Fundamentos Doutrinários. Brasília: ABIN, 2016.

EMC. The Digital Universe of Opportunities: Rich Data and the Increasing Value of the Internet of Things, 2014. Disponível em: <www.emc.com/leadership/digital-universe/2014iview/executive-summary.htm>. Acesso em: 15 nov. 2017.

EPSTEIN, Robert; ROBERTSON, Ronald. The search engine manipulation effect (SEME) and its possible impact on the outcomes of elections. PNAS, [S.I.], v. 112, n. 33, p. E4512-E4521, 04 ago. 2015.

FILHO, Fábio N. de M. Ferramenta de interpretação de textos para o uso da Inteligência. *Revista Brasileira de Inteligência*. Brasília, n. 11, p. 47-66, dez. 2016.

FLETCHER, James. Spurious correlations: *Margarine linked to divorce?* Disponível em: <www.bbc.com/news/magazine-27537142>. Acesso em 15 nov. 2017.

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

HELBING, Dirk. *Will Democracy Survive big data and Artificial Intelligence?*. Scientific American, 2017. Disponível em: <www.scientificamerican.com/article/will-democracy-survive-big-data-and-artificial-intelligence/>. Acesso em: 15 nov. 2017.

IBM. Big data for the intelligence community. Sommers: [s.n.], 2013.

JANI, Karan. The Promise and Prejudice of *big data* in Intelligence Community. Atlanta: [s.n.], 2016.

JOHNSON, Eric J.; GOLDSTEIN, Daniel. Do Defaults Save Lives? In: Science, New York, v. 302, p. 1338-1339, 21 nov. 2003.

KISSINGER, Henry A. Better Intelligence reform: Lessons from four major failures. In: *The Washington Post*, ago. 2004.

LAVINDER, Kaitlin. *IARPA Director on Forecasting: Human-Machine Pairs Work Best.* Disponível em: <www.thecipherbrief.com/iarpa-director-on-forecasting-human-machine-pairs-work-best>. Acesso em: 15 nov. 2017.

LEETARU, Kalev H. Culturomics 2.0: Forecasting large–scale human behavior using global news media tone in time and space. *First Monday*, [S.l.], v. 16, n. 9, set. 2011. Disponível em: <firstmonday.org/article/view/3663/3040>. Acesso em 15 nov. 2017.

NEJROTTI, Federico. *A bolha de filtros do Facebook está deixando você cada vez mais burro*. Disponível em: <motherboard.vice.com/pt_br/article/nz38y8/a-bolha-de-filtros-do-facebook-esta-piorando>. Acesso: 15 nov. 2017.

PARISER, Eli. *The Filter Bubble*: How the new personalized Web is changing what we read and how we think. New York: The Penguin Press, 2011.

PRESS, Gil. *12 big data Definitions: What's Yours?, 2014*. Disponível em: <www.forbes.com/sites/gilpress/2014/09/03/12-big-data-definitions-whats-yours/>. Acesso em: 15 nov 2017.

RAMAKRISHNAN, Naren et al. "Beating the news" with EMBERS: forecasting civil unrest using open source indicators. In: *Proceedings of the 20th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, 20, 2014. New York. Anais… [s.l.]: ACM, 2014. p. 1799–1808.

REVELATIONS. In: Courage Snowden. Disponível em: <edwardsnowden.com/revelations>. Acesso em: 27 abr. 2017.

ROSENFIELD, Denis. Democracia e Liberdade de Escolha. Revista Opinião Filosófica, n. 01, v.1, 2010.

RUEDIGER, Marco A. Robôs, redes sociais e política no Brasil. Estudo sobre interferências ilegítimas no debate público na web, riscos à democracia e processo eleitoral de 2018. Rio de Janeiro: FGV, DAPP, 2017.

SIMCOX, Robin. *French Intelligence reform* - the counterterrorism commission won't prevent the next attack. Foreign Affairs, 17/07/2016. Disponível em: <www.foreignaffairs.com/articles/france/ 2016-07-17/french-intelligence-reform>. Acesso em: 04 nov. 2017.

STEELE, Robert. World Brain as EarthGame, 2014. Disponível em: <phibetaiota.net/2008/10/2008-world-brain-as-earthgame-full-text-online-for-google-translate/>. Acesso em: 15 nov. 2017.

THALER, Richard H.; SUNSTEIN, Cass R. *Nudge - O Empurrão para a Escolha Certa:* Aprimore suas Decisões sobre Riqueza, Saúde e Felicidade. Trad. de Marcello Lino. Rio

de Janeiro: Elsevier, 2009. 313 p.

TEMPLE-RASTON, Dina. *Predicting the future: fantasy or a good algorithm?* Disponível em: <www.npr.org/2012/10/08/162397787/predicting-the-future-fantasy-or-a-good-algorithm>. Acesso em: 15 nov. 2017.

TETLOCK, P. E.; GARDNER, D. *Superprevisões:* a arte e a ciência de antecipar o futuro. Rio de Janeiro: Objetiva, 2016. 352 p.

TODD, Emmanuel. *The final fall*: an essay on the decomposition of the Soviet sphere. New York: Karz Publishers, 1979. 236 p.

TOFFLER, Alvin. *A terceira onda*. Trad. João Távora. 8. ed. Rio de Janeiro: Record, 1980.

TOFFLER, Alvin. *Choque do futuro*. Trad. Eduardo Francisco Alves. 3 ed. Rio de Janeiro: Record, 1970.

VIDIGAL, Armando A. F. Inteligência e Interesses Nacionais. In: *ENCONTRO DE ESTUDOS*: Desafios para a atividade de Inteligência no século XXI, 3., 2004. Brasília. *Anais*... Brasília: Secretaria de Acompanhamento e Estudos Institucionais, 2004, p. 05-50.

VIGEN, Tyler. Spurious Correlations. Disponível em: <www.tylervigen.com/spurious-correlations>. Acesso: 15 nov. 2017.

YOUYOU Wu; KOSINSKIB, Michal; STILLWELLA, David. Computer-based personality judgments are more accurate than those made by humans. PNAS, [s.l], v. 112, n. 04, p. 1036-1040, 27 jan. 2015.

AMBIENTES COMPLEXOS E A SUPERAÇÃO DA GESTÃO POR COMANDO E CONTROLE NAS OPERAÇÕES DE INTELIGÊNCIA

Marcelo Furtado M. Paula *

Resumo

A gestão baseada em comando e controle pressupõe o exercício de direção centralizada, com pouca liberdade criativa e decisória para as equipes. Inspirada em modelos gerenciais de princípios do século passado, como o taylorismo e o fordismo, tende a ser pouco efetiva em cenários complexos, caracterizados pela multiplicidade de conexões entre os atores, imprevisibilidade e mudanças constantes. Nesses cenários, planejamentos minuciosos de tarefas são contraproducentes porque variáveis inopinadas alteram, inexoravelmente, as condições que os baseiam. Por meio de uma revisão de literatura, esse trabalho objetiva apresentar instrumentos de gestão que rompam com a estrutura de comando e controle e aportem contribuições significativas ao gerenciamento da Atividade de Inteligência. Esses modelos privilegiam a adaptabilidade e a resiliência, entregando poder de decisão aos executores e alterando a função das lideranças. Os gerentes passam a ser responsáveis por melhorar as relações entre as equipes e seus canais de comunicação, em lugar de planejar tarefas. Equipes de alto desempenho tornam-se a essência das organizações e articulam-se em rede, superando as ligações verticais.

Palavras-chaves: Gestão, Inteligência, Comando e Controle

COMPLEX ENVIRONMENTS AND THE OVERCOMING OF COMMAND-AND-CONTROL MANAGEMENT IN INTELLIGENCE OPERATIONS

Abstract

Command-and-control management demands a centralized organizational structure, restricting teams' creativity and decision power. Developed from last century's managements frameworks, like Taylorism and Fordism, tends to be less effective in complex environments, usually featured by multiple connections between its actors, unpredictability and constant change. In these scenarios, thorough task planning is inefficient because unexpected variables change the underlying basis of the panning. Through a brief literature review, this paper intends to show management tools that break the command-and-control structure and enhance the Intelligence managerial competence. These models rely on adaptability and resilience, delivering decision power to the operational level and shifting the leadership's role. Managers turn responsible of improving liaisons between teams, instead of planning tasks. High performance teams become the organization's building block and operate as networks, overcoming the vertical structure.

Keywords: *Management, Intelligence, Command and Control.*

* Oficial de Inteligência

Artigo recebido em julho/2018
Aprovado em setembro/2018

Introdução

Ao longo do século XX, agências de Inteligência se estruturaram em modelos de gestão baseados em comando e controle que conformaram seus desenhos institucionais e cultura organizacional (McCHRYSTAL, 2015; RUBIN, 2013; SUTHERLAND, 2016). É o caso, por exemplo, do Serviço Nacional de Informações (SNI), da *Central Intelligence Agency* (CIA) e do Comitê de Segurança do Estado (KGB). Pela definição do Departamento de Defesa norte-americano (EUA, 2017), "Comando e Controle" é o "exercício de autoridade e direção, no cumprimento da missão, por um comandante devidamente designado sobre as forças que lhe estão atribuídas e associadas" (tradução). Segundo McChrystal (2015), esse modelo sofreu influência da *administração científica* de taylorismo e do fordismo[1], teorias que revolucionaram a indústria na primeira metade do século passado.

O gerenciamento conformado nessa maneira de pensar demanda planejamento minucioso e objetiva ganhos de eficiência. No caso das agências de Inteligência brasileiras, essa cultura gerencial se manifesta, por exemplo,na maneira criteriosa com que as Operações de Inteligência são planejadas de forma a garantir o cumprimento da missão e a proteção das identidades do órgão e de seu pessoal, com o mínimo de custo e risco.

Ocorre que as Operações de Inteligência estão geralmente inseridas em cenário complexo, caracterizado por mudanças constantes e existência de variáveis significativas desconhecidas e independentes. Com o avanço das tecnologias de informação, esse cenário se torna ainda mais líquido[2]. Como afirma Clark (2010), o alvo de inteligência típico não é mais um indivíduo, fato ou instalação, mas um sistema em rede complexo.

Além disso, as demandas das frações analíticas estão sujeitas a mudanças constantes. Novos dados obtidos, alterações de cenário, mudanças no interesse do decisor e a própria dinâmica dos alvos interferem nas demandas a serem atendidas. O modelo analítico pode mesmo alterar-se com tudo mais constante, resultado de novas percepções do analista. Segundo Clark (2010, p. 31-32), "não há definição conclusiva de problema na Inteligência. (...) Na medida em que o usuário de Inteligência aprende mais sobre os alvos, as suas necessidades e interesses mudarão" (tradução nossa). Tampouco é recente a percepção dos impactos contraproducentes da especialização e, já em 1949, Sherman Kent (2015, p. 109) criticava o modelo fordista[3] de produção do conhecimento, destacando a necessidade de profissionais que, além de qualificados, tenham visão do todo. A especialização e a compartimentação,

1 Para uma introdução a respeito do tema e os impactos da organização do trabalho taylorista e fordista na sociedade do século XX e sua superação, ver HARVEY, 2008.

2 Bauman (2001) afirma que vivemos em tempos líquidos, em que nada foi feito para durar. Segundo o autor, as relações sociais foram modificadas na modernidade, tornando-se líquidas, fluidas, inconstantes e não duradouras. Isso se deve, particularmente, às novas tecnologias, ao individualismo e ao consumismo. Retomamos a ideia de "cenário líquido" com o objetivo de reforçar a noção de mudança e inconstância.

3 Embora não utilize o termo, as características do modelo criticado por Kent são eminentemente fordistas.

claro está, favorece a profundidade de conhecimento, mas, no limite, provocam viés de cognição e déficit de informações.

A partir dessas ideias, este ensaio realiza uma revisão de literatura que avalia a atualidade do gerenciamento baseado em comando e controle na Atividade de Inteligência. Objetiva-se apresentar técnicas contemporâneas de gestão[4] crescentemente aplicadas na indústria, com efeitos observáveis de ganho de tempo e qualidade, e que podem ser absorvidas pela gestão pública em proveito do desempenho de suas instituições. Para isso, apresentam-se os conceitos de ambientes complicado e complexo, buscando identificar, para esse último, métodos gerenciais que superem o comando e controle. Pretende-se demonstrar que métodos que proporcionam resiliência às organizações e que permitam planejar em contexto complexo, com adequação dos níveis de tomada de decisão e construir equipes de alto desempenho atendem primorosamente as Operações de Inteligência.

Comando e Controle

Como observado na introdução, a cultura gerencial taylorista e fordista inspirou a estruturação de organizações em geral, e agências de Inteligência em particular - como é o caso do antigo Serviço Nacional de Informações (SNI) -, no modelo de "comando e controle". Nesse paradigma, o responsável pelas ações operacionais exerce controle sistemático das atividades, avalia seus resultados e verifica se são desenvolvidas conforme o planejamento (ESNI, s. d.).

McChrystal (2015, p. 47) demonstra que a estrutura das organizações é, tradicionalmente, uma combinação de colunas verticais (departamentos ou divisões) e escalões horizontais que denotam níveis de autoridade. Nesse desenho, o mais poderoso fica no topo, e é o único escalão capaz de acessar e controlar todas as colunas. Segundo o autor (2015, p. 96), em um comando, o líder distribui tarefas entre as unidades subordinadas. Essas não precisam conhecer suas contrapartes. No comando, as conexões são ligações verticais: uma unidade comunica-se com seu superior e seus inferiores, sem vínculos laterais.

Contudo, como observa Sabbagh (2013, p. 33), "abordagens tradicionais de gestão com comando e controle não são eficientes nesses contextos de mudança e imprevisibilidade". Exigem ainda grande quantidade de requisitos escritos que, como critica Sutherland (2016), são geralmente inúteis.

Clark (2010, p. 13-15) defende que a Inteligência atue como processo em rede, social, com todos os participantes focados no objetivo. Se as partes interessadas compartilharem informações de forma sistemática ou como processo dinâmico de gestão do caso ou conhecimento, terão melhores condições de identificar lacunas em seu conhecimento e compreender as questões que o rodeiam.

4 Particularmente aquelas inspiradas no Manifesto para o Desenvolvimento Ágil de *Software* (Beck *et al.*, 2001).

Um gerenciamento da Atividade de Inteligência que rompa com o modelo de comando e controle e se baseie na interação entre as partes interessadas, seja iterativo (no sentido de repetir-se recorrentemente) e estruturado para incorporar a mudança (no lugar de ater-se a um plano detalhado), contorna as dificuldades causadas pela complexidade do ambiente e tende a ganhar em agilidade. Como resultado, espera-se reduzir custos, prazos e riscos, além de atingir resultados melhores.

Em lugar das ligações verticais do modelo de comando e controle, autores como Sutherland (2016) e McChrystal (2015) sugerem a estruturação de conectividades horizontais – ou seja, potencializar as ligações entre unidades situadas no mesmo nível hierárquico. Isso é muito diferente daquilo que comumente se observa nas organizações contemporâneas. As conectividades horizontais desafiam a noção de autoridade e chefia, centrais no paradigma de comando e controle.

Complicado e Complexo

As mudanças tecnológicas das últimas décadas, particularmente relacionadas ao dinamismo da informação, tornou o mundo mais interdependente e acelerado. Milton Santos (1993) atribui essa fluidez ao que chamou de tirania do mercado, enquanto Susan Strange (1998) argumenta que a aceleração da globalização provocou o enfraquecimento do poder político dos Estados. Esse fenômeno altera o ambiente em que estão inseridas empresas e organizações governamentais, criando um estado de *complexidade*.

McChrystal (2015, p. 57) conceitua coisas complicadas como aquelas constituídas por muitas partes, embora essas estejam ligadas umas às outras de formas relativamente simples. Exemplo de estrutura complicada são os motores de combustão interna. Não obstante suas muitas peças sejam de difícil compreensão, seu funcionamento pode, em última instância, ser dividido em uma série de relações simples, coerentes e determinísticas.

Para o autor, as coisas são complexas quando o número de interações entre seus componentes é significativamente grande. Em razão dessa densidade de ligações, sistemas complexos variam muito, no sentido de serem instáveis, e por isso apresentam imprevisibilidade acentuada. Na mesma linha, Rubin (2013) conceitua "domínio complexo" como uma situação em que as coisas são mais imprevisíveis do que previsíveis. Respostas ou decisões corretas, se é que existem, são percebidas com pouca ou nenhuma antecedência.

A cultura organizacional inspirada em taylorismo e no fordismo é altamente eficiente para trabalhar com problemas complicados, em processos conhecidos e replicáveis em escala. (McCHRYSTAL, 2015; SABBAGH, 2013). Nessa tradição, admite-se que qualquer problema pode ser conhecido em sua totalidade.

Contudo, no estado de *complexidade* não há entidade capaz de monitorar a quantidade de eventos que ocorrem simultaneamente. A realidade estrutura-se em rede, assemelhando-se mais a um organismo vivo ou ecossistema do que aos sistemas lineares de Taylor (McCHRYSTAL, 2015, p. 71).

Soluções complicadas não funcionam para problemas complexos. Exemplos dessa inadequação podem ser observados em diversos contextos. No campo militar, a Força Tarefa Conjunta de Operações Especiais norte-americana no Iraque de 2003 a 2008, para fazer frente à Al Qaeda – que se estruturava como uma rede – transformou-se de estrutura complicada para complexa (McCHRYSTAL, 2015).

O campo econômico fornece outro exemplo clássico: a União Soviética apresentava uma economia dinâmica e robusta baseada em modelos *fordistas* de produção até meados da década de 1970, mas não se adaptou às rápidas mudanças que o mundo observava, ao passo que o *sistema Toyota de produção* indicava ao ocidente o caminho para fazê-lo (SEGRILLO, 2000).

Por fim, no Brasil, a segurança pública se organiza em instituições e escalões especializados, com baixa interação e pouca confiança nas suas relações, para enfrentar um problema complexo em rede que é o crime organizado.

Em contextos muito complexos, planejamentos minuciosos são geralmente irrelevantes, não importa quão engenhosos seus desenhos iniciais (McCHRYSTAL, 2015, p. 69). Isso se deve ao fato de que modelos de gestão baseados em planejamento (comando e controle) necessitam de previsibilidade, o que não é possível em ambientes complexos. As mudanças, inexoráveis e rápidas nesse ambiente, tornam a ancoragem a planos determinados custosa, ineficiente e arriscada. Em última instância, diminuem a probabilidade de se alcançarem os objetivos estabelecidos.

Independentemente dessa complexidade contemporânea, a Atividade de Inteligência desenvolve-se, desde sempre, em ambientes onde a imprevisibilidade é a regra e a mudança é constante. Os alvos atuam como variáveis independentes, sobre as quais não é possível exercer controle. O ambiente operacional sofre interferência das ações do alvo e de fatores desconhecidos ou inopinados.

Eficiência e Resiliência

Peter Drucker (1963), considerado o pai da Administração moderna, definia eficiência como "fazer certo as coisas", e eficácia "fazer a coisa certa". Tornou-se célebre sua afirmação de que não há nada mais inútil do que fazer com grande eficiência algo que não deveria ter sido feito.

Segundo McChrystal (2015, p. 80), o foco da administração de empresas, por mais de um século, esteve na eficiência. Nessa cultura, pretende-se obter o máximo de um resultado *x* com o mínimo do insumo *y*. O problema, segundo o autor, é que para otimizar essa equação, é necessário que *x* e *y* sejam identificados com antecedência suficiente para se construir mecanismos para converter um no outro. "A busca pela eficiência está baseada na predição" (McCHRYSTAL, 2015, p. 80).

Takeuchi e Nonaka (1986) argumentam que equipes auto-organizáveis – como aquelas observadas em empresas *start-up*, que desenvolvem sua própria agenda e tomam iniciativas e riscos – são mais

eficazes, em grande medida, em razão de sua adaptabilidade. McChrystal (2015) avança o argumento, e defende que essa adaptabilidade seja escalada ao nível da organização como um todo. Para Sherman Kent (2015, p. 185) quadros de pessoal rígidos aumentam a inércia de qualquer grande organização.

Nesse sentido, McChrystal (2015, p. 76) relaciona adaptabilidade ao conceito de resiliência: a capacidade de um sistema absorver distúrbios e ainda manter suas funções e estrutura básica. No paradigma de resiliência, inspirado no ambientalismo[5], os gerentes aceitam a inexorabilidade de ameaças inopinadas. Em lugar de desenharem defesas robustas e especializadas, criam sistemas que absorvam ou mesmo se beneficiem das dificuldades. Com efeito, uma boa análise prospectiva admite a existência de infinitos cenários futuros possíveis e, precisamente por isso, é importante que se identifiquem cenários de "wild cards" (curingas) – a respeito, ver James A. Dewar (1993).

Nessa linha, Taleb (2017) tipifica os sistemas em frágeis, que são afetados por choques; robustos, que resistem a choques; e antifrágeis, que se beneficiam de choques. Segundo McChrystal (2015, p. 80), a robustez é alcançada fortalecendo-se as partes do sistema, enquanto a resiliência resulta da melhor ligação entre essas partes, o que permite ao sistema reconfigurar-se ou adaptar-se em resposta a mudanças ou danos. Para o autor, é importante mudar o foco da predição para a reconfiguração. Reconhecendo a inevitabilidade de situações inopinadas e utilizando sistemas que sobrevivam ou mesmo se beneficiem dessas surpresas, é possível superar cenários de incerteza.

Absorver a volatilidade (mudanças) é crucial na atividade de Inteligência. Como referido, Clark (2010) argumenta que o alvo típico da Inteligência é uma rede. Para McChrystal (2015, p. 84), é preciso ser uma rede para vencer outra rede. Redes mudam de forma e tamanho. São adaptáveis e resilientes, embora, por isso mesmo, nem sempre sejam absolutamente eficientes.

Por essa razão, um sistema preditivo, porque frágil, embora eficiente, é incapaz de superar uma rede adaptável. Operações de Inteligência minuciosamente planejadas, com pouca margem de decisão para as equipes, desenhadas para serem eficientes e precisas, tendem a ser custosas, lentas e confusas. Sistemas frágeis são eficientes em ambientes complicados. Em cenários complexos, é necessário resiliência ou, se possível, *antifragilidade* [6].

Planejamento: relações em lugar de tarefas

Analistas e usuários são os únicos capazes de avaliar conteúdo e assim determinar valor para a busca (CLARK, 2010, p. 152). Isso reforça a necessidade de planejamento integrado e, mais do que isso, envolvimento do analista durante a execução de uma operação. A ideia de que

5 Para aprofundar a respeito, ver Waker e Salt (2006) e Flaherty (2018).

6 Taleb (2017) afirma ter pesquisado em diversos idiomas e não encontrado termo que defina o conceito de antifrágil.

a Inteligência se desenvolve em um "ciclo"[7] induz a interpretar a atividade em fases estanques e condiz pouco com a realidade (HERMAN, 1996; CLARK, 2010). Além disso, como argumenta Herman (1996, p. 292), sistemas de requerimentos, em que analistas prescrevem necessidades específicas aos responsáveis pela busca, distanciam-se da realidade e não garantem sucesso. Clark (2010) agrega que esses sistemas são estruturas burocráticas que consomem tempo e recursos, adicionando pouco valor ao produto. Nesse modelo, não há priorização ou critérios para avaliação de conteúdo. Com isso, arrisca-se priorizar a quantidade de produção em prejuízo da qualidade.

Outro ponto importante é que, como observa McChrystal (2015, p. 98), times cujos membros se conhecem desempenham muito melhor. Em ambientes verdadeiramente complexos, as situações ultrapassam a habilidade de um único líder prever, monitorar e controlar. Equipes bem integradas e conectadas interna e externamente estarão melhor preparadas do que esse líder para decidir e inovar. É como se uma equipe de velejadores, em plena regata, dependesse de ordens do treinador para folgar a adriça da genoa ou passar a retranca.

Não obstante, há, pela própria cultura de compartimentação da Atividade de Inteligência, resistências à integração. Exemplo notório é a aversão das frações operacionais à participação de agentes externos no planejamento e gestão de sua atividade. Como observa Clark, os "operacionais resistem aos esforços dos analistas em se envolverem no processo de desenvolvimento de sistemas e estratégias de busca. Seu mantra é 'diga-me o que você precisa, que eu te entrego o dado'" (CLARK, 2010, p. 154, tradução nossa).

Compromete o planejamento minucioso o fato de, como demonstra Clark (2010, p. 150), o analista geralmente não saber o que o operacional pode fazer e, frequentemente, enfrentar dificuldades em delimitar com precisão sua necessidade específica. Por isso é importante que o responsável pela busca[8] entenda o que o analista realmente precisa e, da mesma forma, auxilie-o nessa definição.

No caso das Operações de Inteligência, quando geridas no modelo de comando e controle, a documentação elaborada para planejar as ações se distancia da realidade tão logo se executem as atividades. As demandas recebidas das frações analíticas, também documentadas, tendem a passar pelo mesmo processo. É que fatores importantes comprometem a utilidade de planejamentos inspirados na cultura fordista. Como observam Sutherland (2016) e Sabbagh (2013), em ambientes complexos, caracterizados pelo desconhecimento de variáveis significativas, mudança e imprevisibilidade, não é possível prever o que irá acontecer. Assim, em lugar de se impor um caminho, é mais eficaz uma abordagem

7 Há diversos modelos de "ciclos de Inteligência" na literatura. Lowenthal (2006, p. 65) reproduz e critica ciclo apresentado pela CIA em 1993 no guia *A Consumer's Handbook of Intelligence,* em que são representados cinco "passos" dentro do ciclo: (1) planejamento/direcionamento → (2) coleta de dados → (3) processamento → (4) análise → (5) difusão → (1)...

8 O termo busca aqui entendido em sentido *lato*, como aquisição de dado de difícil obtenção, não importando o meio empregado)

empírica e adaptativa, com tolerância a falhas e abertura a formas inovadoras de trabalhar durante a execução.

Sabbagh (2013, p.19) faz um paralelo entre o planejamento na construção civil e no desenvolvimento de *software*. Pode-se substituir o desenvolvimento de *software* pela condução de caso na Inteligência: diferente da construção civil, em que as variáveis são conhecidas e dominadas, aqui não se conhecem todas elas e grande parte das conhecidas não estão sob controle.

Nesses ambientes complexos, Sabbagh (2013, p. 24) afirma que praticamente tudo, exceto a visão do produto, pode mudar em tempo diminuto. Em Operações de Inteligência, é comum haver alterações no ambiente operacional, nas rotinas de trabalho, nos métodos empregados, nas demandas do usuário e mesmo nos alvos. Sabbagh (2013) argumenta que iterações curtas, no sentido de desenvolver o trabalho em parcelas intermediárias com *feedback* constante, permitem que essas mudanças possam ser mais rapidamente inseridas no projeto.

Segundo Sutherland (2016, p. 16), as gerências cobram, tradicionalmente, dois elementos dos projetos: controle e previsibilidade. O resultado é uma grande quantidade de documentos. O planejamento de detalhes para que não haja erros, comprometimento do orçamento ou perda de prazo, consome tempo e energia. Para o autor, isso é difícil de ser realizado em cenários complexos. Na prática, é recorrente o surgimento de problemas ou inspirações para solucioná-los.

É necessário ter um plano, mas segundo Sutherland (2016, p. 119), ele deve ser refinado ao longo do projeto. O autor defende que se planejem mais detalhadamente as atividades que serão realizadas num período curto de tempo, como uma ou duas semanas, deixando as ações futuras traçadas em linhas gerais.

Para que as principais partes interessadas (por exemplo, analista responsável, encarregado de caso, equipe operacional, gerência média e alta direção) possam avaliar e direcionar a estratégia operacional, é fundamental que se defina qual objetivo ou necessidade se pretende atender. Dito de outra forma, estabelecer quais condições se querem satisfeitas ao final do caso, operação ou ação de inteligência favorece a definição da estratégia de execução.

A partir dessa definição é que as equipes decidirão, de forma dinâmica, o que devem fazer (ver item seguinte: níveis de tomada de decisão). Os argumentos de Clark (2010) e Herman (2006) reforçam a necessidade de o analista identificar e priorizar lacunas em seu conhecimento. A busca de dados atuará nessas lacunas priorizadas. Os operacionais devem ser incentivados a testar novas ideias em lugar de manter estratégias de busca que nem sempre obtêm o dado necessário (CLARK, 2010, p. 160). Trazendo os princípios de gestão apresentados por Sutherland (2016) para esse contexto, a melhor forma de otimizar esse planejamento é realizá-lo de forma integrada, envolvendo as principais partes interessadas.

Para Clark (2010), fechar as lacunas em curto prazo de alvos prioritários requer alocar de forma eficiente as fontes de busca existentes

baseadas a) na importância da necessidade ou tarefa específica; b) no valor do dado obtido, em caso de sucesso da busca; c) na probabilidade de sucesso do esforço de busca; d) nos custos e riscos. O autor defende que os operacionais podem ajudar na reunião[9] de dados se tiverem acesso à estratégia de análise. Ao fim, ambos os esforços de busca e análise se beneficiam dessa abordagem integrada.

Para isso, as lideranças devem trabalhar para criar um ambiente abrangente que estabeleça vínculos produtivos e criativos entre as partes, em lugar do microgerenciamento por comando e controle (McCHRYSTAL, 2015). Mais do que traçar planos que descrevam tarefas minuciosas, o desejável é que se planejem essas relações entre pessoas. A inovação e a criatividade serão produtos do trabalho coletivo.

Para isso, o planejamento precisa mapear as principais partes interessadas (SABBAGH, 2013) no caso– ainda que outras partes possam ser incluídas depois. Esse mapeamento auxiliará os responsáveis a calibrar os esforços da coleta, análise e busca, além de delimitar os participantes de reuniões de acompanhamento. Mais importante, propiciará aos gestores desenhar as melhores formas de interação entre essas partes.

Essas relações não se resumem ao pessoal interno. Como afirmou Sherman Kent (2015, p. 180), a parte mais importante do negócio da Inteligência é o relacionamento adequado com quem a utiliza. É fundamental que se planejem as relações com o usuário, devidamente mapeado como parte interessada, para que a atividade possa ser melhor guiada e adaptar-se a variações em sua demanda. Como lembra Kent, a não ser que a Inteligência seja completa, precisa, oportuna e aplicável a um problema existente ou que está por existir para o usuário, ela é inútil.

Níveis de Tomada de Decisão

Segundo Sabbagh (2013), a superação das dificuldades impostas pelos ambientes complexos exige das organizações que incorporem coragem para confiar em suas equipes e deixem-nas livres para realizar seu trabalho. Sutherland (2016, p. 61) lembra que "abrir mão do microgerenciamento cotidiano e do controle é difícil, mas fazer isso no mundo secreto da inteligência e das operações especiais é ainda mais desafiador" (tradução nossa). Não obstante, transferir para os executores decisões e capacidade de se organizar proporciona eficácia e redução de riscos. Com isso, acaba-se por entregar eficiência por meios distintos daqueles empregados no fordismo.

Segundo a *International Federation of Accountants* (IFAC, 2014, p. 8) a governança no setor público compreende as disposições instituídas para garantir que os resultados desejados pelas partes interessadas sejam definidos e alcançados. De forma mais ampla, o sistema de governança (ver TCU, 2014) representa a forma como diversos atores se organizam, interagem e procedem para obter boa governança. Isso envolve

9 Entendida como a juntada de dados por qualquer meio e de qualquer origem

estruturas administrativas, processos de trabalho, instrumentos, fluxo de informações e o comportamento das pessoas envolvidas na avaliação, no direcionamento e no monitoramento da organização.

Nesse sistema, governança e gestão se diferenciam pelo nível em que atuam na organização. A governança tem como funções definir o direcionamento estratégico; supervisionar a gestão; envolver as partes interessadas; gerenciar riscos estratégicos; gerenciar conflitos internos; auditar e avaliar o sistema de gestão e controle; e promover a *accountability* (prestação de contas e responsabilidade) e a transparência. Por sua vez, a gestão tem como funções colocar programas em prática; garantir a conformidade com as regulamentações; revisar e reportar o progresso de ações; garantir a eficiência administrativa; manter a comunicação com as partes interessadas; e avaliar o desempenho e aprender (TCU, 2014).

De acordo com essa perspectiva, no âmbito da organização há três instâncias de gestão: administração executiva, tática e operacional. A administração executiva avalia, direciona e monitora a organização. Trata-se da autoridade máxima da organização, e seu nível estratégico torna-a responsável pela harmonização da organização com sua governança externa. A gestão tática coordena a gestão operacional em áreas específicas. A gestão operacional executa processos produtivos finalísticos e de apoio. (TCU, 2014)

A interposição de decisões táticas e operacionais à alta administração acaba por saturá-la de informações e demandas, prejudicando o desempenho institucional e comprometendo sua função de governança.

Na lógica de comando e controle, a gestão executiva e tática deixa pouca liberdade para a operacional. Já na década de 1980, Takeuchi e Nonaka (1986) apontavam para a pouca efetividade desse tipo de abordagem para a criatividade e inovação. Em seu estudo, os autores identificaram seis caraterísticas nas equipes que se destacavam no desenvolvimento de produtos. Particularmente em atividades inseridas em cenários complexos que atendem a demandas cambiantes, métodos de gestão baseados em times (1) com instabilidade embutida[10], (2) auto-organizáveis, (3) resilientes[11], (4) cujas fases de desenvolvimento são sobrepostas, (5) com aprendizado baseado em múltiplas fontes de informação e (6) inseridos em corporações com controle sutil (oposto ao comando e controle), apresentavam níveis significativamente maiores de sucesso.

Modelos de governança que estabelecem o controle da gestão operacional[12] por níveis muito estratégicos têm sido criticados de forma recorrente. Sherman Kent (2015, p. 125-129) argumenta que esse controle, na Atividade de Inteligência, deve ser mais relacionado ao foco, qualidade e gerenciamento de equipes do que quanto

10 No sentido de definir objetivos genéricos altamente desafiadores sem fornecer conceitos claros do produto que, ao fornecer ampla liberdade e, ao mesmo tempo, objetivos altamente desafiadores,

11 No original, os autores utilizam o conceito "instabilidade incorporada". Aqui utiliza-se *resiliência* em razão da proximidade com a definição apresentada acima (adaptação a mudanças).

12 No sentido de inferior a tático e estratégico.

à forma, que é responsabilidade dos executores. Para o autor, a descentralização da função de controle é fundamental. O ideal é descer a função de controle o mais baixo possível na hierarquia. Da mesma forma, o controle deve controlar, continuamente, a quantidade de documentação que exige das frações, mantendo-a ao menor nível possível.

Esse movimento de descer o nível decisório proporciona ainda ganhos de motivação com impacto na produtividade. McChrystal (2015, p. 211) cita estudos que demonstram que o "empoderamento" aumenta a satisfação dos funcionários e que a descentralização do controle cria uma motivação intrínseca pelas tarefas. Para o autor, "um indivíduo que toma uma decisão se torna mais interessado em seu resultado" (tradução nossa). Ele defende um sistema descentralizado que empurre o controle (autoridade) para as franjas da organização.

Esse movimento permite a divisão de responsabilidades, preservando a autoridade máxima e transferindo implicação por decisões técnicas para instâncias inferiores. A alta gestão fica mais livre para dedicar-se à criação e manutenção de um ambiente favorável ao trabalho, melhorando a relação entre as equipes, entregando-lhes as melhores ferramentas e batalhando pelo seu bem-estar.

Equipes: transparência e fluxo de informações

A formação de equipes analíticas e operacionais motivadas, competentes e eficientes é fundamental na Atividade de Inteligência. Equipes, desde que não sejam muito grandes, produzem muito mais que indivíduos. Estudos demonstram que o tamanho recomendado para uma equipe é de sete pessoas, tolerando-se duas a mais ou menos. Se a equipe é muito grande, sua produtividade diminui (para referências a respeito, ver Sutherland, 2016).

Takeuchi e Nonaka (1986) identificaram que as melhores equipes são transcendentes, autônomas e multifuncionais. Sutherland (2016) recomenda que elas se identifiquem com o produto que estejam desenvolvendo e não com a especialidade de cada um. Para o autor, é desejável que a equipe possua todos os requisitos materiais e intelectuais necessários para concluir sua tarefa.

Contribui para essa transcendência o sentimento de pertencimento e a consciência que cada indivíduo tem da importância de seu trabalho para o todo. Por isso, é importante que todos na equipe saibam do que os outros fazem e acreditem na relevância de seu trabalho.

McChrystal (2015, p. 139-141) argumenta que o hábito de reter informações deriva de preocupações com segurança, mas também da influência de processos mecanicistas bem definidos, em que indivíduos necessitam conhecer apenas o que lhes compete para realizar seu trabalho. O autor critica a lógica da "necessidade de conhecer" em razão de ela supor a existência de algum ente superior com conhecimento total capaz de distribuir cada material a quem "precisa conhecer". Contudo, prossegue, para transitar em segurança em um ambiente interdependente é necessário que cada equipe possua um entendimento holístico das interações entre todas as partes. Para que os planos

funcionem, todos devem enxergar o sistema como um todo.

Sabbagh (2013, p. 20) ressalta a importância da qualidade da interação entre os membros do time para a redução de problemas no desenvolvimento dos trabalhos e facilitar a comunicação e o *feedback*.

Como observa Sutherland (2016), liderança não se confunde com autoridade. Um gerente deve possuir conhecimento e ser um líder-servidor. Deve ser capaz de constantemente repassar o *feedback* dos clientes (no caso de operações de inteligência, analistas) para a equipe.

Ou seja, um bom gerente operacional conhece a temática e o ambiente em que trabalha. É fundamental que tenha poder de tomar decisões e esteja disponível para explicar à equipe o que tem de ser feito e por quê. É, em última instância, o responsável pelo valor do produto operacional.

É importante que, periodicamente, as frações operacionais apresentem à análise alguma produção com valor, preferencialmente de forma documentada. Contudo, como observa Sabbagh (2013, p. 22-23), a documentação não substitui a interação. Ela a facilita, pode ser utilizada como um registro permanente, mas é importante que haja reuniões de avaliação. Clark (2010) sugere medir a satisfação do usuário com perguntas como "Qual o percentual do assunto-alvo foi resolvido?" Com base nessas reuniões, as frações operacionais podem rever seus procedimentos e atualizar o planejamento.

Como observa Sutherland (2016, p. 77), quanto mais cedo o cliente tiver amostras do resultado, mais rápido será capaz de sinalizar se o que se está produzindo é algo de que ele precise. A entrega de documentos com resultados periódicos é uma oportunidade para avaliar junto ao analista se o seu conteúdo coincide com suas necessidades, se resolve ao menos parte de seu problema e se as equipes caminham em boa direção. Para Sabbagh (2013, p. 23) essa entrega iterativa possibilita um *feedback* confiável. As frações operacionais devem buscar o máximo de *feedback* sobre o que foi entregue, de forma que a próxima entrega seja melhor planejada. Essa interação e iteratividade desconstrói a ideia de "nós" e "eles", colocando operacional e analista do mesmo lado (SABBAGH, 2013).

É fundamental que essa equipe motivada, transcendental, autônoma e multifuncional, com alto nível de interação entre seus membros e com acesso a *feedbacks* constantes, confiáveis e consistentes, esteja também absolutamente conectada às demais equipes da organização. Nesse sentido, McChrystal (2015, p.125) alerta para a importância de que, quando confinadas em "silos", as equipes podem alcançar uma adaptabilidade tática, mas no nível estratégico a organização permanecerá rígida. Com isso, o autor defende que haja fluxos produtivos de informação entre as equipes, integrando-as de forma similar à integração entre os indivíduos que conformam uma única equipe. Para isso, o autor defende que sejam mantidas conferências abertas e transparentes, coordenadas pelas lideranças, com o objetivo de aproximar as pessoas da organização.

Conclusão

A velocidade das mudanças e a interdependência observadas atualmente criam um ambiente complexo, organizado em redes, diferente do que a ideia de "ciclo de inteligência" deixa transparecer. Processos estanques, com funções bem delimitadas, são pouco eficazes nesse contexto.

Para adaptar-se a isso, é necessário que os órgãos de Inteligência revejam suas definições em relação ao compartilhamento de informações, equacionem melhor os níveis para tomada de decisão, e repensem suas formas de liderança.

O planejamento e a execução das Operações de Inteligência devem ser liquidificados[13] e abordar um gerenciamento leve e dinâmico, capaz de absorver inovação, criatividade, novas formas de trabalhar e aprendizado com as falhas. Com efeito, esse tipo de abordagem merece discussão e estudos aprofundados que avaliem sua adequação em situações nas quais a atuação em rede se faça necessária, como é o caso do combate ao crime organizado.

No escopo desta revisão bibliográfica, essa mudança passa pela superação do modelo baseado em comando e controle, com "empoderamento" decisório das equipes operacionais, para que se tornem mais eficazes e criativas. Para isso, é importante que o planejamento priorize as relações entre pessoas, mais do que as tarefas que serão executadas, de forma a maximizar a transparência e o fluxo de informações entre as equipes. Isso inclui a aproximação entre equipes operacionais, analistas e demais partes interessadas nas Operações de Inteligência.

Finalmente, e igualmente importante, é fundamental que as equipes trabalhem motivadas, identificadas com o produto de seu esforço e cientes do impacto de seus resultados no desempenho das demais frações.

13 No sentido adotado por Bauman (2001).

Bibliografia

BAUMAN, Zygmunt. *A Modernidade Líquida*. São Paulo: Zahar, 2001.

BECK, Kent *et al. Manifesto para Desenvolvimento Ágil de Software.* <www.agilemanifesto.org>. Acesso em 01/10/2017.

BRASIL. Escola Nacional de Informações (ESNI). *Resumo da proposta de nota de aula. Operações de Inteligência: Planejamento.* Brasília: s.d.

BRASIL. Tribunal de Contas de União – TCU. *Referencial Básico de Governança*. 2014. Disponível em: <www.tcu.gov.br/governanca> Acesso em: 17 set. 2017.

CLARK, Robert M. *Intelligence Analysis: a target centric approach*. 3. ed. Washington: CQ Press, 2010.

DEWAR, James A. *The importance of "wild card" scenarios.* <www.au.af.mil/au/awc/ awcgate/cia/nic2020/dewar_nov6.pdf>. Acesso em: 15 out. 2018.

DRUCKER, Peter. "Managing for business effectiveness". In: *Harvard Business Review*, Boston, maio 1963.

ESTADOS UNIDOS DA AMÉRICA (EUA). *Department of Defense* – DOD. *DOD Dictionary of Military and Associated Terms 2017*. Disponível em: <www.dtic.mil/doctrine/dod_dictionary/> Acesso em: 10 out. 2017.

FLAHERTY, Eoin. *Complexity and Resilience in the Social and Ecological Sciences.* Londres: Palgrave Macmillan, 2018.

HARVEY, David. *A Condição Pós-Moderna.* São Paulo: Edições Loyola, 2004.

HERMAN, Michael. *Intelligence power in peace and war*. Cambridge: Cambridge University Press, 1996.

IFAC. *International Federation of Accountants. International framework: good governance in the public sector.* 2014. Disponível em: <www.ifac.org/publications-resources/> Acesso em: 12 out. 2017.

KENT, Sherman. *Strategic Intelligence for American World Policy*. New York: Princeton University Press, 2015.

LOWENTHAL, Mark M. *Intelligence: from secrets to policy.* Washington: CQ Press, 2006.

McCHRYSTAL, Stanley (Gen) et al. *Team of Teams: new rules of engagement for a complex world.* New York: Portfolio/Penguin, 2015.

RUBIN, Kenneth. *Essential Scrum: practical guide to the most popular Agile Process.* Donneley: Addison-Wesley, 2013.

TAKEUCHI, Hirotaka e NONAKA, Ikujiro. "The new product development game". *In: Harvard Business Review*, Boston, n. 64, jan./fev. 1986.

TALEB, Nassim Nicholas. *Antifrágil: coisas que se beneficiam com o caos.* Rio de Janeiro: Best Seller, 2017. (Ed. Kindle)

SANTOS, Milton. "A aceleração contemporânea: tempo-mundo e espaço-mundo". *Boletín Geográfico*. Neuquén, n. 19, 1993.

SABBAGH, Rafael. *Scrum Gestão Ágil para projetos de sucesso.* São Paulo: Casa do Código, 2013.

SEGRILLO, Angelo. *O declínio da URSS: um estudo das causas.* Rio de Janeiro: Record, 2000.

SIMS, Chris e JOHNSON, Hillary Louise. *Scrum: a breathtakingly brief and Agile introduction.* Kindle Edition: 2012.

STRANGE, Susan. *The Retreat of State.* Cambridge University Press, 1998.

SUTHERLAND, Jeff. *Scrum: A arte de fazer o dobro do trabalho na metade do tempo.* São Paulo: Leya, 2016.

WAKER, Brian e SALT, David. *Resilience Thinking: sustaining Ecosystems and People in a Changing World.* Washington, DC: Island Press, 2006.

A CONFIANÇA COMO REQUISITO PARA A GESTÃO DE SEGURANÇA EM ORGANIZAÇÕES DE INTELIGÊNCIA DE ESTADO

Marcel Carrijo de Oliveira *

Resumo

Os níveis de confiança intraorganizacional estão associados ao engajamento no trabalho e à predisposição a observar normas e comportamentos seguros. Este estudo objetiva analisar como as relações de confiança e desconfiança podem impactar a gestão de segurança em Organizações de Inteligência de Estado (OIEs), instituições encarregadas de realizar missões especializadas que requerem sigilo e são condicionadas por esse imperativo. De modo a viabilizar o estudo em modelo analítico, e na ausência de estudos anteriores sobre esse tema, foram analisadas as interações entre os estudos sobre confiança e desconfiança, sobre gestão de segurança e de segurança da informação, e sobre a Atividade de Inteligência. A partir disso, observou-se que a promoção da confiança e a mitigação da desconfiança poderiam trazer benefícios para esse tipo institucional, cujas características dificultam e favorecem - simultaneamente - a adoção de medidas de construção e manutenção da confiança. Enfim, são apresentadas medidas identificadas na literatura que objetivam a modernização da gestão de segurança a partir do fortalecimento da confiança intraorganizacional.

Palavras-chaves: Inteligência, Gestão de Segurança, Confiança,

TRUST AS A REQUIREMENT FOR SECURITY MANAGEMENT IN STRATEGIC INTELLIGENCE AGENCIES

Abstract

The levels of trust within organizations are widely associated with employee engagement, their willingness to observe rules, as well as the internalization of secure behaviors. This study analyzes how trust and distrust may impact security management in Strategic Intelligence Agencies (SIAs), specialized public organizations that operate in secrecy and are constrained by this requirement. In the absence of other known studies in this field, we have chosen to analyze the interactions between studies on trust and distrust, on security and information security management, and on Strategic Intelligence. We then identified and described how the characteristics common to SIAs tend to simultaneously favor and hamper measures designed to build and preserve trust, as well as those aimed at mitigating distrust. Lastly, we propose that fostering trust and reducing distrust would be beneficial to SIAs, and derive from the literature alternatives potentially beneficial to security management based on the promotion of trust.

Keywords: *Intelligence, Security Management, Trust*

* Mestre em Relações Internacionais pela Universidade de Brasília.

Artigo recebido em julho/2018
Aprovado em outubro/2018

Introdução

"O mundo está mudando". Essa talvez seja a justificativa mais comum quando revisitamos ideias, planos ou formas de fazer. Tal noção - antes precursora da inovação - é, atualmente, óbvia, difusa e limitada. Em um contexto global no qual as mudanças ocorrem de forma constante, acelerada, sobreposta e colidente, seriam as práticas tradicionais de gestão e a filosofia de liderança organizacional suficientes para explicar o sucesso de organizações no século XXI?

O mais recente relatório Gallup (2017, p. 71) sobre o estado do ambiente de trabalho nos Estados Unidos, centro nevrálgico dos estudos e das práticas de gestão contemporânea, informa que apenas 33% dos trabalhadores estadunidenses estão engajados - ou seja, altamente envolvidos e entusiásticos a respeito de suas funções e de seu local de trabalho-, contra 27% dos trabalhadores no Brasil e 70% daqueles que atuam nas empresas com melhores índices no mundo. Essas estatísticas são ainda mais impactantes quando se considera que colaboradores ativamente engajados são, em média, 17% mais produtivos e 21% mais lucrativos (GALLUP, 2017, p. 68).

O baixo engajamento no trabalho extrapola, contudo, as questões meramente produtivas. De interesse para este estudo, o engajamento afeta a observância de regras de segurança e de segurança da informação, a disposição para reportar incidentes, o compromisso de manutenção do sigilo, a intenção de permanecer na instituição, entre outros (D'ARCY e GREENE, 2014, pp. 476-479). A promoção de relações funcionais seguras envolve, nesse contexto, compreender como indivíduos e organizações interagem e quais fatores potencializam essa interação.

O estudo ora proposto objetiva discutir como dois fatores de influências sobre o engajamento no trabalho - as relações de confiança e de desconfiança intraorganizacionais - impactariam a gestão de segurança em Organizações de Inteligência de Estado (OIEs), organizações cujos processos e produtos são transversalmente afetados pelo sigilo e cujo objetivo fundamental é o assessoramento ao processo decisório nacional de mais alto nível. Esse tipo institucional tende a modelar suas estruturas de proteção no formato "castelo e fosso", em que são estabelecidos pontos exclusivos de entrada e saída física e lógica da instituição - como a ponte levadiça de um castelo - de modo a restringir o acesso de indivíduos indesejáveis. Considera-se que tal modelo requer relações de confiança intraorganizacional sólidas para ser efetivo, pois uma vez concedida autorização de acesso, a pessoa poderá mover-se com razoável liberdade nos ambientes internos.

Estabelece-se como cerne desse estudo a noção de que a promoção de relações de confiança e a mitigação daquelas de desconfiança seriam essenciais para a gestão de segurança em OIEs, embora algumas características desse tipo institucional, especialmente o sigilo, tendam a ter efeito deletério sobre esses objetivos. Essa proposta foi abordada por meio de revisão da literatura especializada e da análise das interações paradigmáticas entre os estudos sobre: confiança e desconfiança; gestão de segurança e de segurança da informação; e Atividade de Inteligência. Identificou-se que

as características das OIEs podem dificultar a promoção da confiança, ao mesmo tempo em que favoreceriam a implementação de medidas de controle e de conscientização em segurança, ambos em decorrência da centralidade do sigilo na dinâmica institucional. Por fim, são apresentadas medidas identificadas na literatura que objetivam modernizar a gestão de segurança a partir do fortalecimento da confiança intraorganizacional.

Confiança e confiabilidade

A confiança, independente de outras considerações, é um estado psicológico. Aquele que confia expõe-se àquele em quem se confia, sujeita-se aos riscos de depender de outrem, cujas intenções e motivações não são inteiramente conhecidas, de modo a reduzir a complexidade das relações humanas. A decisão de confiar está atrelada, portanto, a um conjunto de elementos que ultrapassam a racionalidade estrita e podem incluir percepções culturais, reações emocionais, relações sociais, entre outros. Em suma, uma pessoa "não apenas pensa confiança, mas sente confiança" (FINE e HOLYFIELD, 1996, p. 25 apud KRAMER, 1999, p. 572).

Na prática, a confiança manifesta-se todas as vezes em que um indivíduo depende de outro, por sentir-se incapaz ou por conveniência. Por isso, trata-se a confiança como uma escolha, uma decisão, que é estudada a partir de duas abordagens principais. A "confiança como escolha racional" provém das ciências sociais, econômica e política, e está centrada na noção de que a decisão de confiar é calculada, visa maximizar ganhos e minimizar perdas esperadas (KRAMER, 1999, p. 572). O indivíduo confia quando considera que o outro será capaz de satisfazer seus interesses melhor do que ele próprio, porque o outro tem mais competência ou porque julga arriscado ou excessivamente custoso realizar ele mesmo as ações de seu interesse.

Em que pese seu valor preditivo para comportamentos "ideais", o modelo racional carece de instrumentos que expliquem por que razão as pessoas decidem confiar em outras que seriam, sob melhor juízo, inconfiáveis. Para suprir essa lacuna, foram desenvolvidos os chamados "modelos relacionais de confiança", que incorporam os elementos sociais e relacionais, inclusive em suas dimensões cognitiva, motivacional e afetiva, como antecedentes da decisão de confiar. Mais do que um cálculo objetivo de risco, a confiança, nessa abordagem, é "uma orientação social em relação a outras pessoas e à sociedade como um todo" (KRAMER, 1999, p. 573).

Möllering (2006, p. 105) defende que resumir a confiança a uma dessas duas abordagens afetaria a capacidade explicativa única do construto e, por isso, seria mais coerente contextualizar a influência dos cálculos racionais, dos estímulos sociais e, também, da "reflexividade", o impacto da percepção de sucesso/fracasso da confiança depositada em outrem, sobre a disposição para confiar. Trata-se de reconhecer que a confiança se estabelece em um contexto de risco para quem confia e que é do interesse individual mitigar esse risco e reduzir a insegurança. A confiança é, portanto, "a disposição de uma parte a estar vulnerável às ações de outra, baseada na expectativa de que o outro vai realizar uma ação específica importante para

quem confia, independente de sua habilidade para monitorar ou controlar aquela outra parte" (MAYER et. al., 1995, p. 712).

De modo a operacionalizar essa concepção, Hardin (1992, p. 152-154) propõe que a confiança depende da relação estabelecida entre um confiante *(truster)*, um confiado *(trusted)* e o contexto/domínio específico em que a confiança é conferida. Logo, a confiança está condicionada tanto por elementos pessoais e psicológicos que condicionam a disposição em confiar (atrelados ao ambiente familiar, a aspectos socioculturais e a características de personalidade) como por fatores construídos relacional e historicamente.

Naturalmente, é preciso reconhecer que a decisão de confiar não ocorre no vácuo, que os indivíduos baseiam essa escolha em um julgamento, com vistas a determinar a "confiabilidade" de outro. Três atributos pessoais são centrais para essa avaliação: a capacidade, o conjunto de habilidades, conhecimentos e características do confiado que viabilizam sua influência sobre determinado domínio; a benevolência, o quanto se acredita que o confiado quer o bem do confiante; e a integridade, a percepção de que o confiado adere a um conjunto de princípios e valores que o confiante julga aceitáveis (MAYER et. al., 1995, p. 717-719). Essas expectativas sobre a confiabilidade são validadas ou refutadas pelas repetidas interações entre as partes, o que induz sucessivas readequações do modelo mental (KRAMER, 1999, p. 576).

Interagir é, portanto, requisito essencial para relações de confiança duradouras. Seria inimaginável, no entanto, considerar que todas as partes de uma organização complexa lograriam relacionar-se com frequência e profundidade suficientes para viabilizar uma avaliação criteriosa de confiabilidade. Entre empregado e empregador, há gestores, gerentes, supervisores, colegas; e, nesse contexto, percepções são muitas vezes "emprestadas", ora na forma de avaliações de desempenho, ora como "fofoca". Nesse sentido, Burt e Knez (1996, p. 83) destacam que as informações obtidas de terceiros/intermediários tendem a refletir apenas uma porção da dinâmica intraorganizacional, geralmente enviesada de acordo com as expectativas do emissor a respeito do que interessa ao receptor. Em outras palavras, se um gestor sabidamente não confia em um servidor, é provável que o supervisor imediato deste apresente àquele informações que confirmem a baixa confiabilidade do subordinado, reforçando a avaliação do superior.

A confiabilidade, por fim, também é atribuída nas relações baseadas em identificação de grupo, inclusive funcional. O membro de um grupo - de uma categoria profissional ou o servidor ocupante de um cargo - é percebido como parte de um *ethos* específico, sujeito a regras formais e informais de conduta e a modelos mentais compartilhados. A sua confiabilidade é, portanto, parcialmente despersonalizada, decorre da expectativa de que aquela pessoa possui as competências necessárias para pertencer àquele grupo e está disposta a cumprir as obrigações relacionais e organizacionais esperadas dela, quaisquer que sejam.

Benefícios da confiança intraorganizacional

A crença de que todos na organização compartilham o mesmo entendimento a respeito do contexto vivenciado e do comportamento esperado de cada um motiva as instituições a confiar, a estabelecer regras formais ou informais, de modo que cada parte do sistema comprometa-se com um processo de socialização baseado na aderência aos princípios, valores e normas que regem a organização. Busca-se, assim, fomentar o engajamento, facilitar os processos de trabalho e difundir a cultura organizacional.

Esse processo adquire características específicas quando se trata de organizações públicas, que são governadas por forças políticas, tem objetivos diversos e relativamente vagos, e são expostas a princípios de controle finalístico decorrentes da delegação de poderes (MEIER e KRAUSE, 2003, p. 13). Para cumprir suas missões, o setor público costuma organizar-se de acordo com a concepção weberiana, baseada na "autoridade racional-legal", que envolve divisão do trabalho, pessoal de carreira com treinamento especializado e *expertise*, estruturas organizacionais formais e hierárquicas que não replicam outras unidades administrativas da instituição, bem como regras e procedimentos que garantam clareza de autoridade e responsabilidade. Como esse modelo é voltado para situações de estabilidade, é também afrontado pela dinamicidade do mundo contemporâneo, razão pela qual o setor público busca soluções no setor privado, a exemplo da incorporação de técnicas e melhores práticas de gestão (KHAN e KHANDAKER, 2016, p.2875).

Outra característica de organizações públicas é a prevalência da dinâmica principal-agente na gestão institucional. Nesse paradigma, o principal considera firmar contrato com o agente, sob a expectativa de que este fará escolhas que produzirão os resultados desejados por aquele. Como o agente também tem os seus próprios interesses, repousará sobre a estrutura do contrato entre as partes tornar vantajosa a compatibilização de seus interesses. Mesmo assim, haverá, sempre, assimetrias de informação, e o principal precisará delegar atribuições ao agente sem ter conhecimento completo e/ou preciso de suas ações e intenções (MEIER E KRAUSE, 2003, p. 8).

Quando observamos as OIEs, os efeitos dessas problemáticas tendem a ser exponencializados, em decorrência de sua característica mais marcante: o sigilo. Em ambientes construídos a partir de protocolos de produção e proteção de conhecimentos, cujo descumprimento pode resultar em prejuízos de imagem, vazamento de informações, morte, entre outros, o modelo weberiano tende a ser praticado enfaticamente e a relação principal-agente tende a atingir níveis mais elevados, e potencialmente danosos, de assimetria de informação. Isso afeta gravemente a "aversão à traição" *(betrayal aversion)* por parte dos principais, a noção de que os confiantes receiam confiar por sofrer duas perdas de utilidade quando a interação principal-agente falha: o insucesso e a percepção de que a confiança foi traída, violada (BOHNET et al., 2008, p.296).

O desempenho organizacional, nesse contexto, é facilitado pelo estabelecimento de relações de confiança, com três efeitos positivos de maior destaque. Primeiro, o

nível de confiança influencia os custos de transação dentro da organização, reduzindo a necessidade de repetidas negociações individuais que estabeleçam credibilidade e mecanismos de controle entre os membros da instituição (KRAMER, 1999, p. 582). A confiança também favorece a sociabilidade espontânea entre os servidores, a sua disposição a realizar ações cooperativas, altruísticas e que excedam seu rol de atribuições, sem esperar recompensa além da melhoria das condições coletivas de bem-estar (FUKUYAMA, 1995, p. 27). Esse é um dos objetivos clássicos dos modelos de gestão e influencia a resiliência organizacional, a capacidade para resistir a períodos de instabilidade e aprimorar processos de modo a fortalecer-se internamente a médio prazo.

Enfim, a confiança impacta como os indivíduos se relacionam em estruturas hierárquicas, especialmente aquelas de matriz weberiana, a exemplo das OIEs. Para aqueles em posição de liderança, é impraticável explicar e justificar cada uma de suas decisões a cada um dos colaboradores, assim como é inviável monitorar cada indivíduo, punir cada conduta desviante e premiar cada ação positiva. A confiança intraorganizacional é, assim, fundamental para que os servidores reconheçam que são tratados de forma justa e imparcial, principalmente quando afrontados com situações em que eles estejam investidos emocionalmente, como promoções, reestruturações, investigações internas e demissões.

Óbices ao estabelecimento da confiança intraorganizacional

Embora pareça óbvio e desejável que as organizações possuam níveis adequados de confiança interna, o baixo índice de engajamento de trabalhadores nos EUA e no Brasil, apresentados anteriormente, indicam que há descompasso entre o discurso contemporâneo sobre gestão organizacional e a realidade percebida por mais de dois terços da força de trabalho. O desafio talvez seja o fato de que - assim como o ar que respiramos - "a confiança é, na maioria das vezes, 'transparente', e não se permite perceber verdadeiramente até que ela seja posta em perigo: é quando a confiança é violada que ela parece, subitamente, ser indispensável" (VAN BELLEGHEM, 2003, p. 53). Nesse sentido, Kramer (1999, p. 587-594) destaca quatro fatores que atuam como óbices ao desenvolvimento da confiança: a fragilidade inerente à confiança; a quebra do contrato psicológico; as novas tecnologias; e a dinâmica de suspeição e desconfiança.

Como dito acima, a confiança depende de interações continuadas e positivas. Rupturas na sua frequência ou qualidade acarretam óbices ao desenvolvimento da confiança e favorecem a formação de um círculo vicioso, em que a pouca confiança desestimula a relação entre as partes, reduzindo as possibilidades de interações positivas e contribuindo para que a pouca confiança, ou até mesmo a desconfiança, consolide-se prematura e/ou equivocadamente (KRAMER, 1999, p. 593). Por isso, considera-se que é mais fácil destruir do que construir confiança.

Com efeito, a construção de confiança é promovida quando os processos decisórios são transparentes e fragilizada quando são opacos. Se um processo (orçamentário,

seletivo etc.) é percebido como logicamente compatível com a estratégia organizacional, torna-se legítimo para os servidores, mesmo que não lhes seja favorável. Em sentido contrário, a desconexão estratégica incentiva interpretações de favoritismo, injustiça, descompromisso da alta gestão, entre outros, e mina a confiança (KIM e MAUBORGNE, 2003).

Em OIEs, a reduzida visibilidade externa e o alto risco envolvido na atividade tendem a aprofundar a importância das relações de confiança, ao mesmo tempo em que parece mantê-las em um estado de fragilidade quase permanente. Isso porque, para cumprir uma de suas missões (manter e proteger o sigilo sobre as informações, as demandas e os métodos da atividade), a lógica que rege o processo de segurança das OIEs tende a ser proteger o máximo possível e revelar o mínimo estritamente necessário. Por meio de medidas de controle como a classificação, o acesso e a necessidade de conhecer, o sigilo tanto viabiliza a missão institucional das OIEs como inibe as interações sociais e profissionais que estruturam as relações de confiança.

A segunda barreira ao estabelecimento de ambientes de confiança é a quebra do contrato psicológico, o conjunto de promessas realizadas por empregado e empregador, que se comprometem a cumprir os termos pactuados explicitamente ou interpretados a partir do convívio. Como as promessas estipuladas de parte a parte estão sujeitas ao entendimento, à percepção e à interpretação, é comum a ocorrência de desentendimentos. Seja porque uma promoção não foi dada a um servidor competente ou porque o desempenho da equipe é considerado insuficiente pelo gestor, violações do contrato básico de expectativas tendem a enfraquecer a confiança e a prejudicar o relacionamento. Essas tensões e quebras do contrato psicológico são associadas à reduzida performance dos trabalhadores, ao baixo nível de iniciativa e comprometimento e às intenções de saída da organização.

No caso das OIEs, o modo como o contrato psicológico é estabelecido tende a variar significativamente, de acordo com o país, sua história e seu contexto. Acredita-se, em geral, que os indivíduos que almejam integrar OIEs tendem a apresentar características pessoais favoráveis ao desenvolvimento de confiança no âmbito do contrato psicológico, a exemplo do sentido de propósito, geralmente externado na forma de patriotismo, e da dedicação altruística em favor de objetivos institucionais e nacionais (HERMAN, 2006, p. 324-326). Porém, em decorrência do imperativo do sigilo e da consequente necessidade de altos padrões de segurança e excelência como alicerces da confiabilidade em situações de risco, a eventual fragilização do contrato psicológico em OIEs tende a ser desastrosa, motivando questionamentos a respeito da segurança e do bem-estar individuais e podendo acarretar descompromisso com os princípios institucionais.

Por sua vez, as novas tecnologias, principalmente aquelas que visam remediar desafios de segurança, como ferramentas de monitoramento e auditoria, geram efeitos contraditórios. Tentam solucionar o desafio de confiabilidade interna, garantindo o respeito às normas e expectativas organizacionais e, ao mesmo tempo,

impactam a percepção que os servidores têm do modo como a organização os vê – do quanto são confiáveis –, reduzindo os incentivos sociais ao comportamento adequado e, potencialmente, gerando ressentimento. Em OIEs, a relação com as novas tecnologias talvez seja, excepcionalmente, melhor do que nas demais organizações, em decorrência das expectativas inerentes ao trabalho em Inteligência e à sua tendência a aproveitar rapidamente os avanços tecnológicos que fomentam a segurança. Como consequência do sigilo, o controle é esperado, ainda que por vezes possa ser considerado incômodo.

Enfim, a suspeição e a desconfiança estão interligadas e combinam-se para minar a possibilidade de construção da confiança. Fein e Hilton (1994, p. 168, apud KRAMER, 1999, p. 587) definem suspeição como um estado psicológico em que o indivíduo ativamente considera múltiplas, potencialmente antagônicas, hipóteses a respeito dos motivos ou do comportamento de outrem. A suspeição afeta o modo como o indivíduo calcula a confiabilidade alheia, tornando-o mais cuidadoso ao avaliar as motivações potenciais do outro. A depender do contexto, a pessoa pode ser alvo de suspeição sem sequer ter se comportado de forma inadequada no ambiente de trabalho, bastando para a suspeita que tenha havido algum fato, inclusive na esfera pessoal, que contrarie as crenças cognitivas, morais, éticas ou mesmo culturais de quem a está avaliando.

A desconfiança, por sua vez, representa desafio peculiar, pois é menos compreendida racionalmente do que a confiança e, *a contrario sensu*, não é seu antípoda. Quando pensamos essas duas categorias, tendemos a imaginar um contínuo, que se inicia no estado "perfeito" de confiança e se encerra no estado "imperfeito" de desconfiança. Não obstante, somos plenamente capazes de confiar pontualmente em alguém de quem desconfiamos usualmente. Para tanto, dependemos, tão somente, de um contexto favorável ou inescapável. As interações entre OIEs são exemplo desse tipo de coexistência entre a confiança e a desconfiança; embora antagonistas no ambiente concorrencial que define as relações internacionais, esses órgãos logram compartilhar informações específicas a respeito de temas de interesse mútuo.

Na desconfiança em estado absoluto, o estado da mente que prevalece não só não confia, mas também promove, ativa e reiteradamente, o desconfiar. Se é mais fácil destruir a confiança do que construí-la, é mais fácil construir a desconfiança do que destruí-la. Pior, a construção de uma não resulta, necessariamente, na destruição da outra (VAN DE WALLE e SIX, 2013, p. 3). Em decorrência dessa coexistência, e na ausência de opção viável na literatura, define-se a desconfiança a partir do conceito de Mayer para a confiança, visto anteriormente, evitando os antagonismos que poderiam equalizá-la com a não-confiança. Considera-se, assim, que um indivíduo desconfia quando tem uma disposição a não estar vulnerável às ações de outra pessoa, porque acredita que ela seria incapaz de realizar uma ação específica que lhe importa, a menos que esteja plenamente habilitado para monitorar e/ou controlar sua atuação.

Para a gestão de uma OIE, a desconfiança pode ser especialmente destrutiva. Com

efeito, ela inviabiliza as ações básicas da instituição, pois afeta a disposição em assumir riscos, cumprir missões a partir de informações compartimentadas e atuar em conjunto com pessoas ou equipes pouco conhecidas. Mais ainda, a desconfiança tende a impactar a incorporação da visão estratégica da instituição pelos servidores, pois indivíduos em estado de desconfiança tendem a desconfiar mesmo das boas intenções de mudança. Por isso, considera-se que a mitigação da desconfiança exige estratégias de longo prazo e consistência organizacional quanto às iniciativas de construção e manutenção de confiança (VAN DE WALLE & SIX, 2013, p. 22).

Interessantemente, alguns autores têm propagado a ideia de que existiriam níveis legítimos de desconfiança, cuja mitigação dependeria de controle e dissuasão (VAN DE WALLE & SIX, 2013, p. 12). Novamente, as OIEs ilustram o fenômeno, uma vez que a preservação do sigilo impõe uma série de constrangimentos e exige mecanismos de monitoramento e controle, considerados não só coerentes com a missão desse tipo institucional, mas também necessários para a proteção individual dos servidores e a consecução dos objetivos organizacionais.

Medidas de promoção da confiança e de mitigação da desconfiança na gestão de segurança em OIEs

A segurança em OIEs consiste em medidas defensivas espelhadas em técnicas ofensivas de Inteligência, como as coletas de Inteligência Humana (HUMINT) e Inteligência Cibernética. A fim de combatê-las, adotam-se medidas de segurança humana, física, de documentação e de redes e sistemas, a exemplo da investigação pessoal, do controle de viagens ao exterior e de contatos com estrangeiros, da restrição ao acesso físico a áreas e instalações e lógico a redes e sistemas e de regras para a classificação, custódia e transmissão de documentos. Tudo isso sublinhado pelo sigilo e pelo princípio da necessidade de conhecer (HERMAN, 2006, p. 167).

O desafio que aqui se propõe está situado, contudo, em um momento anterior à definição de normas e práticas de segurança. Em verdade, trata-se do que é "gestão de segurança". Usulmente, associa-se à palavra "gestão" noções como liderança, transparência, participação, autonomia e necessidade de compartilhar *(need to share)*. "Segurança", por outro lado, é atrelada a controle, regras, risco, burocracia, incômodo, e necessidade de conhecer *(need to know)*. De outro modo, percebe-se que a gestão mantém alinhamento conceitual com a confiança, enquanto a segurança tende a ser associada com os elementos de suspeição e de desconfiança.

Como, então, avançar de um estado em que, muitas vezes, as organizações acabam "gerindo desconfiança" para outro, em que elas promovem a confiança de forma segura? A resposta para essa questão envolve o papel desempenhado pelos três elementos-chave da gestão de segurança (a política de segurança, os líderes e gestores, e os servidores) na promoção da confiança e na mitigação da desconfiança intraorganizacional.

As políticas de segurança são compostas por

princípios e normas que orientam as atitudes e o comportamento dos trabalhadores e estipulam sanções para eventuais violações. Essa lógica de "obedeça ou sofra as consequências" indica que os servidores são vistos, *a priori*, com desconfiança, como potenciais causadores de danos institucionais e como a principal vulnerabilidade na cadeia de componentes da segurança. Não à toa, popularizou-se a imagem do indivíduo como elo mais fraco de uma "corrente" da segurança organizacional.

Flechais et. al. (2005, p. 37), no entanto, destacam que as pessoas não quebram relações de confiança de maneira automática e insensível. Se, por exemplo, um servidor é credenciado a acessar documentos estratégicos e sigilosos, ele tenderá a sentir que a organização confia nele, porque incumbiu-lhe um ativo institucional valioso. Internamente, será difícil violar essa relação, a menos que o indivíduo identifique outros elementos que justifiquem o desrespeito à confiança nele depositada, geralmente associados à percepção de injustiça, insegurança e incoerência institucional. Para fazer frente a esses desafios psicológicos, é recomendável que as políticas de segurança vinculem normas e contramedidas à proteção de ativos institucionais, inclusive os servidores, em vez de enfocarem a conformidade comportamental por meio de sanções. Em outras palavras, tende a ser mais efetivo informar que o uso de crachás é mandatório porque visa à identificação oportuna, pela equipe de monitoração em vídeo, de indivíduos estranhos e potencialmente perigosos, do que simplesmente estabelecer que o uso do crachá é mandatório e a desobediência à norma resultará em suspensão.

Outro ponto destacado é que as normas de segurança costumeiramente demandam que os trabalhadores incorporem comportamentos que podem ser interpretados como evidências de desconfiança em relação a colegas de trabalho, a exemplo de não compartilhar senhas de sistemas e bancos de dados. Em alguns casos, esses mecanismos favorecem a criação de estruturas *ad hoc* de segurança no nível produtivo, que contornam ou subvertem as regras estabelecidas em favor de ganhos produtivos supostamente maiores, socialmente convenientes e organizacionalmente mais arriscados (KIRLAPPOS & SASSE, 2015, p. 1). Um grupo de servidores poderá, nesse sentido, compartilhar a senha de acesso individual a um banco de dados de modo a evitar o preenchimento de formulários de cadastramento extensos.

As pessoas, porém, não são apenas as principais causas de preocupação para a gestão de segurança; são também a primeira linha de defesa e a principal forma de prevenção, detecção e solução de problemas. Afinal, são elas que desenham, implementam, operam e utilizam os sistemas. Mais ainda, como dito acima, os servidores tendem a considerar legítimas certas formas de controle, desde que sensíveis ao desejo dos indivíduos de serem reconhecidos como confiáveis e coerentes com a missão institucional.

Considera-se positivo, portanto, que a gestão de segurança esteja alinhada com os objetivos estratégicos da organização. Para tanto, gestores e líderes têm papel fundamental. Estudos realizados no setor privado indicam que esses atores

institucionais influenciam em até 70% os índices de engajamento e confiança dos trabalhadores e atuam como modelos de alta visibilidade, a partir dos quais os empregados chegam a inferências genéricas a respeito da confiança institucional (KRAMER, 1999, p. 592; HARTER e ADKINS, 2015).

A construção de confiança inicia-se, assim, pela seleção e pelo treinamento de líderes e gestores, a fim de que atuem, prioritariamente, como catalisadores, facilitadores e *coaches*, e apenas secundariamente como figuras de autoridade. Nesse ponto, estudos sobre liderança e gestão informam que a tendência das organizações de promover servidores a cargos de gestão com base em tempo de serviço ou em desempenho técnico em funções operacionais, em vez de talento, treinamento e competência, não traz resultados ótimos (BECK & HARTER, 2015). Em OIEs, esperar que a "nata" se destaque naturalmente pode ser arriscado, pois tende a favorecer o sucesso a curto prazo, muitas vezes desconsiderando o "fator sorte" e a consistência funcional - inclusive o compromisso com a segurança - ao longo da carreira (HATFIELD, 2008, p. 15).

Líderes e gestores mal selecionados e treinados precariamente acabariam por favorecer o que Galford e Drapeau (2013) chamam de "inimigos da confiança". Esse tipo de gestor diz o que as pessoas querem ouvir, esperando com isso obter maior engajamento, ao invés de dizer o que elas precisam ouvir; ignora que os empregados monitoram todas as suas ações e que se eles acreditarem haver algum favoritismo, reduzirão seu nível de confiança; despreocupa-se com a incompetência, "porque não faz mal a ninguém" e desconsidera o impacto que isso gera sobre a equipe; fornece *feedback* inconsistente com o desempenho - ou nem fornece - muitas vezes para evitar conflito; não confia nos servidores e impede o seu crescimento por meio da realização de tarefas complexas e inéditas; evita discutir os "elefantes na sala", os problemas e desafios que exigem comprometimento e podem causar desconforto entre alguns servidores, se tratados devidamente; e, para completar, permite que rumores circulem livremente, ao invés de abordar claramente as questões que preocupam a equipe.

Uma vez abordadas as medidas mais genéricas de fomento à confiança e mitigação da desconfiança, passa-se do nível individual (líder/gestor/servidor) para a "cultura de segurança", o conjunto de premissas compartilhadas e ativamente difundidas entre os membros da organização sobre segurança. Nesse aspecto, a literatura especializada registra seis grupos de medidas pró-confiança que podem ser adaptados à gestão de segurança em OIEs e são abordados a seguir (FLECHAIS et. al, 2005; BINIKOS, 2008; LACEY, 2009; KIRLAPPOS & SASSE, 2015).

Primeiro, recomenda-se *simplificar a segurança*, facilitar a observância de seus preceitos por meio de ferramentas e normas bem elaboradas, com especial atenção à redução de exceções normativas, que costumam acarretar confusão e abuso. Kirlappos e Sasse (2015, p. 7) chamam de "higiene de segurança" *(security hygiene)* a noção de que as regras devem ser desenvolvidas ao redor dos processos de produção, de modo a reduzir a necessidade de violação da segurança por

razões de produtividade. Com isso, ataca-se a noção de que a urgência justifica a má conduta e incute-se entre os gestores de segurança a ideia de que seus sistemas devem ser de simples aplicação e compreensivos, sob pena de serem somente incômodos e dispendiosos.

A partir de normas e procedimentos simples e compreensivos é possível *promover uma cultura legítima de segurança*, que não seja punitiva, nem injusta ou seletiva. Com efeito, busca-se desenvolver processos transparentes de gestão de segurança, inclusive de punição, que priorizem a proteção dos ativos e da missão institucional e favoreçam o diálogo interno. Nesse sentido, é salutar que os servidores sejam convidados a participar da segurança, inclusive da elaboração de normas, o que tende a facilitar o engajamento laboral e a incentivar o desenvolvimento de um senso de propriedade e pertencimento *(ownership)* sobre o futuro da organização.

Na mesma direção, considera-se relevante *promover a identidade de grupo*, incentivar os servidores a reconhecerem-se como membros de uma instituição cujas peculiaridades implicam em exigências diferenciadas de trabalho. Diversas medidas podem ser adotadas nesse sentido, como a inclusão dos trabalhadores em "grupos de segurança", com atribuições e sistema de recompensas próprios que tendem a tornar essa atividade parte de seu negócio. Infelizmente, para a maior parte deles, cumprir preceitos de segurança e comportar-se de forma segura não constituem atividades fundamentais que levariam a resultados de trabalho; não compõem suas avaliações de desempenho e raramente são recompensados pelo bom comportamento.

Todas essas propostas seriam inócuas caso a instituição falhe em *promover a educação em segurança*, oferecer treinamento em relação ao que é esperado dos servidores e quais são as ameaças identificadas pela organização. É recomendado que a organização sinalize aos servidores que eles têm a sua confiança - que as questões de segurança são parte do negócio da organização, não questões pessoais - e divulgue informações a respeito de ameaças identificadas pela instituição. Passa-se, assim, de uma abordagem puramente centrada em normas e sanções para outra guiada por riscos e objetivos organizacionais, o que amplia o foco de atenção e responsabilidade dos servidores, extrapolando o mundo físico para incluir, também, as ameaças ao sucesso organizacional e ao seu bem-estar profissional.

Por outro lado, é recomendável evitar campanhas mal desenhadas, principalmente aquelas que ocorrem logo após incidentes de segurança graves. Embora a inspiração tenha efeitos mais poderosos e duradouros do que o exercício da autoridade, muitas culturas de segurança são determinadas pela reação da alta direção a grandes incidentes, os quais são, além de danosos, embaraçosos e politicamente nefastos (LACEY, 2009, p. 8). A lógica de "cabeças vão rolar", no entanto, raramente aborda as causas profundas dos incidentes de segurança e pode, em verdade, prejudicar a confiança e a produtividade organizacionais, pois o servidor que trabalha com mais afinco, dinamicidade e empoderamento tende a ser mais vulnerável a cometer erros do que aquele que simplesmente obedece ordens.

Quando as medidas inclusivas e preventivas falham, a promoção da confiança e a mitigação da desconfiança dependem de medidas que visam *assegurar a segurança*. Servidores conscientes trabalhando em ambientes com sistemas efetivos de segurança não têm razão para violar as normas institucionais, a menos que o façam por descaso ou má fé. Por isso é recomendável que ações maliciosas ou que não foram relatadas oportunamente tenham consequências graves e visíveis para o grupo de servidores, de modo a desencorajar comportamentos desviantes no futuro e a incentivar e motivar os servidores que respeitam os preceitos de segurança. Reforça-se, assim, a noção de que a confiabilidade, a responsabilidade e o comprometimento são valorizados pela instituição (KIRLAPPOS e SASSE, 2015, p. 7-8).

Por fim, a evolução de qualquer sistema baseado em confiança estará condicionada à capacidade organizacional de *apoiar a comunicação de incidentes de segurança*. Quando a organização opta por agir contra quem informa incidentes, não apenas vitimiza o empregado como perde a oportunidade de corrigir desvios e fomentar a confiança. Isso é ainda mais relevante nos casos em que a decisão de informar/denunciar está fora das atribuições regulares do indivíduo, que precisaria buscar em seu senso de ética e de justiça a motivação para relatar incidentes e expor-se ao crivo da organização e de colegas. Por isso é recomendado que a instituição viabilize os meios para que o servidor confie a ela esse tipo de informação, desde um canal apropriado e seguro de comunicação até a percepção, a crença, de que as práticas organizacionais excluem da normalidade as atitudes ilegais, ilegítimas e/ou antiéticas (BINIKOS, 2008, p. 58).

Considerações finais

Como visto, as OIEs podem beneficiar-se da promoção da confiança e da mitigação da desconfiança, em termos gerais e no âmbito da sua gestão de segurança. Esse esforço, contudo, depende de iniciativas institucionais que desvinculem o sigilo de eventuais práticas secretistas que suprimam o diálogo interno e do fortalecimento da comunicação de segurança. Fomentar-se-ia, assim, a transparência na atuação da alta gestão, a clareza de objetivos por parte dos gestores e o senso de responsabilidade por parte dos servidores. No mesmo sentido, líderes e gestores tendem a desempenhar melhor suas funções quando são selecionados com base em seu comprometimento com os valores organizacionais - entre os quais se encontra a segurança - e treinados de modo a se tornarem promotores de relações profissionais, com os servidores e entre os servidores, conducentes com o estabelecimento de um ambiente de trabalho pautado pela excelência, pelo respeito à política de segurança e pela gestão embasada em confiança.

A estruturação de políticas de segurança baseadas em confiança, a seleção e o treinamento adequado de líderes e gestores, a inclusão participativa e o empoderamento dos servidores na gestão da segurança tendem a tornar instituições como as OIEs mais resilientes. À medida que os agentes adversos tornam-se mais criativos e imprevisíveis, um corpo funcional adepto de preceitos de segurança e motivado a proteger sua instituição tende a suspeitar

de ações estranhas, adotar comportamentos seguros e consultar os gestores de segurança a respeito de situações imprevistas. Reconhece-se que eliminar completamente os incidentes de segurança é inviável, porém reputa-se plenamente cabível aspirar que eles ocorram com menos frequência e que sejam informados e tratados oportunamente. Para isso, considera-se essencial deixar de entender a confiança intraorganizacional como sintoma de saúde institucional e passar a observá-la como uma de suas principais causas.

Referências

BECK, Randall e HARTER, Jim. *Why good managers are so rare?* Disponível em: <hbr.org/2014/03/why-good-managers-are-so-rare?cm_sp=Article-_-Links-_-Comment>. Acesso em: 7 jun. 2018.

BINIKOS, Elli. Sounds of Silence: organizational trust and decisions to blow the whistle. In: *SA Journal of Industrial Psychology*, 2008. v. 34, n. 3, p. 48-59.

BOHNET, Iris; GREIG, Fiona; HERRMANN, Benedikt; ZECKHAUSER, Richard. Betrayal *Aversion: evidence from Brazil*, China, Oman, Switzerland, Turkey, and The United States. In: The American Economic Review, 2008. v. 98, n.1, p. 294-310.

BURT, Ronald S. e KNEZ, Marc. Kinds of Third-Party Effects on Trust. In: KRAMER, Roderick M. e TYLER, Tom R. *Trust in Organizations: frontiers of theory and research*. Thousand Oaks: SAGE Publications, 1996, p. 68-89.

D'ARCY, John e GREEN, Gwen. Security Culture and the Employment relationship as drivers of employees' security compliance. In: *Information Management & Computer Security*, 2014. v. 22, n. 5, p. 474-489.

FLECHAIS, Ivan; RIEGELSBERGER, Jens; SASSE, M. Angela. *Divide and Conquer: the role of trust and assurance in the design of secure socio-technical systems.* Disponível em: <www.nspw.org/papers/2005/nspw2005-flechais.pdf>. Acesso em: 6 jun. 2018.

FUKUYAMA, Francis. *Trust: the social virtues and the creation of prosperity.* International New York: The Free Press, 1995.

GALFORD, Robert M. e DRAPEAU, Anne Seibold. *The Enemies of Trust.* Disponível em: <hbr.org/2003/02/the-enemies-of-trust>. Acesso em: 6 jun. 2018.

GALLUP. *State of the American Worplace*. Disponível em: <news.gallup.com/reports/199961/state-american-workplace-report-2017.aspx>. Acesso em: 7 jun. 2018.

HARDIN, Russel. The Street-Level Epistemology of Trust. In: *Analyse & Kritik*, 1992. v. 14, n. 2, p. 152-176.

HARTER, James e ADKINS, Amy. *What great managers do to engage employees*. Disponível em <hbr.org/2015/04/what-great-managers-do-to-engage-employees>. Acesso em: 7 jun. 2018.

HATFIELD, E. L. *Finding Leaders: preparing the Intelligence Community for succession management*. Washington, DC: National Defense Intelligence College, 2008.

HERMAN, Michael. *Intelligence Power in Peace and War*. Cambridge: University of Cambridge Press, 2006.

KHAN, Anisur R.; KHANDAKER, Shahriar. Public and Private Organizations: how different or similar are they. In: *Journal of Siberian Federal University Humanities & Social Sciences*, 2016. v. 12, n. 9, p. 2873-2885.

KIM, Chan e MAUBORGNE, Renee. *Fair Process: managing in the knowledge economy*. Dispnível em: <hbr.org/2003/01/fair-process-managing-in-the-knowledge-economy>. Acesso em 6 jun. 2018.

KIRLAPPOS, Iacovos e SASSE, M. Angela. *Fixing Security Together: leveraging trust relationships to improve security in organizations*. Disponível em: <discovery.ucl.ac.uk/ 1461243/3/Kirlappos-Usec2015.pdf>. Acesso em: 6 jun. 2018.

KRAMER, Roderick M. Trust and Distrust in Organizations: emerging perspectives, enduring questions. In: *Annual Review of Psychology*, 1999. v. 50, p. 569-598.

LACEY, David. Understanding and transforming organizational security culture. In: *Information Management & Computer Security*, 2010. v. 18, n. 1, p. 4-13.

MAYER, Roger C.; DAVIS, James H.; SCHOORMAN, F. David. An Integrative Model of Organizational Trust. In: *The Academy of Management Review*, 1995. v. 20, n. 3, p. 709-734.

MEIER, Kenneth J. e KRAUSE, George A. The scientific study of bureaucracy: an overview. In: KRAUSE, G. A. and MEIER, K. J. (eds.). *Politics, Policy, and Organizations: Frontiers in the Scientific Study of Bureaucracy*. Ann Arbor: University of Michigan Press, 2003. p. 1-22.

MÖLLERING, Guido. *Trust: Reason, Routine, Reflexivity*. Oxford: Elsevier, 2006.

VAN BELLEGHEM, Laurent. Réciprocité des enjeux de confiance au travail: le cas de coursiers et de leur dispatcheur. In: KARSENTY, L. (cord.). *La confiance au travail*. Toulouse: Octarès, 2013. p. 53-75.

VAN DE WALLE, Steven e SIX, Frédérique. Trust and distrust as distinct concepts: why studying distrust in institutions is important. In: *Journal of Comparative Policy Analysis*, 2014. v. 16, n. 2, p. 158-174.

NOTAS PARA UMA GEOPOLÍTICA AMBIENTAL: NARRATIVAS TRANSTERRITORIAIS E O APARATO DE INTELIGÊNCIA PARA A AMAZÔNIA.

Rodrigo Augusto Lima de Medeiros *

Resumo

Este artigo propõe refletir sobre uma geopolítica ambiental amazônica por meio da análise de narrativas burocráticas que servem ao propósito de um governo estratégico do espaço amazônico. As relações entre política (processos enunciativos de governo) e território (simbolização do espaço) definem concepções para a Amazônia. Assim, analisar de que modo concepções geopolíticas fundamentam práticas ambientais para a Amazônia brasileira é o propósito deste artigo. Tanto a *intelligentsia administrativa* brasileira quanto *think tanks* estadunidenses procuram estabelecer práticas territoriais para a Amazônia, fundamentando estratégicas de comércio e desenvolvimento para o Brasil, em geral, e para a Amazônia, em particular. Há uma forte matriz militar nas reflexões/ações das burocracias especializadas tanto no Brasil quanto nos EUA que projetam modelos hegemônicos de desenvolvimento. Por um lado, observamos que a intelligentsia administrativa brasileira procura integrar territorialmente a região amazônica ao centro dinâmico da economia nacional, subordinando essa integração a concepções de segurança nacional. Por outro lado, *think tanks* estadunidenses concebem a Amazônica como sendo um armazém de recursos naturais subordinado a interesses comerciais e industriais de seu complexo produtivo civil-militar. Concluímos que os receituários institucionais estabelecem regimes práticos que criam territórios com base na soberania de um ordenamento político-institucional, dando a dimensão de um estado de guerra permanente por narrativas que legitimem planos para a Amazônia.

Palavras-chaves: Geopolítica Ambiental. Amazônia. Burocracia.

NOTES FOR ENVIRONMENTAL GEOPOLITICS: TRANSNATIONAL NARRATIVE AND THE INTELLIGENCE APPARATUS FOR THE AMAZON REGION.

Abstract

The objective of this article is to reflect on environmental geopolitics. Some bureaucratic narratives provide argumentative elements to elaborate governmental actions to the Amazon region. In this sense, conceptions of an Amazon are made through the relationship between policy (a set of ideas or a plan) and territory (embodiment of space). Thus, this article aims at analysing the way geopolitical conceptions can impact environmental practices in the Brazilian Amazon. Both the Brazilian administrative intelligentsia and North American think tanks seek to establish territorial practices for the Amazon, grounding trade strategies. Specialized offices in Brazil and the United States work with a military framework in the reflections and actions for the Amazon, which project hegemonic models of development. The Brazilian administrative intelligentsia seeks to territorially integrate the Amazon region into the dynamic centre of the

* Doutor, mestre e bacharel em Ciências Sociais pela Universidade de Brasília. Sua tese de doutorado foi premiada no V Concurso de Tese do Ministério da Defesa. Possui experiências profissionais em docência, serviço público, instituições multilaterais e licenciamento ambiental. É professor do Centro Universitário de Brasília (UniCEUB) e Especialista em Política Ambiental do Ministério do Meio Ambiente (MMA).

Artigo recebido em julho/2018
Aprovado em setembro/2018

national economy, subordinating this integration to a national security conception. In turn, US think tanks comprehend the Amazon as a natural resource warehouse, which can be subordinated to their civil and military industrial complex. Therefore, the paper comes to the conclusion that institutional prescriptions establish pragmatic actions which build up an unlike kind of territorialities through different institutional narratives.

Keywords: *Environmental Geopolitics. Amazon. Bureaucracy.*

Introdução: uma geopolítica marcada no planejamento estatal

O objetivo deste artigo é analisar de que modo concepções geopolíticas fundamentam práticas ambientais para a Amazônia brasileira. Em outro trabalho (MEDEIROS, 2018), traçamos genealogias de concepções geopolíticas tanto de uma *intelligentsia administrativa* brasileira quanto de *think tanks* estadunidenses. Ambos procuram estabelecer práticas territoriais para a Amazônia, fundamentando estratégias de *comércio e desenvolvimento* para o Brasil, em geral, e para a Amazônia, em particular. Há uma forte matriz militar nas reflexões/ações das burocracias especializadas tanto no Brasil quanto nos EUA que projetam um modelo hegemônico de desenvolvimento. Observa-se que a *intelligentsia* administrativa procura integrar territorialmente a região amazônica ao centro dinâmico da economia nacional, subordinando essa integração a concepções de *segurança nacional*. Por sua vez, *think tanks* estadunidenses concebem a Amazônia como sendo um armazém de matérias-primas subordinado aos interesses comerciais e industriais.

Não cabe aqui realizar levantamento teórico-metodológico de categorias analíticas da geografia política, tampouco formular discussão crítica sobre a vertente "determinista" da geopolítica de Friedrich Ratzel (1988) ou sobre a vertente "possibilista" vinculada a Paul Vidal de La Blache (1954). As preocupações deste artigo não se vinculam exclusivamente aos questionamentos da geopolítica em si, mas, principalmente, de que modo a geopolítica é utilizada na elaboração de construtos técnico-burocráticos, ou melhor, de que modo as *narrativas geopolíticas se tornam pressupostos que constroem projetos político-territoriais para a Amazônia.* Na argumentação deste artigo, esses pressupostos são entendimentos de senso comum que flertam com concepções desenvolvimentistas e ambientalistas, mas que não verticalizam nas compreensões (MEDEIROS, 2018). Assim, os projetos político-territoriais são narrativas geopolíticas em torno de *práticas burocráticas que servem ao propósito de um governo estratégico da natureza.* As relações entre política – processos enunciados de governo (FOUCAULT, 2005) – e território – simbolização do espaço (MASSEY, 2008).[1] – definem as políticas estratégicas para a Amazônia.

Em síntese, para Bertha Becker, geopolítico é o "campo de conhecimento que analisa relações entre poder e espaço" (2005, p. 71). O Estado é o principal ator geopolítico na medida em que possui o legítimo monopólio da violência física (WEBER, 2004). O Estado impõe a soberania de seu ordenamento jurídico-institucional dentro de seu território, podendo, pretensiosamente, impor suas concepções territoriais para outros Estados, em condições assimétricas de negociações. Entretanto, o *Estado não é o único ator no jogo*

1 De acordo com Massey (2008, p. 212), espaço é "como a esfera de relações, da multiplicidade contemporânea e, como sempre, em construção". Na esteira das discussões de Latour (2005) sobre agentes humanos e não humanos, Massey procura um conceito de espaço relacional no qual agrega as noções de que há atores naturais (não sociais), por exemplo, aspectos biofísicos, que também inventam lugares em interação com atores sociais. É nesse conceito de espaço em que me apoio. Para uma discussão detalhada sobre a história da apropriação do espaço em dinâmicas de cartografia e mapas, recomendamos John Pickles (2004).

geopolítico. Para uma compreensão adequada da geopolítica, da ordem narrativa e do governo do território, *esse monopólio precisa ser detalhado (destrinchado ao patamar das elaborações burocráticas)*. A formulação do processo decisório assume feições múltiplas e não só estatais. São variados os atores-sociais que se associam (ou competem) para efetivar um *governo territorial*. As discussões dos neoinstitucionalistas sobre governança, governabilidade e custo de transações (NORTH, 1990) dão conta de uma das instâncias dessa realidade de instituições formais e informações na configuração do processo de formulações políticas. Porém, essa abordagem institucionalista, de inspiração neoclássica, deixa muitas outras instâncias fora de suas análises. A intenção deste artigo é dar um passo mais adiante no intuito de compreender como operam os sistemas classificatórios nas formulações de políticas estratégicas[2] . É dentro da dinâmica metamorfoseada do espectro político (RIBEIRO, 1991) que podemos encontrar o engajamento teórico-prático de burocracias especializadas em políticas estratégicas.

As associações, ao longo da história do Brasil, entre políticos e militares, para a realização de projetos de poder, sempre levaram, inevitavelmente, a rupturas institucionais, e descontinuidade jurídico-legal (CARVALHO, 2004; SODRÉ, 1979). A geopolítica é uma teoria do poder, apoiada fundamentalmente no território, e só tem valor se utilizar os fatores geográficos na formulação de uma política (MIYAMOTO, 1981, p. 7). A dinâmica de uma geopolítica militar que fundamenta um pensamento político-administrativo para o governo do território, da natureza e da nação, se institui em práticas e categorias historicamente fabricadas para lidar com a complexidade territorial brasileira, em geral, e amazônica, em particular, nitidamente de inspiração alemã e francesa durante a primeira república (SPRANDEL, 2005; STEINBERGER, 1997). É nesse contexto que *opera de modo explícito uma geopolítica ambiental que se utiliza de todo o estoque prático-simbólico das categorias anteriormente instituídas* na lógica da administração do território amazônico (MEDEIROS, 2018). Em que se pese a institucionalização de práticas e categorias expressas em um ordenamento jurídico, o deslocamento do centro dinâmico de como governar o território amazônico – anteriormente estabelecido por fortificações militares, por fluxos migratórios e por tratados internacionais – intensifica-se, no século XXI, com as *narrativas transterritoriais* do meio ambiente, tais como, mudança climática, bioprospecção, recuperação florestal, e conservação da biodiversidade, entre outros, incorporando a Amazônia dentro de uma lógica política globalizante.

Por sua vez, apesar das contradições internas, os Estados, em geral, planejam suas ações nas formulações de uma burocracia especializada que deve ser capaz de lidar com diferentes contextos, países e situações,

2 Durkheim procura refundar as concepções aprioristas e empiristas com relação à definição de categoria, inventando uma terceira ordem de coisas por meio das representações coletivas na elaboração de uma teoria sociológica do conhecimento. Durkheim estabelece a base para um pensamento sociológico radical que busca explicação e compreensão para as coisas (fenômenos) na sociedade. Desse modo, ele institui as categorias na organização social, por consequência a regra da classificação vem da regra da organização social que serve para pensar as coisas via elaboração de categorias e classificações, ou seja, sistemas classificatórios (DURKHEIM, 1996).

a fim de manter sob controle oportunidades comerciais (para seus nacionais) e de segurança (para seus investimentos). Todo esse aparato burocrático está focado em monitorar a conjuntura político-militar dos países. Especificamente, no Brasil, há constante batalha por mobilização de recursos (materiais e humanos) para legitimar ações estratégicas na Amazônia. A burocracia brasileira especializada em questões de segurança nacional, contrainteligência e políticas ambientais não coordena entre si consenso mínimo para viabilizar uma agenda política comum que possa mobilizar atividades socioambientais capazes de contemplar os *interesses estratégicos nacionais* e da cidadania brasileira. Ao contrário, protagonizam disputas por narrativas hegemônicas, as quais propagam convicções reducionistas, a fim de obter mais visibilidade na opinião pública brasileira que legitime orçamentos maiores para suas pastas. De modo reduzido, este artigo pretende trazer primeiros esboços de uma geopolítica ambiental.

A epistemologia do segredo: geopolítica ambiental e planos estratégicos para a mineração na Amazônia brasileira.

As burocracias estatais especializadas em lidar com estratégias de defesa possuem em suas constituições funcionais a aura do segredo. Pesquisar burocracias estatais especializadas com a temática da Segurança Nacional torna recorrente expressões tais como: *dados sensíveis; confidencial; dado negado; dado ostensivo;* tramita em *segredo administrativo; informação classificada;* entre outras. As práticas de informação nessas burocracias especializadas são regulamentadas em ordenamento jurídico específico que disciplina a divulgação de dados e informações em poder dos órgãos de Inteligência.

Este artigo busca argumentar de que modo narrativas que fazem uso dessas categorias procuram legitimar (ou deslegitimar) ações institucionalmente edificadoras de realidades amazônicas.[3] No Brasil, o aparato jurídico-legal sobre acesso à informação e o Serviço de Inteligência fundamenta-se nos seguintes dispositivos: Lei nº 9.883/1999 que institui o Sistema Brasileiro de Inteligência e cria a Agência Brasileira de Inteligência (ABIN); Decreto nº 4.376/2002 que dispõe sobre a organização e o funcionamento do Sistema Brasileiro de Inteligência (SISBIN); Decreto nº 8.905/2016 que aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções de Confiança da Agência Brasileira de Inteligência; Lei nº 12.527/2011 que regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37; e no § 2º do art. 216 da Constituição Federal. Nos EUA, a regulamentação e a disponibilização de documentos estão mais consolidadas. Eles têm o *U.S. Department of State Freedom of Information Act* que não só regulamenta o acesso aos documentos produzidos pelo governo federal dos EUA, mas também centraliza

3 A leitura de Max Weber (1979) sobre a dominação legitima estabelece três tipos puros: tradicional, carismático e legal. Veremos que o domínio em virtude da legalidade, na validade do estatuto legal (lei), é a mais reivindicada nas disputas sobre a Amazônia.

nos serviços do *National Archives and Records Administration,* em prédio próprio, a maioria dos documentos já desclassificados, além de disponibilizar serviços on-line de acesso.

De acordo com Eva Horn e Sara Ogger (2003, p. 66), o que diferencia o tipo de Inteligência produzida por servidores públicos militares e civis, entocados em seus gabinetes, arquivos e repartições, do conhecimento construído em universidades, é sua *epistemologia do segredo.* Isso cria, ainda segundo essas autoras, um peculiar efeito de hipnose e paranoia. O segredo e a natureza fechada do serviço de Inteligência obstaculizam qualquer competição, desde instrumentos de correção até a mensuração dos ganhos com os esforços empregados (medidas de eficiência e eficácia). Os serviços de Inteligência, em cooperação com o aparato de guerra, projetam inúmeros cenários hipotéticos de guerra, catástrofes naturais, tudo o que coloque à prova a capacidade de as agências governamentais manterem a segurança nacional, i.e., ratificar a aptidão de reproduzir o poder dos Estados nacionais e de proteger os interesses dos que se vinculem a ele. A sanha da *máquina de guerra* (DELEUZE & GUATTARI 1992) se transforma no furor das ações estratégicas que se projetam na premissa de uma *guerra permanente* (LEIRNER, 2009). O consenso na literatura especializada é que coletar e interpretar são o que caracterizam o trabalho de Inteligência (KENT, 1945; HILSMAN, 1958; BETTS, 1978; HEYMANN, 1985; LAQUEUR, 1985; HAMILTON, 1987; HERMAN, 1996; SHULSKY, 1992; WARNER, 2002; SCOTT & JACKSON, 2004). Coleta de dados ostensivos (públicos), manejo de fontes e produção de informações em investigações próprias com agentes de campo são um lado da moeda. O outro lado contém processamento, avaliação, interpretação e, o mais importante, repasse da informação para decisão dos formuladores de políticas públicas, os quais decidem agir com base nos diagnósticos apresentados (HORN & OGGER 2003, p. 68)[4]. Esses dois lados de uma mesma moeda compõem o que a literatura especializada denomina de trabalho de Inteligência e, mesmo que desde os atentados de 11 de setembro de 2001 nos EUA, essa concepção venha recebendo pesadas críticas e se reformulando, ainda é a fórmula empregada.

Há uma extensa literatura especializada que procura codificar os trabalhos de Inteligência dentro dos Estados modernos contemporâneos. Geralmente, os próprios operadores da máquina administrativa que executa os trabalhos de Inteligência também são seus maiores formuladores. Por exemplo, Mark M. Lowenthal, presidente do Intelligence & Security Academy (LLC) dos EUA e ex-membro da CIA, define Inteligência como sendo algo que se refere a dados reconhecidamente ou declaradamente necessários para informar *policy makers* e que tenham sido coletados, processados e especificados para suprir tais demandas. Nas próprias palavras do autor:

> *Intelligence is a subset of the broader category of information. Intelligence and the entire process by which it is identified, obtained, and analyzed respond to the needs of policy makers. All intelligence is information; not all information is intelligence (…) Intelligence is the process by*

4 A separação entre o analista de informação e o agente de campo no modelo de Inteligência norte-americana levou a críticas da NSA, CIA e do FBI após os ataques suicidas de 11 de setembro de 2001.

> *which specific types of information important to national security are requested, collected, analyzed, and provided to policy makers; the products of that process; the safeguarding of these processes and this information by counterintelligence activities; and the carrying out of operations as requested by lawful authorities* (LOWENTHAL, 2009, p. 1-8)[5].

Essa definição estabelece a Inteligência estatal como processo de informar mediante uma demanda por informações específicas que orientem políticas governamentais, significando requerer, coletar, disseminar e produzir certos tipos de informações estratégicas para os interesses que alguns julguem como da nação e do Estado. Assim, Inteligência é todo o processo de coleta e análise de informação que se formula em organizações estatais com a função de reproduzir orientações nacionais estratégicas de defesa, proteção, projeção de poder geopolítico, entre outros. Ainda de acordo com essa literatura específica, as agências de Inteligência existem por quatro razões principais: evitar surpresas estratégicas; promover *expertise* em longo prazo; dar suporte ao processo político; e manter o sigilo de informação. Para as questões acerca da *Amazônia* e dos mecanismos político-administrativos e político-militares de formulação de uma geopolítica ambiental amazônica, precisamos reconhecer a necessidade de um serviço de Inteligência instrumentalizado e capaz de exercer suas funções de planejamento em longo prazo.

Na literatura norte-americana especializada, há relativo consenso em relacionar Inteligência com segurança nacional, i. e., política de defesa e política externa, por um lado, e segurança territorial e segurança interna, por outro. As instituições brasileiras seguem a mesma doutrina, mas ainda com pouca publicação. No Brasil o *Gabinete de Segurança Institucional* (GSI) tem promovido, por meio da *Secretaria de Acompanhamento e Estudos Institucionais,* seminários, congressos e publicações na área. Há também nas universidades centros e institutos voltados para as questões estratégicas e de Inteligência, geralmente vinculados às pesquisas de departamentos de Relações Internacionais, Ciência Política e História. Outra instituição que converge para promover discussões e publicações nessa temática no Brasil é a Associação Brasileira de Estudo de Defesa (ABED). Mesmo havendo uma distinção entre temáticas e objetos de Inteligência e política estratégica quando comparamos Brasil e EUA, percebemos que em termos conceituais as publicações brasileiras ainda acompanham a doutrina da segurança nacional norte-americana.

Desde a aprovação do *National Security Act* (1947), em acréscimo com outros atos administrativos do executivo, que instituíram a Agência de Segurança Nacional (National Security Agency), o Conselho Nacional de Segurança (National Security Council) e a Agência Central de Inteligência (Central

5 "Inteligência é um subgrupo de uma categoria mais abrangente de informação. Inteligência e todo o processo pelo qual ela é identificada, obtida, e analisada, respondem às necessidades dos legisladores (policy makers). Toda inteligência é informação; nem toda informação é inteligência. [...] Inteligência é o processo em que tipos específicos de informação, importantes para a segurança nacional, são solicitados, coletados, analisados e apresentados aos legisladores; os produtos deste processo; a salvaguarda dos processos e da informação por meio de atividades de contrainteligência; e a realização de operações por demanda das autoridades competentes" (tradução livre).

Intelligence Agency)[6], a *Inteligência* nos EUA mudou bastante com os ataques de 11 de Setembro de 2001 e a aprovação da Lei nº 108-458 *(Intelligence Reform and Terrorism Prevention Act,* de 2004). As práticas de Inteligência norte-americanas precisaram se reinventar porque a ameaça à *segurança nacional* não era mais uma questão de guerra convencional contra exércitos instituídos, mas contra insurgentes contra seus próprios governos pró-EUA e militantes com convicções político-religiosas profundas. No início do século XXI, há uma aproximação da Inteligência estatal com atores não-estatais na formulação de novas estratégias de produção de informação (LOWENTHAL, 2009, p. 5).

Por sua vez, a Inteligência brasileira foi reformulada pela Lei nº 9.883, de 7 de dezembro de 1999 e pelo Decreto nº 4.376, de 13 de setembro de 2002, que institui o *Sistema Brasileiro de Inteligência,* cria a Agência Brasileira de Inteligência (ABIN) e estabelece a integração das ações de planejamento e execução da atividade de Inteligência no Brasil. A redemocratização do país demandou um novo modelo de Inteligência. De acordo com a lei 9.883,

> [...] entende-se como Inteligência a atividade que objetiva a obtenção, análise e disseminação de conhecimento dentro e fora do território nacional sobre fatos e situações de imediata ou potencial influência sobre o processo decisório e a ação governamental e sobre a salvaguarda e a segurança da sociedade e do Estado.

Nem todas as agências ou sistemas de Inteligência no mundo são comparáveis. Elas exercem funções e possuem objetivos distintos conforme as legislações de cada Estado. Os principais modelos de Inteligência são os da: Inglaterra (M15, M16 e *Government Communications Headquarters)*; China *(Central Military Commission e Communist Party)*; França (DGSE – *Généreale de la Sécurité Extérieure,* desde 1982); Rússia (antiga KGB – *Soviet Socialist Republic State Security Committee)*; e o de Israel *(Mossad)*. O modelo brasileiro se aproxima mais do norte-americano, na medida em que possui várias agências estatais integradas em um sistema com uma agência central, sendo os controles e as fiscalizações externas exercidos pelo Congresso Nacional.

Trazendo essa discussão para refletirmos sobre o impacto do aparato de Inteligência para o planejamento da Amazônia brasileira, aludimos à questão da *geopolítica ambiental*. Não é novidade relacionar riscos de segurança nacional com as crescentes questões ambientais. Johan Holst (1989), Alexander López (2009), Thomas Homer-Dixon (1991; 1994; 1995; 1996), Andrew Hurrell (1992), Ans Kolk (1996), entre outros, realizaram pesquisas que vinculam a politização e a militarização dos desafios ambientais no mundo e se aproximam do que denominamos *geopolítica ambiental*. Em termos analíticos, a Amazônia como região estratégica está cada vez mais politizada e militarizada dentro de construções teórico-empíricas da região, o que impacta diretamente nas formulações técnico-burocráticas de instituições estatais e não-estatais. Não há uma limitação evidente, as formulações das instituições estão muito

6 É na administração do presidente Herry Truman (1945-1949) que é instituída a lei de Segurança Nacional nos EUA. A bibliografia especializada atribui a este ato presidencial uma completa mudança da organização das Forças Armadas dos EUA, dando novos contornos à condução da política externa.

atreladas às análises acadêmicas, havendo muita porosidade nos enunciados. Por exemplo, há preocupações com hipóteses de escassez de recursos ambientais e o impacto disso em conflitos sociais. Algumas das análises, tanto acadêmicas quanto de instituições estatais, apontam para a deterioração das condições ambientais que desfrutamos hoje, o que causará consideráveis riscos de desestabilização social (violência civil, conflitos étnicos, insurgências, desobediência civil, guerras por recursos naturais). Muitas das previsões dizem que mudanças ambientais levarão a profundas consequências sociais. Não é difícil, como temos analisado, perceber que a Amazônia entra tanto na ordem das proposições de potenciais soluções às ameaças de *mudança climática* quanto na ordem prática de estabelecimento de ações territoriais efetivas para concretizar decisões políticas.

Os significados operacionais da *guerra permanente* opõem os Estados nacionais: por um lado, o aparato de Inteligência dos EUA procura projetar para além de suas fronteiras os objetivos nacionais. Nesse sentido, cada vez mais a Amazônia constitui ponto relevante para a segurança interna dos EUA quando se fala em recursos naturais, mudança climática, escassez de água, produção de alimento, metais estratégicos (por exemplo, nióbio); por outro lado, o aparato de Inteligência brasileiro desempenha o papel de desarticular interesses estranhos aos objetivos nacionais brasileiros (contrainteligência), idealmente, disposto a exercer sua função de promover os interesses internos; contudo, com o enorme desafio de limitar as ingerências políticas. Esse é o jogo posto. Só que muitos outros jogadores estão em campo além dos aparatos de Inteligência estatais e para além do que se julgue interesse nacional e objetivos nacionais.

Outros atores no jogo geopolítico: minerais estratégicos, tecnologia e sociedade civil.

Instituições não-estatais possuem convicções bastante diversas, porém se assemelham em alguns aspectos na medida em que procuram realizar suas convicções particulares ao mesmo tempo em que instrumentalizam operações estatais, a fim de concretizar missões e interesses que se atribuem. Mesmo que no nível das proposições não haja fronteiras rígidas entre práticas estatais e não-estatais, as instituições estatais elaboram narrativas estratégicas e possuem competências de planejamento com execução orçamentária pública e se servem de uma formalidade diferenciada em termos de operacionalidade de agentes públicos investidos em cargos públicos. As organizações não-estatais combinam narrativas ativistas direcionadas a programas, obras e projetos específicos, muitas vezes, vinculados a recursos e regulamentações estatais, mesmo sendo uma ação privada[7]. Aqui, optamos por analisar uma instituição não-estatal, Organização Não-Governamental (ONG), que se coloca como contraponto para pensar os limites, os

7 Há ampla área de pesquisa interdisciplinar que discute as relações entre poder público e privado. Contudo, foge de competência deste artigo fazer levantamento exaustivo dessa temática (RUA, 1998; ABRUCIO, 2002).

conflitos e as interferências de ações estatais e demonstrar como as disputas por conceitos estão para além do aparato estatal.

É nesse sentido que iremos analisar o documento que a ONG *Environmental Defense Fund* (EDF), organização da sociedade civil estadunidense que atua na defesa de direitos indígenas e na preservação da floresta amazônica em cooperação com ONGs brasileiras, elaborou, no fim da década de 1990, para contrapor argumentos de que os interesses norte-americanos em questões indígenas e ambientais tinham, antes de quaisquer convicções humanitárias e ecológicas, um viés geopolítico para conservar minerais potencialmente estratégicos. O Fundo consultou os anuários produzidos pelo *Bureau of Mines*, órgão vinculado ao *U.S. Department of the Interior*. Os documentos analisados pelo EDF foram: Mineral Commodity Summaries, 1995; e "Potentially Critical Materials (Bureau of Mines, OFR-28-88, Division of Policy Analysis, March 1988). O *Bureau of Mines* produzia anualmente relatórios de acompanhamento de minerais estratégicos no mundo. Com base nesses documentos o EDF afirma que

> [...] pensar que a política internacional gira em torno de depósitos de matéria prima é a geopolítica do século passado (séc. XIX), geopolítica jurássica. Recursos naturais são menos 'estratégicos' do que a tecnologia que os transforma. E ainda, se não fosse assim, os norte-americanos estariam se preocupando com o subsolo do Canadá, da África do Sul e da Rússia muito antes do da Amazônia.

O EDF procura desconstruir a perspectiva de que haveria um "complô planetário" para se apropriar ou para se manter em reservas minerais estratégicas na Amazônia brasileira. De acordo com o EDF, o argumento do "complô planetário" pressupõe dois fatos: primeiro que existem na Amazônia recursos em escassez nos mercados internacionais; segundo que há reservas minerais excepcionais na Amazônia. Com base nisso, imagina-se que a defesa de direitos indígenas está a serviço de um controle do mercado de minérios, gerando um grande concerto estratégico para controlar essas reservas. O documento do EDF procura desfazer esses dois pressupostos. Primeiro, diz que o Brasil só tem 12% (doze por cento) da reserva de ouro do mundo, portanto, uma importância relativa com relação ao ouro. Com relação ao estanho (feito da cassiterita), o Brasil possui a maior reserva mundial, mais do que o dobro do segundo colocado (China), contudo, de acordo com o documento do EDF, os EUA possuem uma enorme reserva interna, além de o estanho ser produto superabundante no mercado internacional. A Associação de Países Produtores de Estanho (APPE) realiza esforços para diminuir a oferta para obter preços mais vantajosos. Portanto, não é um mineral estratégico, na perspectiva do EDF. Mesmo que fosse, a mudança tecnológica pode mudar esse quadro a qualquer momento. O EDF diz:

> [...] quando nos meados da década de 1980, o Paranapanema abriu a mina de Pitinga, no Amazonas, virou as costas para a APPE e encheu o mercado internacional com grandes quantidades de cassiterita de alto teor de estanho. Resultado: o preço caiu pela metade e os mineiros bolivianos, cujos custos de produção eram maiores, e cujo minério era de teor mais baixo de estanho, foram para a rua. Ninguém, nos EUA, que importa estanho, se preocupou nem um pouco.

Ainda segundo o documento do EDF, com relação a diamantes industriais, o Departamento de Minas dos EUA avaliava que o Brasil possuiria 15 milhões de quilates de reserva base, "quase nada perto da Austrália, que tem 900 milhões, ou do Zaire, com 350 milhões". O maior argumento é acerca dos minérios realmente estratégicos que têm aplicabilidade na produção bélica e na indústria aeroespacial. O documento do EDF analisa o documento "Materiais Potencialmente Críticos", publicado pelo *Bureau of Mines*, OFR 28-88, Division of Policy Analysis (1988). O documento analisa 14 substâncias-chave de uso em alta tecnologia dos quais os EUA dependem da importação e que não possuem estoques suficientes. Alguns exemplos são: o germânio (Ge) "usado nos instrumentos de ótica infravermelha, sistema de direcionamento e mira de armas, sensoriamento remoto e outros"; háfnio (Hf) que é o "único material admissível para varas de controle nos reatores nucleares dos submarinos da marinha dos EUA"; gálio (Ga) utilizado em "instrumentos óticos-eletrônicos e lasers para fibras óticas dos mais avançados". O relatório do EDF conclui que para esses 14 metais estratégicos existiria um país com reservas importantes, em oito desses casos, o Canadá:

> O Brasil aparece, uma vez, como uma das cinco fontes principais de alumina (o *galium* ocorre como subproduto da transformação da bauxita em alumina). O Departamento de Minas fez essa listagem em 1988 e, depois, não fez mais. É difícil acompanhar as mudanças tecnológicas, tanto em materiais novos para alta tecnologia quanto em processos de produção.

O relatório da EDF afirma que muito dos materiais estratégicos são subprodutos do processamento de um ou mais metais comuns, demandando processos mais qualificados de processamento para se aferir benefício comercial e industrial da mineração. A Amazônia brasileira tem reservas consideráveis de minerais "não-estratégicos", como ferro, manganês e bauxita, "mas a oferta mundial é abundante e barata".

De acordo com o especialista do EDF, durante a preparação do artigo sobre metais estratégicos, o levantamento anual e a publicação do boletim sobre os metais estratégicos no mundo foram suspensos sem explicação prévia. O especialista, com quem conversei, afirmou que ligou nos órgãos competentes para saber a razão do fim do monitoramento. Segundo ele, o responsável pelo levantamento afirmou que não havia mais minerais estratégicos no mundo porque isso dependeria da tecnologia. O estratégico é a tecnologia, portanto, o mineral pode mudar de prioridade com facilidade. Também a extração é o mais complexo. Garantiu ainda que não adianta ter o mineral na terra, é preciso ganho de escala para viabilizar economicamente a extração.

Em pesquisa na *Library of Congress* em Washington D.C., consegui encontrar o *U.S. Geological Survey*, vinculado ao Departamento do Interior, que ainda mantém o monitoramento e a publicação desse material. Agora em bases muito mais amplas. Eles monitoram 91 substâncias. Por exemplo, no último levantamento, o Brasil possui 84% da reserva mundial de nióbio (Nb), Canadá 9%, Alemanha 2%, Estônia 2%, outros 3%. O nióbio é considerado um metal extremamente estratégico por

ser um supercondutor com potencial uso em processadores mais sofisticados do que os de silício para a indústria aeroespacial, tem utilização na indústria nuclear e na produção de jatos e foguetes. A pesquisa do EDF ainda precisa ser atualizada porque o monitoramento continua sendo feito e o cenário mudou um pouco na medida em que o Brasil possui a maior reserva de nióbio. O Brasil produz 91% do minério comercializado no mundo. O segundo maior produtor, o Canadá, é responsável por 7% da produção mundial. A dependência norte-americana do nióbio brasileiro é ponto de preocupação deles. Recentemente o site WikiLeaks publicou um relatório do *Homeland Security Department* em que se expõe essa dependência classificando-a de preocupante (REF: STATE 6461).

Podemos tirar algumas conclusões de uma geopolítica amazônica que envolva o Estado brasileiro e o Estado norte-americano, organizações não-governamentais brasileiras e norte-americanas, todos atuando na lógica do *governo do território*. Primeiro, é fato que existe um aparato político-institucional nos EUA interessado em práticas de gestão ambiental e governança global que se traduzem em monitoramentos de ofertas de minerais classificados como "materiais potencialmente críticos", entre outros tópicos. Segundo, o monitoramento de oferta de minérios e o financiamento a instituições não-estatais interessadas em gestão ambiental não significam necessariamente que haja um complô por trás para destituir a soberania brasileira sobre seu território. Terceiro, pode-se argumentar sobre a legitimidade de interesses comerciais estratégicos em matérias-primas em território brasileiro na medida em que tais interesses procurem prever comercialmente a oferta internacional de produtos, sem politizar a questão. Quarto, não há dúvidas, dentro dos atuais pressupostos do direito internacional público, que a regulamentação da extração de minerais estratégicos e do governo territorial da Amazônia brasileira cabe ao poder público brasileiro.

Conclusões

Tanto os articuladores de teorias da conspiração quanto os atores institucionais mais pragmáticos de instituições brasileiras concordam que o poder dos EUA se faz sentir em diversas instâncias institucionais que lidam com a Amazônia: seja no financiamento de sua infraestrutura; no desenvolvimento de empreendimentos privados; em financiamento de ONGs; na influência de missionários religiosos; na venda de tecnologia de monitoramento aeroespacial; em acordos bilaterais de processamento de imagens de satélites para monitorar desmatamento; e em modelos e concepções de preservação ambiental. Ou seja, a presença dos EUA se faz sentir em múltiplas dimensões.

Em última instância, podemos concluir que a Amazônia se torna uma peça de ficção codificada em conceitos, regulamentações legais e convicções políticas que não expõem as contradições de suas formulações internas. Apresentam-se ao público verdades especializadas com pouco espaço de contestação e reflexão. Nesse sentido, as narrativas burocráticas, intelectuais, ambientais, militares, comerciais, históricas, jurídicas, midiáticas e não-governamentais pavimentam fluxos de conhecimento entre as redes especializadas e o público em geral, sem

prover, efetivamente, trâmites contraditórios próprios das reflexões, edificando narrativas de verdades hegemônicas, impróprias para contextos socioambientais tão diversos como o território amazônico.

A geopolítica ambiental no século XXI é sutil e se apresenta na necessidade de dominação técnica, no controle do conhecimento em patentes, na logística de compra e venda de minerais estratégicos que precisam de escala para se tornar rentáveis, e no processamento da natureza. Não adianta ter a maior reserva de nióbio do mundo se não se processa sua potencialidade industrial e tecnológica. É fundamental pensar nas potencialidades internas que, em última instância, só se realizam em território estrangeiro ou com recurso estrangeiro. Instituições estadunidenses procuram influenciar os interesses brasileiros, estabelecendo a lógica das políticas para a Amazônia, em uma dinâmica de troca de dólares por natureza (exportação de recursos naturais ou preservação da floresta). Ou seja, em nossa análise, as instituições estatais e não estatais dos EUA utilizam-se de mecanismos financeiros para prover recursos tecnológicos, investimentos, diminuição de dívidas, entre outros, em troca de opinar no destino da floresta e dos recursos naturais do território amazônico. Por sua vez, em geral, instituições brasileiras estatais e da sociedade civil pouco fazem para integrar suas ações no nível estratégico. Na maior parte do tempo, as instituições brasileiras exercem papel subsidiário no jogo transnacional de conhecimento estratégico sobre a Amazônia à medida que pouco promovem a integração interna com orientação estratégica. Assim, assuntos como monitoramento aeroespacial, controle de desmatamento, empreendimentos de infraestruturas para garantir o suprimento de matéria prima para o mercado internacional, oferta de produtos agropecuários *in natura* (soja, laranja, algodão e proteína animal), vigilância das fronteiras terrestres, criação de áreas protegidas, entre outros, são desmembrados e não integram um plano nacional para a Amazônia brasileira.

Referência

ABRUCIO, Fernando Luiz e Marcos Vinícius. Trajetórias da literatura sobre reforma do Estado (1995-2002): transformações e desafios para a pesquisa em Administração Pública. *Relatório de pesquisa* ENAP. Brasília: ENAP, 2002.

BECKER, Bertha. Geopolítica da Amazônia. *Estudos Avançados* 19 (53), 2005.

BETTS, R. Analysis, war, and decision: why intelligence failures are Inevitable. *World Politics, Princeton,* n. 31, out. 1978.

CARVALHO, J. M. Cidadania no Brasil: o longo caminho. 5. ed. Rio de Janeiro: Civilização Brasileira, 2004.

DELEUZE, Gilles & Féliz Guattari. O que é a Filosofia? Trad. de Bento Prato Jr. e Alberto Muñoz. Rio de Janeiro: Editora 34, 1992.

DURKHEIM, Emílio. As formas elementares da vida religiosa. São Paulo: Martins Fontes, 1996.

FOUCAULT, Michel. *Em defesa da sociedade. Curso no Collège de France* (1975-1976). Trad. de Maria Galvão. São Paulo: Martins Fontes, 2005.

_____ *A verdade e as formas jurídicas.* Trad. de Roberto Cabral Machado e Eduardo Jardim Morais. Rio de Janeiro: NAU Editora, [1973] 2003.

HAMILTON, Lee. *The Role of Intelligence in the Foreign Policy Process.* Essays on Strategy and Diplomacy. Claremont, CA: Claremont College, Keck Center for International Strategic Studies, 1987.

HERMAN, Michael. *Intelligence Power in Peace and War.* New York: Cambridge University Press, 1996.

HEYMANN, Hans. Intelligence/Policy Relationships. In: *Intelligence: Policy and Process.* Ed. Alfred C. Maurer and others. Westview Press, 1985.

HILSMAN, Roger. *Strategic Intelligence and National Decisions.* Glencoe. Free Press, 1958.

HOLST, Johan. Security and the Environment: A Preliminary Exploration. *Bulletin of Peace Proposal,* no. 29 (2), pp.123-128, 1989.

HOMER-DIXON, Thomas. On the Threshold. Environmental Change as Cause of Acute

Conflict. *International Security,* vol.16, no.2. pp. 76-116, 1991.

_____ Environmental Scarcities and Violent Conflict: Evidences from the Cases. In: *International Security,* v.19, n. 1, summer, p. 5-40, 1994.

_____ *Strategies for Studying Causation in Complex Ecological Political Systems.* Toronto. Occasional Paper for the project on Environment, Population and Security, 1995.

_____Debate. In: *Environmental Change and Security Project Report,* issue 2, pp. 49-57, 1996.

HORN, Eva ; Sara Ogger. *Knowing the Enemy:* The Epistemology of Secret Intelligence. Published by The MIT press, 2003. Disponível em: <www.jstor.org/stable/1262623>. Acesso em: 11 maio 2003.

KENT, Sherman. *Strategic Intelligence for American Foreign Policy.* Princeton: Princeton University Press, 1945.

KOLK, Ans. *Forests in International Environmental Politics.* Utrecht: International Books, 1996.

LA BLACHE, Paul Vidal de. *Princípios de Geografia Humana.* 2. ed. rev. Lisboa (Portugal): Ed. Cosmos, 1954.

LAQUEUR, Walter. *A World of Secrets:* The Uses and Limits of Intelligence. New York: Basic Books, 1985.

LEIRNER, Piero. Etnografia com militares: fórmula, dosagem e posologia. In: *Antropologia dos militares: reflexões sobre pesquisas de campo.* Celso Castro e Piero Leirner (orgs). Rio de Janeiro: Editora FGV, 2009.

LÓPEZ, Alexander. The Brazilian Amazon in an Environmental Security and Social Conflict Framework. In: *Facing Global Environmental Change.* Springer Berlin Heidelberg (Publisher), v. IV. June 04, 2009.

LOWENTHAL, Mark M. *Intelligence from Secrets to Policy.* Fourth Edition. Washington, DC: CQ Press, 2009.

MASSEY, D. *Pelo espaço: uma nova política da espacialidade.* Trad. de Hilda Pareto Maciel e Rogério Haesbaert. Rio de Janeiro: Bertrand Brasil, 2008.

MEDEIROS, R. A. L. de. *Decodificando a internacionalização da Amazônia:* análise de uma Geopolítica Ambiental. Brasília: Tagore Editora, 2018. v. 1. 503p.

MIYAMOTO, Shiguenoli. *O Pensamento Geopolítico Brasileiro* (1920 – 1980). Dissertação de Mestrado. Faculdade de Filosofia, Letras e Ciências Humanas da USP. São Paulo, 1981.

NORTH, Douglass. *Institutions, Institutional Change and Economic Performance.* Cambridge University Press, 1990.

PICKLES, J. *A history of spaces:* cartographic reason, mapping and the geo-coded world. Londres e Nova Iorque: Routledge, 2004.

RATZEL, F. *Géographie Politique.* Paris: Éditions Régionales Européennes, [1903] 1988.

RIBEIRO, Gustavo Lins. Ambientalismo e Desenvolvimento Sustentado. Nova Utopia/ Ideologia do Desenvolvimento.. *Revista de Antropologia,* n. 34, p. 59-101, 1991.

RUA, Maria das Graças. Análise de Políticas Públicas: Conceitos Básicos. In: Maria das Graças Rua; Maria Carvalho (Org.). *O Estudo da Política:* Tópicos Selecionados. Brasília: Paralelo 15, 1998.

SCOTT, Len and Peter JACKSON. *The Study of Intelligence in Theory and Practice.* Intelligence and National Security 19: 139-169; Summer 2004.

SODRÉ, Nelson Werneck. *História Militar do Brasil.* 3. ed. Civilização Brasileira, 1979.

SPRANDEL, M. A. Breve genealogia sobre os estudos e fronteiras e limites no Brasil. In: CARDOSO DE OLIVEIRA, R.; BAINES, S. G. (org.). *Nacionalidade e etnicidade em fronteiras.* Brasília: Ed. UnB, 2005.

STEINBERGER, M. A influência alemã na geografia política do Brasil. In: MENEZES, A.; KOTHE, M. (org.). *Brasil-Alemanha 1827-1997*: perspectivas históricas. Brasília: Thesaurus, 1997.

WEBER, Max. Os três tipos puros de dominação legítima. In: Max Weber. Col. *Grandes Cientistas Sociais.* Org. e trad. Gabriel Cohn. São Paulo: Ática, 1979.

_____ *Economia e sociedade:* fundamentos da Sociologia Compreensiva. v. 1 e 2. Trad. de Regis e Karen Barbosa. São Paulo/Brasília: Imprensa Oficial e Editora UnB, 2004.

AS RELAÇÕES BRASIL-ÁFRICA SUBSAARIANA NO CONTEXTO DA ATIVIDADE DE INTELIGÊNCIA

Jorge Luís dos Santos Alves *

Resumo

O artigo examina as relações entre o Brasil e os Estados da África Subsaariana e tem o propósito de delinear a posição da Atividade de Inteligência no processo de tomada de decisão em um ponto específico e relevante da política externa brasileira: a política africana. A África Subsaariana constitui um amplo espaço geoestratégico aberto para a projeção econômica e política brasileira e no qual a Atividade de Inteligência está vocacionada a atuar na busca de oportunidades e detecção de ameaças. Os países africanos de língua portuguesa são casos exemplares do potencial e dos obstáculos dessas relações no campo da Atividade de Inteligência. São abordadas as características da realidade contemporânea da África e os interesses externos ali atuantes. Descreve as linhas básicas da política africana do Brasil e o papel dos serviços de Inteligência africanos no aparato estatal de segurança. Por fim, busca contextualizar as atribuições e competências da ABIN na temática das relações afro-brasileiras.

Palavras-chaves: Agência Brasileira de Inteligência; Atividade de Inteligência; Relações Brasil-África Subsaariana.

BRAZIL-SUB-SAHARAN AFRICA RELATIONS IN THE CONTEXT OF THE INTELLIGENCE ACTIVITY

Abstract

This study aims at examining the relations between Brazil and the Sub-Saharan African States from the point of view of the Intelligence Activity and its position in the decision-making process of a specific and relevant point of the Brazilian foreign policy: the African policy. Sub-Saharan Africa is a broad strategic space open to Brazilian economic and political projection and in which the Intelligence Activity is geared towards acting in search of opportunities and detection of threats. The Portuguese-speaking African countries exemplify the potential and obstacles regarding these relations. We discuss the characteristics of Africa's contemporary reality and the foreign interests acting there. We describe the basic lines of the Brazilian policy for Africa and the role of the African intelligence services in the state security apparatus. Finally, we seek to conceptualize ABIN attributions and competencies within Afro-Brazilian relations.

Keywords: *Agência Brasileira de Inteligência; Intelligence Activity, Brazil-Sub-Saharan Africa Relations.*

* Doutor em História pela Universidade do Estado do Rio de Janeiro (UERJ). Oficial de Inteligência da Agência Brasileira de Inteligência (ABIN).

Artigo recebido em abril/2018
Aprovado em outubro/2018

Introdução

O artigo examina as relações Brasil-África Subsaariana[1] com ênfase nos Países Africanos de Língua Oficial Portuguesa (Palop) integrantes da Comunidade dos Países de Língua Portuguesa (CPLP) e sob o enfoque de que estas relações propiciam oportunidades de projeção dos interesses do Brasil no ambiente externo. Nesse contexto, pretendemos analisar e refletir como a Agência Brasileira de Inteligência (Abin), órgão central do Sistema Brasileiro de Inteligência (Sisbin), pode contribuir para a identificação dos óbices e potenciais vantagens dessas relações e, desse modo, propiciar maior eficácia no processo de tomada de decisões. Os Palop serão abordados como exemplos da presença de oportunidades capazes de alavancar a projeção econômica e política do Brasil. A primeira premissa do estudo é que a cooperação e a interação com os serviços de Inteligência africanos constituem instrumentos para alavancar a melhoria da segurança coletiva em áreas de conflito ou naquelas identificadas com o entorno estratégico do Brasil (a costa ocidental da África). A segunda premissa é que há um conjunto de oportunidades, inexploradas ou subutilizadas, de projeção de poder do Brasil na África no qual a Atividade de Inteligência é chamada a exercer a sua atribuição de subsidiar de forma prospectiva e preventiva o processo decisório nacional e as ações de governo.

Inicialmente, abordamos a realidade contemporânea da África e os interesses externos ali atuantes (europeus, norte-americanos e chineses). Em seguida, é descrita a política africana do Brasil e os motivos de a África ser um campo de oportunidades aos interesses do Brasil tendo como recorte os Palop. No terceiro tópico, são enfocados os serviços de Inteligência africanos e a sua inserção no aparelho de segurança do Estado e, por fim, situamos o "lugar" potencial da Inteligência de Estado na elaboração e na execução da política africana do Brasil.

Para a elaboração desse estudo, foram empregadas a literatura especializada sobre a temática africana e a Atividade de Inteligência, inclusive os documentos relativos à Política Nacional de Inteligência (PNI) e à Estratégia Nacional de Inteligência (ENI), e fontes disponíveis na internet.

Panorama da África subsaariana

A compreensão da realidade africana deve ter como pressuposto a heterogeneidade cultural, política e social do continente. É um ponto comum entre os africanistas brasileiros (Alberto da Costa e Silva, José Flávio Sombra Saraiva, Pio Penna Filho) a percepção de que a mídia nacional destaca as catástrofes naturais e humanas, os conflitos políticos e sociais; enquanto os aspectos positivos são quase ignorados. Estas percepções dicotômicas geram e reforçam estereótipos que dificultam uma estratégia duradoura dos interesses do Brasil na África (SARAIVA, 2008, p. 89-91).

Dois fatores contribuem para a configuração

1 A África Subsaariana é a porção do continente africano que se estende do deserto do Saara em direção ao sul margeada pelos oceanos Atlântico e Indico.

da realidade africana contemporânea: a herança do colonialismo e a estrutura do Estado africano pós-colonial. O colonialismo europeu foi de curta duração, mas altamente deformador das instituições africanas endógenas. O europeu alterou, em período relativamente curto, as estruturas sociais e políticas, introduziu novas formas de organização da vida sócio-econômica e desenhou fronteiras que escapavam à lógica interna das sociedades pré-coloniais.

Os Estados pós-coloniais na África criaram estruturas semelhantes àquelas dos Estados colonizadores sem possuírem recursos financeiros e estruturas econômicas adequadas para sustentá-las. Assim, formaram-se burocracias numerosas, geralmente recrutadas no meio étnico do qual se originava a liderança política, a exemplo dos quimbundos em Angola, dos balantas na Guiné-Bissau, dos baoulés na Costa do Marfim e dos sereres no Senegal. Os recursos para sustentar essas burocracias são extraídos das atividades produtivas do campo (agricultura, mineração) em benefício das elites inseridas nas burocracias civil e militar. Neste processo, há uma transferência de renda durante a qual os camponeses são obrigados a plantar gêneros para exportação (algodão, cacau, café, borracha, chá) em detrimento de gêneros de subsistência (arroz, feijão, mandioca, milho, sorgo). As Caixas de Estabilização, criadas para regular os preços das matérias-primas, atuam como instrumentos de transferência de recursos do campo para a cidade (M'BOKOLO, 2011, p. 641-642). Esta situação constitui um dos agentes do estado endêmico de insegurança coletiva no continente, pois as constantes guerras civis no período pós-colonial podem ser interpretadas como guerras do campo contra a cidade mesmo quando adquirem contornos ideológicos (Guerra Fria) ou étnicos (Guerra de Biafra). Os conflitos se desdobram em saques ou alianças com negócios ilícitos para financiar clientelas políticas e milícias. Configurou-se, assim, a imagem de falência do Estado na África se pensarmos na sua organização de acordo com o modelo ocidental e desconsiderando-se a permanência de estruturas sociais e tradições políticas pré-coloniais (FERREIRA, 2014, p. 137-144).

O quadro político, econômico e social da grande maioria dos países da África Subsaariana na última década do século XX caracterizou-se por um cenário em que o Estado pós-colonial parecia vergar sob o peso da crise econômica, do esgotamento dos regimes políticos monopartidários, da corrupção, do genocídio e do saque dos recursos naturais. Aos fatores humanos, somaram-se catástrofes naturais, às quais, por certo, não são alheias as ações antropogênicas, a exemplo da seca no Sahel e de epidemias (HIV/AIDS). No início do século XXI, o cenário que dava razão à vertente pessimista de leitura da África foi matizado por dinâmicas externas e internas ao continente. No plano econômico, o *boom* das *commodities* impulsionado pela expansão econômica chinesa proporcionou a entrada de recursos que trouxeram certa estabilização política, muito embora permanecessem os vícios da corrupção, do patrimonialismo e da burocratização. No plano político, desde o fim dos anos 1980, a África testemunha a transição do monopartidarismo, das ditaduras personalistas e dos governos militares para o pluripartidarismo, embora nem sempre haja garantia de concorrência eleitoral equilibrada. Ainda inacabada,

a transição política é dinamizada por pressões externas e pressões domésticas impulsionadas por mobilizações populares e pressão de grupos da oposição (SARAIVA, 2015, p.25-28).

Esta situação constitui o pano de fundo do funcionamento dos serviços de Inteligência (SIs) africanos, da sua percepção pela sociedade civil em relação à legitimidade e da sua influência nas relações de cooperação ou antagonismo com os serviços congêneres.

Panorama dos interesses europeus, norte-americanos e chineses na África

No início do século XXI, ocorreu a renovação do interesse de diversos atores internacionais pela África[2]. Os interesses europeus, notadamente as antigas potências coloniais (França, Portugal, Reino Unido) adquiriram novos contornos inseridos no conjunto de ações de política externa da União Europeia (UE). O Reino Unido, através da Comissão para a África (criada em 2004), propôs soluções para a erradicação da pobreza, o combate à corrupção e o desendividamento dos países africanos com o emprego de "soluções técnicas visando ao desenvolvimento" que se opõem à abordagem norte-americana baseada em critérios políticos (democracia) e de segurança (guerra ao terror) (HUGON, 2009, p.130-131). A França substituiu as ações "paternalistas" (fundos de ajuda ao desenvolvimento e cooperação militar) nas suas antigas colônias africanas por uma estratégia multilateral de valorização da relação União Europeia/ África. Esta estratégia, contudo, não é isenta de oscilações e ambiguidades, como demonstra a intervenção militar nas guerras civis em Côte d'Ivoire em 2004 e 2011, no Mali e na República Centro-Africana (RCA) em 2013. Para os Estados Unidos da América (EUA), os países da África Subsaariana de maioria ou parcela significativa de confissão islâmica, casos de Nigéria, Níger, Somália e Sudão, adquiriram importância geopolítica em razão da disseminação do fundamentalismo religioso, considerado fonte de recrutamento para os grupos terroristas Al Qaeda no Magreb (AQIM), Al Shabaab e, a partir de 2014, o Boko Haram e o Estado Islâmico (EI).

O petróleo constitui outra dimensão da política estadunidense para a África, e o Estado insular de São Tomé e Príncipe é representativo dessa questão. De um lado, empresas norte-americanas obtiveram a concessão para exploração de petróleo (Chevron, ExxonMobil) e, de outro, a posição geográfica (Golfo da Guiné, entre o delta do rio Níger e a foz do rio Congo) faz do arquipélago um "porta-aviões" natural capaz de monitorar países ricos em hidrocarbonetos, a saber, Gabão, Guiné Equatorial, Nigéria e República do Congo (ex-Congo Brazzaville). A criação de um comando militar para o continente (Africom) e a recriação da IV Frota (Atlântico Sul) explicitam as intenções

2 Alguns autores apontam para uma nova partilha da África com participação ativa de Estados emergentes: Brasil, China, Índia e Turquia. Além dos atores estatais, cresceu ou renovou-se a presença de organizações não-governamentais, empresas transnacionais, igrejas e organismos internacionais, a exemplo de Organização das Nações Unidas (ONU), União Europeia, União Africana e CPLP. (CARMODY & OWUSU, 2011, p. 235).

de projeção de poder dos EUA na África baseada no enfrentamento ao terrorismo e na segurança energética.

Outro ponto importante das agendas norte-americana e europeia ocorre no campo das ideias e do poder simbólico. No processo de transição política da África Subsaariana na passagem do século XX ao XXI, houve a difusão de uma agenda de valores considerados "naturais" e essenciais para a reforma das estruturas estatais: a democracia, os direitos humanos, o livre-mercado e a governança. A adesão a esses valores (ainda que de caráter formal) representa, para as elites dirigentes africanas, a oportunidade de obter recursos na forma de investimentos ou doações dos EUA e da UE. A pressão externa por reforma do Estado foi simultânea à expansão das redes criminosas transnacionais e à ameaça do terrorismo, que trouxeram para as potências ocidentais um novo valor estratégico para a África Subsaariana, embora numa dimensão secundária em relação a outras regiões do planeta (PLESSIS, 2005).

Portugal foi o último império colonial a se retirar da África. Após 14 anos de guerras coloniais (1961-1975), a revolução de abril de 1974 iniciou um processo abrupto de descolonização. Nos Palop, a memória do colonialismo desperta animosidade e desconfiança em relação ao antigo colonizador e provoca resistências no âmbito da CPLP (SARAIVA, 2015, p. 110). Portugal ainda possui interesses econômicos robustos no continente, notadamente em Angola, e políticos articulados à cooperação militar e estratégica no Atlântico Sul (BERNARDINO, 2011). Mas não é uma via de mão única, pois, para a África lusófona, a relação com Portugal é uma via de comunicação com a EU e constitui uma forma de manifestar e defender os seus interesses junto a um dos principais polos de investimento e ajuda internacional.

O que dinamizou e abriu novos cenários nas relações externas dos países da África Subsaariana foi o ciclo expansivo da economia da China. A inserção chinesa na África ocorre desde o período da descolonização. As relações sino-africanas eram então guiadas por motivações político-ideológicas enunciadas na Conferência de Bandung (1955), por exemplo, o apoio aos movimentos de libertação nacional e a cooperação bilateral. A necessidade de fontes de abastecimento de matérias-primas (hidrocarbonetos, minérios, madeira, gêneros agrícolas) em razão da expansão econômica constitui o cerne da política externa chinesa para a África no inicio do século XXI. Ao contrário das potências ocidentais, a atuação chinesa nos países africanos não está limitada por contingências de ordem ambiental, política ou direitos humanos. Na África, a China aproveitou o vazio do pós-Guerra Fria para afirmar-se como potência global a partir de meados da década de 1990. A expansão chinesa caracteriza-se pela concepção da não-intervenção nos assuntos internos dos Estados africanos, muitos dos quais acusados de violação dos direitos humanos (Sudão) ou má governança (Zimbábue). Nesse sentido, a China propõe um modelo concorrente aos valores ocidentais de organização do Estado, o que, além de vantagens no campo econômico, proporciona uma alternativa de aliança nas relações internacionais. Os investimentos chineses na África e as exportações desta para a China representaram uma ruptura,

entre as economias africanas e as economias europeias, do modelo vigente desde o período colonial; o intercâmbio sino-africano prossegui após as independências e formou uma relação de dependência. No entanto, a relação com a China não alterou as características das trocas comerciais, que permaneceram centradas na exportação de *commodities* e na importação de bens manufaturados e serviços, mas ganharam a participação ativa de redes mercantis controladas por africanos (SARAIVA, 2008, p. 309-310; TAYLOR, 2010, p. 76).

A política africana do Brasil

A política africana do Brasil caracteriza-se pela oscilação e pela descontinuidade. Estratégias de aproximação são sucedidas por afastamentos motivados por injunções da política externa e interna (adoção do neoliberalismo econômico, fim da guerra fria e globalização) ou pela priorização de resultados políticos e econômicos imediatos (SARAIVA, 2015, p. 95-96; FARIAS, 2017, p. 91-149). Entre a última década do século XX e meados da segunda década do século XXI, ocorreram dois momentos distintos nas relações Brasil-África. A década de 1990 caracterizou-se por uma diminuição gradativa da importância estratégica da África para o Brasil em razão da redefinição de prioridades da política externa. No governo Lula da Silva, ocorre um redimensionamento da agenda diplomática do País com o incremento da cooperação sul-sul, na qual a África Subsaariana adquiriu nova centralidade na formulação da política externa. São marcas desse período a diplomacia presidencial, a inserção de grandes grupos nacionais na economia de países africanos nos setores de construção pesada e mineração, e a celebração de acordos de cooperação nas áreas técnica, humanitária, educacional, econômica e militar (JORGE, 2015, p. 50-57). No contexto do *boom* das *commodities* de meados dos anos 2000, a reorientação da estratégia diplomática do Brasil trouxe um crescimento expressivo do intercâmbio comercial, um objetivo permanente das relações com a África Subsaariana desde os anos 1960. Os seguintes vetores indicam a conjuntura da política africana do Brasil nas primeiras décadas do século XXI:

1. A priorização de projetos de desenvolvimento como obras de infraestrutura, transferência de tecnologia "tropicalizada" brasileira, a produção de biocombustíveis adequada às necessidades locais e políticas de acesso a medicamentos para combater HIV/AIDS, a malária e a tuberculose. Empresas brasileiras estabeleceram, ou ampliaram, as suas atividades na África (Odebrecht, Petrobrás, Vale) e intensificaram-se as ações de cooperação de instituições públicas, a exemplo da Embrapa em Gana e Moçambique e da Marinha na Namíbia (JORGE, 2015, p. 50-57).

2. A concertação da política bilateral orientada para a África do Sul, a Nigéria e os países da África lusófona (principalmente Angola). Mas houve também uma ambiciosa extensão da presença diplomática materializada na abertura ou na reativação de 19 embaixadas em países até então em segundo plano, casos do Sudão e de Benim, e na visita do presidente Lula da Silva a 24 países do continente (JORGE, 2015, p. 43). A diplomacia presidencial

do governo Lula foi o instrumento mais visível da retomada da política africana[3] ocorrida em sincronia com a percepção de um sentimento de "renascimento africano" materializado na fundação da União Africana (UA).[4] A diplomacia brasileira incrementou ainda a participação em fóruns multilaterais: a CPLP, o Fórum de Diálogo Índia-Brasil-África do Sul (IBAS), e a iniciativa América do Sul-África (ASA), cuja primeira cúpula foi realizada em Abuja (Nigéria) em 2006. As iniciativas supramencionadas visavam a conquistar apoio para a obtenção de uma vaga no Conselho permanente das Nações Unidas. Atrelado a este objetivo, o Brasil tem integrado Missões de Paz em Angola, Guiné-Bissau e RDC.

3. A aproximação cultural (*soft power*) devido aos laços histórico-culturais que demonstram o longo percurso comum com as nações africanas e a sua contribuição na construção da brasilidade. Além disso, nos países africanos lusófonos, é bastante difundida a produção da indústria cultural brasileira (música, programas de televisão). Desde a última década do século XX, o *soft power* brasileiro tem se manifestado de uma nova forma. Trata-se da expansão das igrejas evangélicas lideradas por missionários brasileiros com expressiva presença nas mídias locais e importante atuação social em Angola e Guiné-Bissau (MASSEY, 2016).

4. As relações com os Estados africanos situados na vertente atlântico-sul adquiriram maior relevância estratégica conforme os objetivos da Política e da Estratégia Nacional de Defesa (PND/END) (BRASIL, 2016, p. 6). Nestes documentos, a Defesa incorpora, ao seu pensamento estratégico, o Atlântico Sul, área por onde transitam de 70% a 80% do transporte marítimo do Brasil e ponto cada vez mais sensível na geopolítica mundial em razão do potencial de petróleo e gás natural tanto no litoral do Brasil quanto no da África Ocidental. Também é uma área de crescente insegurança marítima em razão das ações de pirataria no Golfo da Guiné (ABDENUR e SOUZA NETO, 2014, p. 5-21).

Não obstante as oportunidades econômicas e políticas apresentadas pelos países africanos, a volatilidade político-social do continente pode propiciar a emergência de situações desfavoráveis para o interesse nacional brasileiro. O desconhecimento, ou o conhecimento insuficiente, das complexas realidades locais dificulta a formulação de estratégias eficazes tanto na esfera pública quanto na privada nas relações Brasil-África. Neste contexto, a ampliação de parcerias e o intercâmbio de informações entre as instituições componentes do Sisbin, coordenado pela Abin, e os serviços de Inteligência africanos são fundamentais para delinear cenários e as suas variáveis mais próximas da realidade.

Os países africanos de língua oficial portuguesa

3 A priorização das relações Brasil-África na agenda da política externa do País é frequentemente criticada por uma fração dos formadores da opinião pública e dos setores intragovernamentais que defendem uma estratégia político-diplomática orientada para o "norte" (EUA e Europa Ocidental).

4 A UA sucedeu a Organização da Unidade Africana (OUA). Fundada em setembro de 2002 e com sede em Adis Abeba/Etiópia, a UA pretende promover a democracia, os direitos humanos e o desenvolvimento na África.

Em julho de 1996, os Chefes de Estado e de Governo de Angola, Brasil, Cabo Verde, Guiné-Bissau, Moçambique, Portugal e São Tomé e Príncipe decidiram a criação da CPLP com três focos básicos: a concertação político-diplomática, a valorização da língua portuguesa e a cooperação técnica, científica e tecnológica. Os Palop têm pouco mais de quarenta anos de existência independente e possuem estruturas políticas ainda em consolidação ou mesmo bastante frágeis. Desde as independências (1975), as antigas colônias portuguesas na África foram objeto da estratégia político-diplomática do Brasil com base na língua e no reconhecimento de um fundo histórico com laços comuns cuja característica fundamental é a herança colonial. Como foi mencionado, a política africana teve inflexões e recuos que não significaram uma ausência completa. No governo Lula da Silva, a aproximação do Brasil com os Palop foi marcada pelo incremento dos investimentos de empresas brasileiras (principalmente em Angola e Moçambique) e de acordos de cooperação técnica nas áreas de agricultura, saúde, educação e capacitação profissional para desenvolvimento industrial, meio ambiente, segurança pública, administração pública, energia e indústria (IPEA/BANCO MUNDIAL, 2011).

Os Palop apresentam características econômicas, sociais e políticas bastante distintas que explicitam o equívoco de tratar o continente africano de forma homogênea e reducionista.

Angola destaca-se pela grande população, pelos seus recursos naturais (petróleo, diamantes, ferro) e uma forte expansão econômica na primeira década do século XXI. A partir de 2014-2015, contudo, a economia angolana entrou em crise com a queda dos preços do petróleo (TV 5 MONDE, 2017). No contexto africano, Angola tem uma política externa bastante ativa voltada para o Golfo da Guiné (São Tomé e Príncipe e Guiné Equatorial), a Guiné-Bissau e a África Central, notadamente a RDC, onde apoia o governo de Joseph Kabila.[5]

Moçambique, ainda muito dependente da cooperação internacional, tem desenvolvido projetos agrícolas (soja) e de exploração mineral (carvão e gás natural). O país adquiriu relativa estabilidade política após quase duas décadas de guerra civil e é visto pela comunidade internacional como um "caso modelar de inserção internacional altaneira na ordem internacional do início do século XXI" (SARAIVA, 2008, p. 99). No entanto, Moçambique enfrenta grave crise financeira e alto endividamento externo.

Os demais países da África lusófona possuem espaço territorial e economias mais modestas. Cabo Verde e São Tomé e Príncipe são estados insulares, com recursos insuficientes para a garantia do bem-estar econômico e social dos seus cidadãos. No entanto, a localização geográfica é um ativo destes países. Cabo Verde constitui uma encruzilhada nas rotas aéreas e marítimas do Atlântico Sul para a Europa. Pobre de recursos naturais, o país depende da ajuda internacional e das remessas de divisas

5 Sobre a política externa angolana nestas regiões, ver Angola no Golfo da Guiné e Atlântico Sul. *Africa Defence & Security:* 16 nov. 2016. Disponível em: <africadefesaeseguranca.wordpress.com/2016/11/16/angola-no-golfo-da-guine-e-atlantico-sul/> Acesso em: 20 ago. 2017.

efetuadas pelos imigrantes. A estabilidade política e a boa governança do arquipélago constituem outro ativo importante para as relações de Cabo Verde junto às instituições e doadores externos. São Tomé e Príncipe está situado numa área crítica da segurança da África Ocidental – o Golfo da Guiné – assolada pela pirataria marítima à qual se soma o enorme potencial de petróleo e gás natural que se estende do continente para o mar. O país padece de crônica instabilidade política e corrupção (FRANCISCO e AGOSTINHO, 2011), mas o potencial econômico e a posição estratégica atraem o interesse chinês e o russo em projetos de infraestrutura, por exemplo, a construção de um porto em águas profundas e um aeroporto internacional.[6] A Guiné-Bissau apresenta um quadro cíclico de instabilidade e violência política. Nenhum governo conseguiu terminar o mandato e guerras civis (1998/1999 e 2011/2012) agravaram a pobreza do país, alvo de missões de paz de 1999 até o presente. A instabilidade crônica atraiu o crime organizado transnacional influenciando a expansão da economia informal fundamentada no ilícito, na corrupção e na cooptação das elites civis e militares (MASSEY, 2016). Os parcos recursos disponíveis pelas forças de segurança (militares e policiais) são assimétricos aos lucros potenciais das seguintes atividades ilícitas: o tráfico de drogas, o tráfico de pessoas, o contrabando de cigarros e de madeira. Em meados dos anos 2000, o cenário de um narcoestado[7] em formação era percebido pelos observadores internacionais que apontavam a crescente ingerência das redes criminosas no aparato estatal e que culminaram nos conflitos de 2011 e 2012 (UNODC, 2013).

A atividade de Inteligência e os desafios à segurança coletiva na África

Os Estados africanos enfrentam ameaças originadas por fatores exógenos, p. ex., o terrorismo e a atuação das redes transnacionais do crime organizado, e outras endêmicas na realidade do continente: a corrupção, os conflitos étnicos e o saque dos recursos naturais. Estas ameaças constituem desafios à segurança coletiva do continente e são, ou deveriam ser, os temas de interesse a orientar os serviços de Inteligência africanos e as ações de cooperação intracontinental e com os serviços congêneres de fora do continente.

A formação e a prática dos serviços de Inteligência na África Subsaariana estão associadas à estrutura de segurança dos impérios coloniais, marcada por autoritarismo, repressão e combate aos movimentos de libertação nacional. Assim, entre os legados mais fortes do período pós-colonial na África, está a associação dos serviços de Inteligência com a proteção de regimes políticos autoritários civis ou militares. Em Benin, Chade, Moçambique, Níger, República Democrática do Congo (RDC), Somália e Uganda, indivíduos

6 Empresas chinesas preparam investimentos em São Tomé e Príncipe. In: *Voa Portugueses*. 09 jan. 2017. Disponível em: <www.voaportugues.com/a/empresas-chinesas-investimentos-sao-tome-e-principe/3668979.html>. Acesso em: 11 set. 2017.

7 A classificação da Guiné-Bissau como narcoestado é polêmica. Para Shaw, as elites da Guiné-Bissau formaram entre 2005-2014 uma rede de proteção (*elite racketeering*) ao narcotráfico no qual o país era utilizado como ponte da América do Sul para a Europa. (SHAW, 2015).

treinados por CIA, KGB, Mossad e agências de Inteligência das antigas potências coloniais tornaram-se presidentes ou o poder atrás do trono. Relações familiares com o governante eram importantes para ocupar a chefia dos serviços de Etiópia, Guiné, Uganda e RDC (PATEMAN, 1992, p, 570-571).

A transição política dos anos 1990 afetou os SIs, porém, os seguintes desafios – a politização da Inteligência, a falta de capacitação, a insuficiência dos recursos humanos e financeiros, a inadequação ou a ausência de legislação regulatória e o baixo nível de coordenação entre os serviços – permanecem até os dias de hoje e estão imbricados nos problemas estruturais do ordenamento jurídico e do aparato de segurança policial e militar dos Estados africanos após o fim do monopartidarismo. Financiados por doações norte-americanas e da União Europeia, os programas de reforma do aparato de segurança (*security sector reform*) dos Estados africanos reúnem, além da Inteligência, a polícia, os sistemas penal e judiciário; enfrentam obstáculos que refletem o processo, ainda não-consolidado, de democratização. No caso da Atividade de Inteligência, a situação é ainda mais complexa em razão, de um lado, dos vínculos da atividade com governos autoritários, aos quais serve como instrumento de controle da oposição, e de outro, em razão da insuficiência de mecanismos institucionais de controle e supervisão dos SIs aliada à adoção de uma política deliberada de opacidade dos governos africanos no seu gerenciamento, o que dificulta o cumprimento de normas jurídicas e éticas (LALÁ, 2004).[8]

Os SIs africanos tiveram de se adaptar ao cenário do pós-Guerra Fria e responder aos desafios da expansão do crime transnacional, do terrorismo e das crises humanitárias, elementos que impactam a segurança coletiva. Assim, o Comitê dos Serviços de Informações e Segurança de África (CISSA) foi fundado em 26 de agosto de 2004, em Abuja/Nigéria, com o propósito de desenvolver a cooperação multilateral entre os serviços africanos de Inteligência e segurança. Em janeiro de 2005, a assembleia da União Africana (UA) aprovou a criação do CISSA e a sua vinculação àquela organização por meio do Comitê de Informações e Segurança (CIS). O CISSA se propõe a ser o principal provedor de informações a todos os órgãos decisores da UA reforçando a capacidade dessa organização de consolidar e manter a estabilidade no continente.[9] Desde 2005, as reuniões do CISSA ocorrem anualmente em alguma capital dos Estados-membros e os temas de interesse incidem sobre a segurança coletiva, a criminalidade organizada e o terrorismo, tendo como referência a cooperação entre agências. O Comitê tem também, entre os seus objetivos, o enfrentamento ao que os governantes africanos consideram intromissão indevida das potências ocidentais nos seus assuntos internos. É o caso das acusações de violação

8 A exceção no continente foi a África do Sul, que promoveu a reorganização dos seus serviços de Inteligência ainda em 1994 ao fim do *apartheid*. (AFRICA, 2007).

9 O Comitê possui três órgãos: Conferência: constituída pelos Diretores dos Serviços de Informações e Segurança dos Estados-membros. O Painel de Peritos: formado por um representante de cada país-membro do CISSA. O Secretariado, com sede em Adis Abeba/Etiópia, órgão de coordenação junto à União Africana. Os funcionários do Secretariado são oficiais recrutados dos Serviços de Informações e Segurança que aderiram ao CISSA.

dos direitos humanos (Sudão), genocídio (Ruanda) ou restrição das liberdades civis (Zimbábue). A sensibilidade desses temas demarca a atuação dos SIs no interior de estruturas políticas ainda vinculadas a regimes, senão autoritários, pelo menos influenciados por práticas dissociadas da transparência (DEHÉZ, 2010). Alguns exemplos demonstram, senão a instrumentalização dos SIs nas entranhas da política da África Subsaariana, ao menos as dificuldades de controle e fiscalização. Na África do Sul, o controle dos serviços de Inteligência foi apontado por opositores de Jacob Zuma como garantidor da manutenção do seu poder em meio aos escândalos de corrupção e às tentativas abortadas de *impeachment*.[10] Em Angola, um mês antes da realização das eleições presidenciais de agosto de 2017, o presidente José Eduardo dos Santos, que deixava a presidência após 38 anos, obteve a aprovação no parlamento de uma lei que, na prática, colocou as forças armadas, a polícia e os serviços de Inteligência sob o controle do seu círculo político por oito anos.

Traça-se, a seguir, breve exposição dos SIs no âmbito dos Palop para se compreender as características e a dinâmica dessas agências no interior do aparato estatal de segurança.

Em Angola, os SIs formam uma comunidade consolidada a partir da experiência nos conflitos armados que opuseram o governo do Movimento Popular para Libertação de Angola (MPLA) à União para a Independência Total de Angola (Unita), à Frente Nacional de Libertação de Angola (FNLA) e aos seus apoiadores externos, notadamente o regime do *apartheid* sul-africano. O Serviço de Inteligência de Segurança do Estado (SINSE), no campo interno, o Serviço de Inteligência Externa (SIE), no campo externo, e o Serviço de Inteligência Militar (SIM) foram capacitados e treinados pelos serviços congêneres de Cuba e da Europa Oriental e desempenharam importante papel na consolidação do Estado angolano e do domínio do MPLA. Após o fim das democracias populares, a comunidade de Inteligência de Angola buscou adaptar-se aos novos tempos. Para Bonzela Franco (2013, p. 81), a atividade de Inteligência em Angola "é um fato consumado, e vem sendo um campo que cresce dia a dia com a necessidade de diminuir as incertezas e melhorar a projeção da atividade governamental no futuro". Essa projeção inclui o campo externo no qual Angola almeja se tornar uma potência regional, como indica a participação em missões na Guiné-Bissau e na RDC com o auxílio do SINSE e do SIE. O peso econômico, político e estratégico de Angola reflete-se no âmbito do fórum de Inteligência da CPLP, em que o país busca ser um protagonista equivalente ao Brasil e a Portugal e exercer um papel de liderança junto aos SIs dos Palop.

Em Moçambique, o Serviço de Informação e Segurança do Estado (SISE) desempenha um papel assemelhado aos serviços congêneres angolanos, embora com recursos mais modestos, e partilha também problemas institucionais, p. ex., a estreita associação à política governamental do

10 Zuma chefiou a unidade de Inteligência do Congresso Nacional Africano (CNA) durante a luta contra o *apartheid*.

partido situacionista, a Frente de Libertação de Moçambique (Frelimo). Recentemente, o SISE envolveu-se em escândalos políticos e financeiros que impactam negativamente o seu gerenciamento (DEUTSCHE WELLE, 2016). Convém salientar que Moçambique é influenciado pela vizinhança anglófona, principalmente sul-africana, e o espaço geoestratégico do Índico.

Os SIs de Cabo Verde, Guiné-Bissau e São Tomé e Príncipe apresentam organização incipiente e, mesmo entre eles, há diferenças que refletem o grau de governança e a estabilidade política. Em Cabo Verde, o Serviço de Inteligência da República (SIR) encontra-se ainda em processo de consolidação pouco mais de uma década após a sua fundação ocorrida em 2005 (EXPRESSO DAS ILHAS, 2015). Na Guiné-Bissau, as chefias do SI estiveram profundamente envolvidas em conflitos armados e negócios ilícitos que contribuíram para a desestabilização política desse país. Atualmente, o Serviço de Informação e Segurança (SIS) encontra-se em processo de reformulação, adaptando-se ao fortalecimento institucional do Estado bissauense. Na mesma dimensão do SIS, encontra-se o Serviço Nacional de Informações de São Tomé e Príncipe (SINFO).

A maior robustez dos SIs angolanos e, em menor escala, do SI moçambicano mostraria um nível de profissionalização e organização mais complexo quando comparado aos demais Palop e à grande maioria dos demais SIs africanos. No entanto, os SIs dos Palop necessitam adequar-se aos parâmetros da moderna gestão da Atividade de Inteligência que a vincula às políticas de Estado e de forma independente dos interesses partidários. No geral, a qualificação profissional é incipiente. Mantem-se o recrutamento direto de policiais, antigos combatentes das guerras de libertação nacional e militares da ativa e da reserva. A capacitação é direcionada para as atividades operacionais (nas quais o emprego de fontes humanas é essencial). A cultura de contrainteligência e a análise são restritas em boa medida pela insuficiência do sistema formal de ensino. Nesse contexto, a necessidade de capacitação é um dos campos mais oportunos para aproximação junto aos SIs da África Subsaariana.

A Atividade de Inteligência e a política africana do Brasil

A Atividade de Inteligência do Estado brasileiro tradicionalmente está direcionada para o campo das ameaças internas (CEPIK e AMBROS, 2009, p. 32). No entanto, a dimensão continental do Brasil e a multiplicidade de desafios que esta característica traz para o processo decisório nacional não isenta de importância o ambiente externo. A geografia torna imprescindível para a segurança do país uma política externa acurada cuja execução durante muito tempo esteve exclusivamente identificada com a diplomacia. A política de defesa, por sua vez, a partir do último terço do século XX, orientou-se de forma mais sistemática para o litoral atlântico com o alargamento do mar territorial para 200 milhas marítimas (1970) até a concepção da Amazônia Azul (2004) e a noção de entorno estratégico. Das burocracias especializadas que constituem o tripé da segurança nacional

– diplomacia, defesa e inteligência – esta foi a última a deslocar-se do campo interno para o externo de uma forma mais assertiva com a intensificação da nomeação de Adidos Civis de Inteligência a partir de 2016, entre as quais aquela estabelecida na África do Sul, a primeira no continente africano. Embora o estabelecimento da adidância na África do Sul esteja mais vinculada aos interesses associados aos BRICs, ela representa um avanço significativo para a consecução mais eficaz da projeção econômica e política do Brasil na África Subsaariana com a utilização da Inteligência de Estado.

A ampliação da capacidade de "detectar, acompanhar e informar sobre ações adversas aos interesses do Estado no exterior" é uma das diretrizes estabelecidas na Política Nacional de Inteligência (PNI) aprovada em 2016. A sua fundamentação parte da necessidade de a Inteligência produzir conhecimento sobre "as principais ameaças e vulnerabilidades a que estão sujeitas as posições e os interesses nacionais no exterior, como forma de bem assessorar o chefe de Estado e os órgãos responsáveis pela consecução dos objetivos no exterior". Entre as ameaças mencionadas na PNI, encontram-se aquelas que ensejam uma atenção ao campo externo, p. ex., a criminalidade organizada transnacional, o terrorismo, os ataques cibernéticos e a interferência externa. A PNI orienta a projeção externa da ABIN de modo a apoiar a inserção do País no cenário internacional marcado tanto por cooperação e convergência para enfrentar ameaças quanto por competição e busca de oportunidades. A atuação da ABIN deve estar em sintonia "com os preceitos da Política Externa Brasileira e com os interesses estratégicos definidos pelo Estado, como aqueles consignados na Política de Defesa Nacional e na Estratégia Nacional de Defesa" (BRASIL, 2017).

A projeção internacional da ABIN, especialmente na África, enfrenta obstáculos estruturais (as inflexões na estratégia político-diplomática) e conjunturais (insuficiência de recursos financeiros e humanos disponibilizados para a Atividade de Inteligência em um contexto de crise econômica). O aumento das adidâncias na África Subsaariana, eventualmente na Nigéria e em Angola, p. ex., dependeria de avaliação e ajustes para consolidar o processo de projeção da ABIN para o exterior.

No caso específico da política africana, conforme os objetivos listados na PNI e no eixo estruturante Projeção Internacional da Estratégia Nacional de Inteligência (ENI), as ações em proveito dos interesses do Brasil no exterior abrangem o incremento dos acordos de cooperação internacional, a formação de parcerias e a ampliação do intercâmbio de informações.

No Fórum de Informações e Inteligência da CPLP, há o propósito de criar-se um ambiente favorável ao fluxo de dados e conhecimentos sobre temas avaliados como fundamentais no âmbito da CPLP: crimes transnacionais, tráfico de pessoas, imigração ilegal, ameaças das redes sociais e enfrentamento ao terrorismo (PANAPRESS, 2011; ABIN, 2017). Não obstante as dificuldades econômicas conjunturais, o esforço de concertação promovido pelas reuniões anuais do Fórum propicia condições favoráveis para o aumento dos encontros técnicos e a oferta de cursos de capacitação aos Palop, o que contribuiria

para ampliar o grau de integração entre os SIs e o protagonismo da ABIN. Elencamos, a seguir, diversos temas de interesse no intercâmbio de informações entre a ABIN, o SISBIN e os SIs da África Subsaariana.

1. O terrorismo. É o tema principal de acompanhamento de vários SIs da África Ocidental e da África Central, não só em razão do interesse externo, mas também por estar inserido em situações de violência insurrecional na política interna desses Estados e das suas relações com os países vizinhos, como ocorre em Camarões, Chade, Costa do Marfim, Mali, Níger, Nigéria e Quênia (JEUNE AFRIQUE, 2015). No entanto, há percepção de baixo grau de confiabilidade entre os SIs africanos e os ocidentais em razão do colonialismo e de prevenções de caráter ideológico.

2. As redes transnacionais do crime. Há tendência de ampliação do fluxo de drogas em direção ao Brasil ou do transporte de drogas do Brasil para a Europa via África com a possível participação de máfias nigerianas. As características singulares do Estado africano pós-colonial apontam a necessidade de conhecer e avaliar a conexão entre a política, o mundo dos negócios e o mundo do crime para entender os mecanismos de funcionamento das atividades ilícitas no continente e as suas relações com os agentes externos e o seu impacto no Brasil.

3. Os fluxos migratórios. Há registro de crescimento da imigração africana (angolanos, congoleses, nigerianos e senegaleses) principalmente para os grandes centros urbanos brasileiros. A emigração para o Brasil é muito menor do que a realizada para a Europa, mas a legislação mais benevolente para refugiados pode acelerar esse fluxo e o envolvimento de redes de tráfico de pessoas, por exemplo, aquelas atuantes na África Ocidental. Os riscos epidemiológicos (ebola e outras viroses) provocados pelo desequilíbrio ecológico constituem outro foco para acompanhamento.

4. A ampliação do processo de cooperação internacional com o engajamento do Brasil em missões de paz em áreas de conflito na África Subsaariana, p. ex., na RCA, onde atua a Missão Integrada Multidimensional de Estabilização das Nações Unidas na República Centro-Africana (MINUSCA). A RCA vive uma situação conflituosa que envolve risco de genocídio, "limpeza étnica" e disputa por recursos naturais com impacto em estados fronteiriços (Camarões, Chade, Congo Brazzaville, RDC, Sudão e Sudão do Sul) cuja segurança é também bastante frágil (STUENKEL, 2017). A participação do Brasil na MINUSCA representaria o comprometimento maior do país na mediação de conflitos na África Subsaariana.

5. A concertação entre o Brasil e os Estados da África Subsaariana nas Nações Unidas, na Organização Mundial do Comércio (OMC) e na Organização das Nações Unidas para Agricultura e Alimentação (FAO) (JORGE, 2015, p. 49), com desdobramentos no apoio às demandas brasileiras de reforma dos mecanismos de governança global.

6. A intensificação dos negócios junto aos países africanos (investimentos, importação e exportação). Desde os anos 1970, este é o principal campo de interesse do Brasil na África. A importância do interesse

econômico é medida pelo fato de 72% do petróleo importado pelo Brasil ser proveniente da África (Nigéria, Angola, Guiné Equatorial) e o intercâmbio comercial aumentou de US$ 4 bilhões para US$ 26,4 bilhões de 2000 a 2014 (FARIAS, 2017, p. 148).

7. A presença chinesa na África. O engajamento chinês na África é bastante complexo e envolve atores oficiais e não-oficiais, nem sempre com interesses convergentes. O acompanhamento da presença chinesa nos Estados da África lusófona e no Atlântico Sul seria orientado para identificar como as estratégias geoeconômicas e políticas chinesas concorrem, geram ou impulsionam obstáculos e oportunidades à projeção do Brasil.

Há um espaço amplo de cooperação em temáticas comuns a partir do terreno conquistado nas últimas décadas. Mas a efetiva ampliação da cooperação na área de Inteligência de Estado necessita da criação, ou do fortalecimento, de ações específicas voltadas para conhecer e prospectar temas estratégicos das relações Brasil-África Subsaariana. Nesse sentido, seria proveitosa a concepção de programas de capacitação em assuntos africanos que visem à formação de um corpo mínimo de africanistas, assim como ampliar o intercâmbio de informações de forma permanente baseado na identificação de uma pauta de interesses comum.

Por fim, há vantagens intangíveis para que a ABIN possa se inserir de forma competitiva no cenário da Inteligência na África. Trata-se de aproveitar as resistências dos SIs africanos em relação aos países ocidentais identificados com o colonialismo e transferir *expertise* de um país (o Brasil) cuja realidade econômica, social e política está mais próxima das necessidades dos países da África Subsaariana.

Considerações finais

Em artigo de divulgação científica publicado em 2009, Marco Cepik e Christiano Ambros (2009, p. 32) destacavam que faltava ao Brasil "mais capacidade de olhar para o exterior, de produzir Inteligência estratégica e tática relativa a eventos e processos cruciais para o Estado brasileiro e que se desenvolvem fora de nossas fronteiras". Atualmente, a ABIN orienta-se para ocupar com mais vigor um espaço que é próprio às suas atribuições: a prospecção de dados e informações relevantes no ambiente externo, de modo a dar mais consistência ao assessoramento do processo de decisões. Nesse contexto, a África Subsaariana é emblemática em razão das oportunidades e dos desafios apresentados neste artigo. A consolidação da projeção para o ambiente externo necessita do estabelecimento de prioridades que o conectem de forma integrada com o campo interno e dentro da identificação do interesse nacional. Esta estratégia depende da disponibilidade de recursos financeiros (necessários para o eventual estabelecimento de novas adidâncias e a formação de rede de colaboradores) e recursos humanos capacitados para a produção de conhecimentos. No caso da produção de conhecimento sobre a África Subsaariana, ainda incipiente apesar da criação da adidância na África do Sul, a capacitação de servidores especializados em África (africanistas) é crucial para processar

e avaliar dados e conhecimentos de uma realidade complexa, pois, como salienta Hugon (2009, p. 146), a (re)valoração estratégica da África está relacionada, de um lado, à segurança coletiva, a matérias-primas e à biodiversidade; e, de outro, aos "efeitos de bumerangue" produzidos pelos "males da África": as migrações, as epidemias, a exportação da violência e o terrorismo. É um contexto desafiante para o qual a ABIN é chamada a fornecer análises e conhecimentos confiáveis, oportunos e relevantes de modo a subsidiar a projeção econômica e política do Brasil.

Referências

ABDENUR, Adriana Erthal &SOUZA NETO, Danilo Marcondes de. O Brasil e a cooperação em defesa: a construção de uma identidade regional no Atlântico Sul. *Revista Brasileira de Política Internacional*, Brasília, v. 57 (1): 2014, p. 5-21. Disponível em: <dx.doi.org/10.1590/0034-7329201400101>. Acesso em: 15 set. 2017.

ABIN. Serviços de Inteligência dos países de língua portuguesa traçam metas para 2017. Disponível em: <www.abin.gov.br/servicos-de-inteligencia-dos-paises-de-lingua-portuguesa-tracam-metas-para-2017/>. Acesso em: 28 set. 2018.

AFRICA, Sandy. Governing intelligence services in Africa. *Workshop on an African SSR Strategy Agenda and ASSN General Meeting*. Addis Abeba: 9-10 oct. 2007. Disponível em: <africansecuritynetwork.org/.../WorkshoponanAfrica>. Acesso em: 21 set. 2017.

_____ . A África na ordem internacional do século XXI: mudanças epidérmicas ou ensaios de autonomia decisória? Rio de Janeiro: *Revista Brasileira de Política Internacional* n° 51 (1), 2008.

AFRICA DEFENCE & SECURITY. *Angola no Golfo da Guiné e Atlântico Sul*. 16 nov. 2016. Disponível em: <africadefesaeseguranca.wordpress.com/2016/11/16/angola-no-golfo-da-guine-e-atlantico-sul/>. Acesso em: 20 ago. 2017.

_____ . *Angola: the untouchable security and defence apparatus?* 23 jul. 2017. Disponível em: <africadefesaeseguranca.wordpress.com/2017/07/23/angola-the-untouchable-security-and-defence-apparatus/>. Acesso em: 20 ago. 2017.

BERNARDINO, Luís Manuel Brás. A segurança Marítima no Seio da CPLP: Contributos para uma Estratégia nos Mares da Lusofonia. *Nação e Defesa*, n° 128 – 5ª Série, 2011, p. 41-65. Disponível em: <comum.rcaap.pt/bitstream/10400.26/4744/1/NeD128_LuisManuelBrasBernardino.pdf>. Acesso em: 28 out 2017.

BONZELA FRANCO, Marcelino Cristóvão. *A Evolução do Conceito Estratégico do Serviço*

de Inteligência e de Segurança do Estado da República de Angola (1975-2010). Dissertação de Mestrado. Lisboa: Instituto Superior de Ciências Políticas e Sociais, 2013. Disponível em: <www.repository.utl.pt/bitstream/10400.5/7130/1/TESETRABPUBL.pdf>. Acesso em: 19 set. 2017.

BRASIL. Decreto de 15 de dezembro de 2017. Cria a Estratégia Nacional de Inteligência. Gabinete de Segurança Institucional. Brasília: 2017. Disponível em: <www.planalto.gov.br/ccivil_03/_Ato2015-2018/2017/Dsn/Dsn14503.htm>. Acesso em: 19 set. 2018.

_____. Decreto de 29 de junho. Cria a Política Nacional de Inteligência. Disponível em: <www.Abin.gov.br/acesso-a-informacao/legislacao-de-inteligencia/coletanea-de-legislacao/ politica-nacional-de-inteligencia/>. Acesso em: 20 ago. 2017.

_____. Ministério da Defesa. *Política Nacional de Defesa/Estratégia Nacional de Defesa*. Disponível em: <www.defesa.gov.br/arquivos/2017/mes03/pnd_end.pdf>. Acesso em: 21 set 2017.

CARMODY, Padraig & OWUSU, Francis. A Expansão da China para a África: Interesses e Estratégias, p. 235-267. *In:* LEÃO, Rodrigo Pimentel Ferreira, PINTO, Eduardo Costa e ACIOLY, Luciana (Orgs.). *A China na nova configuração global: impactos políticos, econômicos e sociais*. Brasília: IPEA, 2011.

CEPIK, Marco Aurélio e AMBROS, Christiano. Os serviços de Inteligência no Brasil. *Ciência Hoje*, v. 45, n° 265, nov. 2009, p. 28-33.

CONTROLO dos serviços secretos garante manutenção de Zuma no poder. *Rede Angola:* 8 maio 2017. Disponível em: <www.redeangola.info/controlo-dos-servicos-secretos-garante-manutencao-zuma-poder/>. Acesso em: 18 set. 2017.

DEHÉZ, Dustin. Intelligence Services in Sub-Saharan Africa. Making Security Sector Reform Work. *ASPJ Africa & Francophonie* - 3rd Quarter 2010, p. 57-63. Disponível em: <www.airuniversity.af.mil/Portals/10/ASPJFrench/journals_E/Volume-01_Issue-3/dehez_ e.pdf>. Acesso em: 13 set. 2017.

DEUTSCHE WELLE. A quem presta contas a secreta moçambicana? 28 jun. 2016. Disponível em: <www.dw.com/pt-002/a-quem-presta-contas-a-secreta-mocambicana/a-19362702>. Acesso em: 17 out. 2017.

DIÁRIO DE NOTÍCIAS: 16 ago 2017. Disponível em: <www.dn.pt/lusa/interior>. Acesso em: 17 ago. 2017.

EXPRESSO DAS ILHAS. *Serviço de Informações da República: Ninguém fala, é segredo.* 23 fev

2015. Disponível em: <www.expressodasilhas.sapo.cv/politica/item/44034-servico-deinformacoes -da-republica-ninguem-fala-e-segredo>. Acesso em: 25 ago. 2017.

FARIAS, Hélio Caetano. *A estratégia do Brasil na África: fundamentos geopolíticos e mecanismos de financiamento no ciclo recente de expansão econômica (2000-2014)*. Tese de Doutorado. UFRJ. Rio de Janeiro: 2017.

FERREIRA, Patrícia Magalhães. *"Estados Frágeis" em África: A intervenção externa nos processos de construção do Estado (Statebuilding) e da Paz (Peacebuilding)*. Tese de Doutorado. Lisboa: Instituto Superior de Ciências do Trabalho e da Empresa (ISCTE-IUC): 2014. Disponível em: <www.pordentrodaafrica.com>. Acesso em: 7 set. 2017.

FRANCISCO, Albertino e AGOSTINHO, Nujoma. *Exorcising devils from the throne: São Tomé and Príncipe in the chaos of democratization*. New York: Algora Publishing, 2011.

HUGON, Philippe. *Geopolítica da África*. Trad. de Constância Morel. Rio de Janeiro: FGV, 2009.

IPEA/BANCO MUNDIAL. *Ponte sobre o Atlântico, Brasil África Subsaariana: Parceria Sul-Sul para o crescimento*. Brasília: 2011. Disponível em: <www.ipea.gov.br/portal/index.php? option =com_content&view=article&id=12637>. Acesso em: 20 ago.2017.

JEUNE AFRIQUE. *Dossier: Les services de renseignements africains*. 21 a 25 sept. 2015. Disponível em: <www.jeuneafrique.com>. Acesso em 13 out. 2017.

JORGE, Nedilson Ricardo. Relações Brasil-África: Panorama Geral. *Cadernos de Política Exterior/Instituto de Pesquisa de Relações Internacionais:* v. 1, n° 2 (out. 2015). Brasília: FUNAG, 2015.

LALÁ, Anícia. Picturing the Landscape: Police, Justice, Penal and Intelligence Reforms in Africa. *In:* FERGUSON, Chris and ISIMA, Jeffrey (Eds). *Providing Security for People: Enhancing Security through Police, Justice, and Intelligence Reform in Africa*. Shrivehan: Global Facilitator Network for Security Sector Reform (GFN-SSR): 2004. Disponível em:

<s3.amazonaws.com/academia.edu.documents/30125165/providing_security_for_people_enhancing_security_though_police>. Acesso em: 21 set. 2017.

M'BOKOLO, Elikia. *Africa Negra. História e Civilizações,* v. II. Trad. de Manuel Resende. Salvador: EDUFBA; São Paulo: Casa das Áfricas, 2011.

MASSEY, Simon. Global Politics and the failure of securitization in Guinea-Bissau. In: CHABAL, Patrick and GREEN, Toby (eds.). *Guinea-Bissau. Micro-state to 'Narco-state'.*

London: C. Hurst & Co. (Publishers) Ltd., 2016.

PANAPRESS. Serviços Secretos de países lusófonos debatem tráfico de droga em Cabo Verde. Disponível em: <www.panapress.com/Servicos-Secretos-de-paises-lusofonos-debatem-trafico-de-droga-em-Cabo-Verde--3-437862-51-lang3-index.html>. Acesso em: 28 set. 2018.

PATEMAN, Roy. Intelligence Agencies in Africa: A Preliminary Assessment. *The Journal of Modern African Studies.* v. 30, n° 4, p. 569-584, Dec., 1992.

PLESSIS, Inus du. The Impact of a War on Terror on Africa. *Security Strategic Review for Southern Africa,* Pretoria v. XXVII , n° 1, p. 47-65, May 2005.

REDE ANGOLA. Controlo dos serviços secretos garante manutenção de Zuma no poder. 8 maio 2017. Disponível em: <www.redeangola.info/controlo-dos-servicos-secretos-garante-manutencao-zuma-poder/>. Acesso em: 18 set. 2017.

RODRIGO, Pimentel Ferreira Leão et alli (Orgs). *A China na nova configuração global: impactos políticos, econômicos e sociais.* Brasília: IPEA, 2011.

SARAIVA, José Flávio. *A África no século XXI: um ensaio acadêmico. Brasília:* FUNAG, 2015.

SHAW, Mark. Drug trafficking in Guinea-Bissau, 1998-2014: the evolution of an elite protection network. Cambridge: *The Journal of Modern African Studies.* v. 30, n° 3, 2015, p. 339-364. Disponível em: <www.cambridge.org/core/terms>. Acesso em: 15 set. 2017.

STUENKEL, Oliver. Envio de tropas brasileiras à África Central seria boa notícia para o Brasil e o mundo. *El País:* 13 set. 2017. Disponível em: <brasil.elpais.com/brasil/2017/09/12/opinion/ 1505234666_502675.html>. Acesso em: 18 out. 2017.

TAYLOR, Ian. *The International Relations of Sub-Saharan Africa.* New York/London: Continuum, 2010.

TV 5 MONDE. L'Angola, pays pétrolier plongé dans une sévère crise économique. 21 ago. 2017. Disponível em: <information.tv5monde.com/en-continu/l-angola-pays-petrolier-plonge-dans-une-severe-crise-economique-187170>. Acesso em: 21 ago. 2017.

UNODC. *Criminalidade Organizada Transnacional na África Ocidental: Avaliação da Ameaça.* Viena: fev. 2013.

VOZ DA AMÉRICA: 9 jan. 2017. Disponível em:<hwww.voaportugues.com/a/empresas-chinesas-investimentos-sao-tome-e-principe/3668979.html>. Acesso em: 11 set. 2017.

O *HARDWARE* COMPROMETIDO: UMA IMPORTANTE AMEAÇA A SER CONSIDERADA PELA ATIVIDADE DE INTELIGÊNCIA

Gustavo Andrade Bruzzeguez *
Clóvis Neumann **
João Carlos Félix Souza ***

Resumo

As questões ligadas à segurança cibernética são complexas e sofisticadas, e estão em constante transformação. Nos últimos anos, pesquisadores vêm demonstrando a possibilidade de implementação de códigos maliciosos em circuitos integrados (*chips*) durante a fabricação destes dispositivos. A ameaça, que ficou conhecida como hardware Trojan, vem atraindo a atenção dos governos e da indústria, dado que potencialmente envolve questões de espionagem e guerra cibernética. O problema vem se agravando com a globalização da cadeia de fabricação de circuitos integrados, considerando que são comumente manufaturados fora dos limites dos territórios nacionais, o que implica em perda de controle sobre as etapas do processo. O presente artigo objetiva alertar para a existência da ameaça do hardware Trojan, e discorrer sobre a relevância do tema para a área de inteligência, a partir de breve revisão da literatura relativa ao assunto, na qual utilizou-se, do ponto de vista metodológico, o enfoque meta-analítico. Observa-se que o potencial lesivo do hardware Trojan é preocupante, com ações que incluem vazamento de dados, espionagem, ataques de indisponibilidade, disrupção de sistemas, sabotagem, dentre outras. Trata-se, portanto, de uma questão que precisa ser abordada e gerenciada no âmbito dos governos e, em particular, nos serviços de inteligência.

Palavras-chaves: hardware Trojan; Atividade de Inteligência; segurança da informação e comunicação; segurança cibernética.

COMPROMISED HARDWARE: AN IMPORTANT THREAT TO BE ADDRESSED BY INTELLIGENCE SERVICES

Abstract

Issues related to cybersecurity are complex and sophisticated, and are constantly changing. In recent years, researchers have been demonstrating the possibility of malicious codes being inserted into integrated circuits (chips) during the fabrication of these devices. The threat, known as hardware Trojan, has been drawing the attention of governments and industry since it potentially involves espionage and cyber warfare issues. The problem is getting worse with the supply chain globalization, since the chips are often manufactured in factories outside the boundaries of the national territories, which implies a loss of

* Servidor público federal, mestre em Computação Aplicada e especialista em Governança de Tecnologia da Informação. É pesquisador na área de segurança cibernética, tendo participado da elaboração da Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal, no âmbito do Gabinete de Segurança Institucional da Presidência da República.

** Doutor em Engenharia, professor e pesquisador da Universidade de Brasília - UnB.

*** Doutor em Economia, professor do Departamento de Engenharia de Produção - UnB e pesquisador no Programa de Pós-graduação em Ciência da Computação Aplicada - UnB.

Artigo recebido em julho/2018
Aprovado em outubro/2018

control over the process steps. This article aims at warning about the existence of the threat of hardware Trojan and to discuss the relevance of the topic to the intelligence service, starting from a brief review of literature on the subject, in which it was used, from the methodological point of view, the meta-analytic approach. The potential of hardware Trojan is a concern, with actions that include data leakage, espionage, denial of service attacks, system disruption, sabotage, and so on. It is, therefore, an issue that needs to be addressed and managed within the government, and in particular the intelligence services.

Keywords: *hardware Trojan; Intelligence Service; information and communications security; cybersecurity.*

Introdução

Imaginemos uma situação hipotética: um alto executivo do governo, supostamente utilizando um *smartphone* seguro, percebe que seu equipamento está travando sem motivo aparente. Nada parece funcionar, nem mensagens, nem ligações, nem qualquer aplicativo. Ele reinicia o dispositivo e os problemas permanecem. Então retira e reinsere a bateria, além de reiniciar o equipamento várias vezes - tudo em vão. Pareceria um simples problema de hardware se, mais tarde, não se descobrisse que o caso não é isolado. Centenas de milhares de *smartphones* também apresentam o mesmo comportamento mundo afora.

A situação hipotética descrita, adaptada de Villasenor (2010), na verdade ilustra um possível e sofisticado ataque cibernético em larga escala. Em tese, qualquer dispositivo que contenha um circuito integrado no hardware está sujeito a esse tipo de ataque, que será abordado em detalhes nesse artigo.

Na atualidade, os circuitos integrados (CIs), também referidos como "*chips*" de computador, estão presentes em uma infinidade de equipamentos, tais como computadores, celulares, equipamentos de redes computacionais e outros dispositivos eletrônicos, que por sua vez são empregados nas mais diversas áreas, muitas delas estratégicas para um país, a exemplo das Atividades de Inteligência, das comunicações, das infraestruturas energéticas, dos meios de transporte, dos mercados financeiros, em sistemas de defesa, em sistemas de controle de tráfego aéreo, dentre outros.

Os CIs concentram boa parte da "Inteligência" dos equipamentos, o que faz com que qualquer mal funcionamento nesses pequenos dispositivos afete de forma relevante a confiabilidade da máquina ou do sistema no qual ele opera. No entanto, tradicionalmente os ataques cibernéticos não exploravam vulnerabilidades do hardware. A Figura 1 exemplifica ataques em diferentes camadas, como aqueles que exploram o usuário (engenharia social[1]) e os ataques implementados por meio do software (*malwares* e macros em softwares de aplicação; e vírus e cavalos de Tróia[2] em sistemas operacionais).

O hardware, "*the root of trust*" (raiz de confiança), como mencionaram Becker *et al.* (2013) e Bhunia *et al.* (2014), é geralmente considerado a parte do sistema cuja confiança é uma premissa. Até recentemente, essa era uma assunção razoável (VILLASENOR, 2011), mas o cenário vem se alterando. A possibilidade de implementação de códigos maliciosos no nível do hardware – os chamados "hardware Trojans" (HT) – vem sendo estudada e discutida há alguns anos. A globalização da cadeia de fabricação de CIs, principalmente em países asiáticos (BEAUMONT, HOPKINS e NEWBY; 2011), e o aumento da complexidade na fabricação desses dispositivos têm incentivado os debates acerca dos problemas

1 Técnica por meio da qual um agente malicioso procura persuadir um usuário a executar determinadas ações, com o fim de aplicar golpes, ludibriar ou obter informações sigilosas e importantes (CERT.BR, 2017).

2 Tipo de código malicioso que, além de executar as funções para as quais foi aparentemente projetado, também executa funções maliciosas e sem o conhecimento do usuário (Cert.BR, 2017).

de se garantir a confiança no nível do hardware e os riscos decorrentes da perda de controle sobre os processos envolvidos na cadeia de fabricação de *chips*.

Figura 1- Visão esquemática de ataques cibernéticos em diferentes camadas. Adaptada de Iqbal (2011).

O fenômeno vem chamando a atenção dos governos de diversos países, como mencionaram Yoshikawa, Takeuchir e Kumaki (2014), a exemplo dos Estados Unidos, que estruturou, em 2004, o chamado *Trusted Foundry Program* (MCCORMACK, 2006), objetivando assegurar a confiabilidade de sistemas críticos para a defesa nacional. Em 2011, a Austrália liberou ao público seus estudos sobre o tema (BEAUMONT, HOPKINS e NEWBY; 2011), abordando formas de implementação do HT, técnicas de detecção e contramedidas.

Estudos revelam a possibilidade de CIs serem "intencionalmente comprometidos durante o processo de *design*, antes mesmo de serem manufaturados" (VILLASENOR, 2013). Ou ainda, a alteração pode se dar durante o processo de manufatura, como alertaram Becker *et al.* (2013). As possibilidades são diversas e potencialmente envolvem comprometimentos na disponibilidade, na integridade e na confidencialidade de dados que trafegam no hardware.

Não obstante os riscos e danos em potencial, a detecção do HT não é uma tarefa simples, e as técnicas existentes atualmente não são efetivas o bastante para detectá-lo (XIAO et al., 2016). O ex-chefe da Agência Central de Inteligência (CIA) e Agência de Segurança Nacional (NSA), General Michael Hayden, chegou a declarar que a questão de hardware comprometido é um problema que não pode ser resolvido, mas uma situação que deve ser gerenciada (RAWNSLEY, 2011).

Portanto, entender a ameaça e criar capacidade de reação é uma necessidade, e estudos futuros terão que focar na combinação das melhores técnicas de prevenção e detecção para prover equipamentos livres da ameaça do HT (BEAUMONT, HOPKINS e NEWBY; 2011).

O presente artigo aborda breve revisão da literatura a respeito do hardware Trojan, demonstrando a relevância do tema para as atividades de inteligência. Para tal, ilustra as características fundamentais do HT, seu potencial lesivo, possíveis pontos de inserção na fabricação de CIs e aborda ainda algumas formas de implementação. Analisa um tipo de implementação específica, de característica furtiva e dissimulada e de difícil detecção. Na sequência, discute implicações do fenômeno nas atividades de inteligência e introduz visão geral sobre possibilidades de detecção e prevenção da ameaça e os desafios da Contrainteligência. Por fim, ideias conclusivas são apresentadas.

No levantamento das fontes de pesquisa bibliográfica, utilizou-se o enfoque meta-analítico, metodologia que surgiu com o objetivo de dotar as revisões de pesquisa com o rigor, a objetividade e a sistematização necessárias para que se constitua o verdadeiro saber científico (SANCHEZ, 1999). As bases de dados consultadas foram ISI Web of Science[3] e Scopus[4], no período de 2007 a 2017.

Circuitos Integrados

Os CIs são constituídos por uma matriz microscópica de circuitos eletrônicos e outros componentes, tais como resistores, capacitores, diodos e transistores, implantados na superfície de um material semicondutor – como o silício, por exemplo (GOERTZEL, 2013). Dessa forma, o circuito resultante é um *chip* monolítico (inteiriço), que pode ser tão pequeno a ponto de ocupar poucos centímetros ou mesmo milímetros quadrados de área (Figura 2).

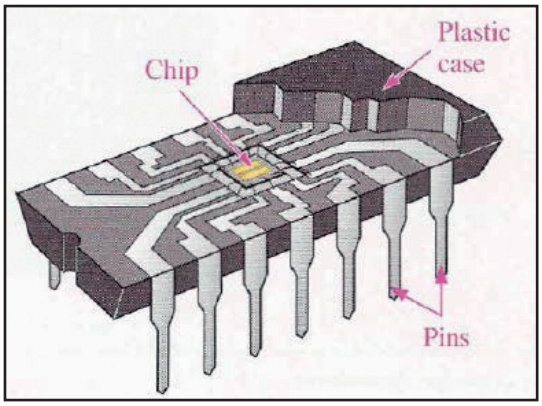


Figura 2 - Visão em corte de um Circuito Integrado típico. Fonte: Floyd (2014)

A fabricação de um CI é um processo complexo que chega a envolver, em alguns casos, mais de quatrocentas etapas (GOERTZEL, 2013). No entanto, visto de uma forma simplificada, pode-se enumerar cinco macroprocessos genéricos, conforme demonstrado na Figura 3.

Conforme Villasenor (2013), o processo de fabricação de um CI se inicia na especificação, que consiste na definição das funcionalidades do CI, incluindo características como velocidade, capacidade de processamento, dentre outras. Na fase do *design*, as especificações são então traduzidas na forma de operações lógicas e, posteriormente, nos circuitos elétricos correspondentes. Uma vez finalizado, o projeto de *design* é então enviado para uma fábrica de semicondutores, onde de fato ocorre a manufatura física do CI. Após essa etapa, testes de qualidade são feitos em amostras do circuito integrado e só então ele estará pronto para ser comercializado e inserido em algum equipamento.

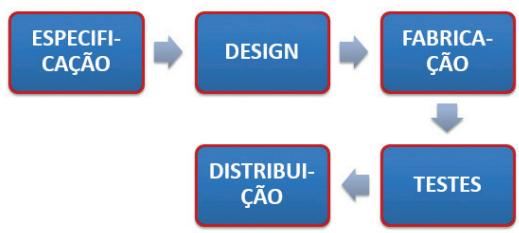


Figura 3 - Etapas da fabricação de um circuito integrado. Adaptado de Villasenor (2013).

3 Disponível em: <www.webofknowledge.com>. Acesso em: 10 set. 2018

4 Disponível em: <www.scopus.com>. Acesso em: 10 set. 2018

O Potencial Lesivo do Hardware Trojan

O hardware Trojan (HT) representa qualquer alteração maliciosa e deliberada no CI (RAJENDRAN *et al.*, 2010). É uma modificação maliciosa, intencional e indesejada no CI, resultando em um comportamento incorreto de um dispositivo eletrônico quando em operação (BEAUMONT, HOPKINS e NEWBY; 2011). São modificações no circuito original inseridas por adversários com o objetivo de expor o hardware ou acessar dados ou software rodando nos sistemas que utilizam o *chip* (TEHRANIPOOR e KOUSHANFAR, 2010).

As consequências de um circuito infectado podem envolver desde modificações na funcionalidade ou na especificação do hardware, conforme apontaram Beaumont, Hopkins e Newby (2011) e Swierczynski *et al.* (2015), passando pelo vazamento de informações sensíveis, efeito citado por diversos autores, a exemplo de Beaumont, Hopkins e Newby (2011); Becker *et al.* (2013); Baumgarten *et al.* (2011), Agrawal *et al.* (2007), Karri *et al.* (2010); e Li, Liu e Zhang (2016); ou mesmo ataques de negação de serviço (Denial of Service – DoS), conforme mencionaram Baumgarten *et al.* (2011); Beaumont, Hopkins e Newby (2011); Chakraborty, Narasimhan e Bhunia (2009); e Tehranipoor e Koushanfar (2010). O hardware Trojan pode ser capaz de derrotar qualquer mecanismo de segurança, seja baseado em software ou hardware, subvertendo ou alterando a operação normal de um dispositivo infectado (BEAUMONT, HOPKINS e NEWBY; 2011). O que pode ser feito em milhões de linhas de código (programação de software), em tese, também pode ser feito com milhões de circuitos impressos em CIs (CLARKE e KNAKE, 2015).

Os HTs não são necessariamente implementados objetivando-se um ataque específico e imediato, mas podem apenas "suportar ataques" (KING et al., 2008), a serem ativados por meio de um gatilho (*trigger*) implementado *a posteriori*. Essa possibilidade permitiria uma espécie de infiltração silenciosa na cadeia de fabricação de CIs, dando ao agente a oportunidade de lançar, em momento oportuno, um "ataque de hardware em larga escala" (VILLASENOR, 2010).

Pontos de Inserção do HT

Dentre as fases envolvidas em um típico esquema de fabricação de circuitos integrados, as mais suscetíveis à inserção do HT são o *design* e a manufatura (CHAKRABORTY, NARASIMHAN e BHUNIA, 2009). As possíveis ações maliciosas nessas fases são descritas a seguir (BHUNIA *et al.*, 2014): no *design*, um agente não confiável que esteja envolvido no processo de escrita do bloco IP (*Intellectual Property* ou Propriedade Intelectual, que constitui o desenho lógico de partes ou blocos funcionais do circuito integrado) pode alterar maliciosamente a lógica, inserindo o HT; ainda nesta fase, o uso de softwares do tipo EDA (*Electronic Design Automation*, ferramentas que facilitam o trabalho de *design*) corrompidos também pode resultar na inserção do código malicioso; e, finalmente, na fase de manufatura, é possível comprometer o CI a partir da ação de um agente mal intencionado, utilizando técnicas

de engenharia reversa.

Implementações do HT

Compreendendo que a ameaça existe e é explorada em diversos momentos na fabricação do circuito integrado, é importante entender como ela é criada e se há meios de detectá-la.

Conforme Becker *et al.* (2013), os esforços de pesquisa concentram-se basicamente em duas áreas: uma relativa ao *design* e implementação do HT; e outra lidando com o desafio de detectar a ameaça.

A seguir, serão apresentados casos de implementação do HT. Em seção posterior, detalhes e possibilidades de detecção e prevenção serão abordadas.

King *et al.* (2008) apresentaram uma forma combinada de ataque envolvendo hardware e software. Neste ataque, um hardware Trojan implementado no CI dá suporte para um ataque por meio do software, ao permitir que o agente malicioso tenha acesso privilegiado (*root*) ao sistema operacional (KRIEG *et al.*, 2013). Tal implementação permite ataques poderosos e de propósito geral, embora utilize pequena quantidade de hardware adicional no circuito (KING *et al.*, 2008). Shiyanovskii *et al.* (2009) apresentaram um HT que implementa um ataque de negação de serviço (Denial of Service - DoS) ao degradar a performance do *chip* de forma gradual. As modificações podem manter os parâmetros iniciais de performance dentro dos padrões aceitáveis de variação, dessa forma permanecendo indetectável pelos testes tradicionais.

A viabilidade de inserção de hardware malicioso em circuitos mapeados em *Field-Programmable Gate Array* (FPGAs[5]) foi discutida por Chakraborty *et al.* (2013). Em particular, os pesquisadores se utilizaram de um HT baseado em um anel-oscilador[6] capaz de reduzir o tempo de vida do *chip* através do aumento da temperatura de operação do circuito.

Em Subramani *et al.* (2017), estudou-se a possibilidade de um ataque de HT em redes *wireless* a partir da infecção de um transmissor 802.11a/g, permitindo ao agente malicioso o vazamento de informações sensíveis na conexão.

Neste artigo, uma implementação específica será abordada com mais detalhes, de forma a demonstrar potencialidades e complexidades da ameaça: o chamado "*Stealthy Dopant-Level Hardware Trojan*" (hardware Trojan furtivo implementado no nível do dopante), proposto por Becker *et al.* (2013).

Trata-se de um HT com duas características peculiares: ele é furtivo ou dissimulado, o que significa que sua detecção não é possível pelos meios convencionais; e ele é implementado no nível do "dopante", ou

5 *Field-Programmable Gate Array*, ou Matriz de Portas Programáveis em Campo, é uma espécie de CI projetado para ser programado após a manufatura. Dessa forma, ele possui blocos lógicos reprogramáveis passíveis de configuração em campo, ou seja, pelo consumidor ou projetista após a fabricação (KRIEG *et al*., 2013).

6 Um anel-oscilador é um circuito serial com número ímpar de portas lógicas e com retorno na entrada. A frequência resultante é uma função do número de portas, da temperatura, dentre outros (KRIEG *et al.*, 2013).

seja, utiliza-se do processo de dopagem do semicondutor.

Conforme Pikma (2013), o processo de dopagem envolve a adição de impurezas no material semicondutor, modificando suas propriedades elétricas. Por exemplo, a adição de átomos de Fósforo ao silício puro atribui-lhe polaridade negativa, enquanto que a adição de átomos de Boro cria polaridade positiva. Esse processo de dopagem é um recurso comumente utilizado na fabricação de transistores que compõem o circuito integrado.

A questão aqui é que o agente malicioso se utiliza desse mesmo procedimento para a implementação do HT, ou seja, ao manipular as polaridades dos transistores presentes no circuito integrado, é possível criar uma lógica maliciosa no funcionamento do CI.

Utilizando-se dessa técnica, Becker *et al.* (2013) provaram que é possível reduzir a segurança dos números aleatórios gerados pelo *Random Number Generator* - RNG (Gerador de Números Randômicos) dos processadores *Ivy Bridge* da Intel (linha de processadores de 22 nanômetros da marca americana), a partir da implementação de códigos maliciosos por meio de dopantes. O RNG do *chip* Intel é uma implementação embarcada no hardware que produz números randômicos de 128 *bits* a partir de ruídos termais. Os números são usados em processos criptográficos.

Com a ação do hardware Trojan, ou seja, com a implementação da lógica maliciosa na fabricação do CI, foi possível reduzir a complexidade da saída do RNG de 128 *bits* para "n" *bits*, no qual "n" pode ser definido pelo atacante, a depender do número de transistores modificados. Essa possibilidade constitui uma importante quebra de segurança na funcionalidade do CI.

Observa-se, ainda, que a ação é possível a partir de modificações em poucos transistores. Em uma das implementações, os autores modificaram apenas 896 transistores (dentre os milhões existentes no *chip*).

Tal tipo de implementação, como mencionado, é extremamente difícil de ser detectada. Conforme se concluiu no estudo conduzido por Pikma (2013), uma vez que o *layout* e a fiação do circuito permanecem exatamente os mesmos quando comparados a um CI não infectado, e considerando que a única diferença está no nível atômico do substrato do semicondutor, esse tipo de HT escapa às formas tradicionais de detecção, como a inspeção ótica, os testes funcionais, ou mesmo a inspeção por uso de *golden chips* (CIs não infectados usados como modelos para comparações).

Caso Síria – Uma Implementação Real?

Em 6 de setembro de 2007, aviões israelenses F-15 Eagle e F-16 Falcon entraram no espaço aéreo Sírio, vindos da Turquia, e bombardearam o que seriam instalações nucleares projetadas pela Coreia do Norte. A imprensa chegou a divulgar ainda suposto envolvimento dos EUA no ataque (CLARKE e KNAKE, 2015).

Não obstante as complexas implicações políticas do episódio, o que chamou a atenção foi o fato de que o sistema de defesa

antiaérea da Síria permaneceu inoperante na ocasião, o que permitiu que os aviões de ataque entrassem e saíssem sem serem alvejados. A Síria havia investido milhões de dólares nos sistemas de defesa antiaérea comprados da Rússia.

Pesquisadores vem trabalhando a hipótese de que o sistema antiaéreo sírio estaria infectado com alguma espécie de *backdoor*[7] inserido nos chips do sistema (QAMARINA, 2017). Cogita-se ainda a hipótese de ter sido, de fato, um hardware Trojan implementado nos sistemas sírios (LI, LIU e ZHANG; 2016). Em outro artigo, Moein *et al.* (2016) destacam a possibilidade de microprocessadores comerciais *off-the-shelf*[8] terem sido adquiridos com um *backdoor* utilizado para desativá-los no momento oportuno. Ou seja, a falha teria sido intencionalmente ativada por meio de um gatilho (*trigger*), em momento definido pelo atacante, conforme defenderam XIAO *et al.* (2016).

A Relevância do Tema para as Atividades de Inteligência

A Política Nacional de Inteligência - PNI (BRASIL, 2016), documento de mais alto nível de orientação da Atividade de Inteligência no Brasil, estabelece, dentre outros, pressupostos, objetivos, instrumentos e diretrizes no âmbito do Sistema Brasileiro de Inteligência (SISBIN).

Neste contexto, declara as principais ameaças às quais o país se sujeita, dentre elas: a espionagem; a sabotagem, sobretudo às infraestruturas críticas do país; e os ataques cibernéticos.

O documento ainda acrescenta que o desenvolvimento das tecnologias da informação e das comunicações impõe a atualização permanente de meios e métodos, obrigando os órgãos de Inteligência a resguardar o patrimônio nacional de ataques cibernéticos.

De fato, conforme demonstrado ao longo do artigo, são inúmeras as possibilidades de ação por meio do uso de HT. Pode-se direcionar um ataque para o vazamento de informações de redes de comunicação na área de defesa ou Inteligência, o que traria graves consequências para a segurança nacional, conforme pontuou Villasenor (2013). Ações de sabotagem ou disrupção de operações militares são possíveis, conforme analisaram Anderson, North e Yiu (2008). A proteção das infraestruturas críticas é estratégica e fundamental para o funcionamento do país (CARUZZO, ZAWADZKI e BELDERRAIN; 2015), e a ação de HTs pode ameaçar todo o sistema de infraestruturas críticas, tais como sistemas financeiros e militares (ALIYU *et al.*, 2014). Enfim, tais inclusões maliciosas de fato agem como "espiões ou terroristas" no CI, e podem ser extremamente poderosas, com consequências catastróficas em diversas aplicações (BHUNIA *et al.*, 2014).

7 O *backdoor* é uma espécie de *malware* que, após incluído em um sistema, é usado para assegurar o acesso futuro ao computador comprometido, permitindo que ele seja acessado remotamente, sem que haja necessidade de recorrer novamente aos métodos utilizados na realização da invasão ou infecção e, na maioria dos casos, sem que seja notado (CERT.BR, 2017).

8 Componentes eletrônicos prontos, de prateleira, com acesso direto para aquisições (KRIEG *et al.*, 2013).

Assim, estamos diante de um instrumento poderoso e potencialmente utilizado em ações de espionagem, sabotagem e ataques cibernéticos, ações essas cujo enfrentamento encontra-se devidamente declarado nas diretrizes da PNI (BRASIL, 2016).

Além disso, a natureza furtiva do HT permite uma infiltração silenciosa, cuja detecção, conforme veremos a seguir, é extremamente complexa, o que o torna um instrumento importante em ações de inteligência.

Detecção e Prevenção do HT e os Desafios da Contrainteligência

As Atividades de Contrainteligência objetivam prevenir, detectar, obstruir e neutralizar a inteligência adversa e as ações que constituam ameaça à salvaguarda de dados, conhecimentos, pessoas, áreas e instalações de interesse da sociedade e do Estado (BRASIL, 2016).

Dessa forma, no contexto do hardware Trojan, as ações de Contrainteligência podem, em tese, atuar antes da inserção do circuito malicioso – na prevenção; e após a ameaça ter se instalado, através da detecção. Neste tópico, serão analisadas as possibilidades e os desafios envolvidos na detecção e na prevenção da ameaça.

Conforme visto, a inserção do HT é possível em diversas fases da criação do CI. Segundo Abramovici e Bradley (2009), não há métodos confiáveis que garantam a detecção de HT antes da utilização efetiva do *chip*. Não há uma solução mágica para detectar todos os tipos de HT (BEAUMONT, HOPKINS e NEWBY; 2011). Assumindo que o atacante pode maliciosamente alterar o *design* antes e após a manufatura, tem-se que a detecção de tais alterações é extremamente difícil, por diversas razões (TEHRANIPOOR e KOUSHANFAR, 2010).

Primeiro, dada a quantidade e a complexidade dos IP cores utilizados nos CIs, detectar pequenas modificações no circuito é extremamente complexo.

Segundo, as características nanométricas dos CIs fazem com que detecções por meio de inspeção física ou engenharia reversa (destrutiva) sejam muito difíceis e caras. Ainda, a engenharia reversa destrutiva (feita em uma amostra) não garante que os demais CIs estejam livres do HT, em especial quando os Trojans são inseridos seletivamente em determinada porção da população de *chips*.

Terceiro, circuitos de HT são geralmente ativados sob condições muito específicas (WANG, TEHRANIPOOR e PLUSQUELLIC; 2008), por exemplo, detectando um sinal específico, como temperatura ou potência, o que os fazem improváveis de serem ativados ou detectados por meio de estímulos funcionais ou randômicos (TEHRANIPOOR e KOUSHANFAR, 2010).

Quarto, testes utilizados para detectar falhas de manufatura, como falhas de atraso (*delay*) não garantem a detecção dos Trojans. Tais testes operam no nível do *netlist* [9] de circuitos livres do Trojan e, consequentemente, não

9 Descrição da conectividade de um circuito eletrônico, conforme Krieg *et al*. (2013).

são capazes de ativar ou detectar os HTs.

Finalmente, uma vez que o tamanho das características físicas de CIs vem se reduzindo em virtude de aprimoramentos na técnica de litografia (processo que imprime a imagem do circuito), variações no processo e no ambiente tem um impacto cada vez maior na integridade da parametria dos circuitos. Assim, a detecção de HT utilizando simples análise desses sinais paramétricos seria inefetiva (TEHRANIPOOR e KOUSHANFAR, 2010).

Assim, há variadas técnicas para a detecção do HT, mas são apenas capazes de detectar classes específicas de Trojan. É de se esperar, como ocorre com os *malwares* de software, que os agentes que projetam HT tentarão escapar de técnicas já conhecidas de detecção, de forma a ter sucesso em seus objetivos (BEAUMONT, HOPKINS e NEWBY; 2011).

Por outro lado, as ações de prevenção buscam impedir que a inserção do HT ocorra. Xiao *et al.* (2016) mencionam três tipos de técnicas de prevenção: ofuscação lógica, que consiste em esconder a funcionalidade genuína de um circuito inserindo mecanismos de bloqueio no *design* original, impedindo portanto que o atacante conheça a lógica (genuína) do circuito, condição necessária para que se projete a lógica maliciosa; camuflagem, um tipo de estratégia de ofuscação no nível do *layout* físico, que consiste na adição de contatos e conexões falsas, dessa forma "enganando" o atacante e impedindo que se extraia a *netlist* correta; e abordagens de preenchimento total de células no circuito, de forma a não deixar espaços vagos no *design*, que poderiam ser utilizados para a inserção do HT.

De fato, não existe uma solução única, que possa garantir proteção segura contra todos os tipos de HT (BHUNIA *et al.*, 2014). No entanto, estratégias que combinem prevenção e detecção podem ser interessantes em cenários que envolvam sistemas críticos e informações sensíveis.

Conclusões

O potencial lesivo do hardware Trojan é preocupante, com ações que incluem vazamento de dados, espionagem, ataques de indisponibilidade, disrupção de sistemas, sabotagem, dentre outros.

O fenômeno envolve uma quebra importante de paradigma na área cibernética, dado que comumente as ameaças são baseadas em software, e não em hardware, em que geralmente a confiabilidade é uma premissa.

Constata-se que o fenômeno hardware Trojan vem preocupando os governos de diversos países, notadamente por envolver, no contexto da guerra cibernética, delicadas questões de espionagem e soberania. De forma geral, países vêm tentando lidar com a ameaça e mitigar os riscos associados, uma vez que o problema não pode ser totalmente eliminado.

O fenômeno traz ainda importantes implicações no contexto das Atividades de Inteligência e da segurança cibernética. A perda de controle na cadeia de fabricação de circuitos integrados, consequência de um modelo forçosamente globalizado por questões de viabilidade econômica, aliada ao crescimento da complexidade dos *chips*, trouxeram relevantes desafios não só para a prevenção da ameaça, como para a sua

detecção.

Como a grande maioria dos sistemas críticos de um país é baseada em arquiteturas que utilizam a Inteligência de circuitos integrados, a ameaça pode trazer relevantes prejuízos para a segurança nacional, devendo ser considerada no âmbito das ações e objetivos das Atividades de Inteligência.

Referências

ABRAMOVICI, Miron; BRADLEY, Paul. *Integrated circuit security: new threats and solutions.* Workshop on Cyber Security and Information Intelligence Research: Cyber Security and Information Intelligence Challenges and Strategies (CSIIRW 09), p. 0–2, 2009.

AGRAWAL, Dakshi; BAKTIR, Selcuk; KARAKOYUNLU, Deniz; ROHATGI, Pankaj; SUNAR, Berk. *Trojan detection using IC fingerprinting.* Proceedings - IEEE Symposium on Security and Privacy, p. 296–310, 2007.

ALIYU, A.; BELLO, A.; MOHAMMED, J.; ALHASSAN, I. H. Hardware Trojan Model For Attack And Detection Techniques. In: *International Journal of Scientific & Technology Research,* 2014.

ANDERSON, M. S.; NORTH, C. J. G.; YIU, K. K. *Towards Countering the Rise of the Silicon Trojan.* Command, Control, Communications and Intelligence Divison. Australian government, 2008.

BAUMGARTEN, Alex; STEFFEN, Michael; CLAUSMAN, Matthew; ZAMBRENO, Joseph. A case study in hardware Trojan design and implementation. In: *International Journal of Information Security,* 10(1):1–14, 2011.

BEAUMONT, Mark; HOPKINS, Bradley; NEWBY, Tristan. *Hardware Trojans - Prevention, Detection, Countermeasures (A Literature Review).* Command, Control, Communications and Intelligence Division. Australian government, 2011.

BECKER, Georg T.; REGAZZONI, F.; PAAR, C.; BURLESON, Wayne P. *Stealthy dopant-level hardware Trojans:* Cryptographic hardware and embedded systems, CHES 2013, p. 197–214, 2013.

BHUNIA, S.; HSIAO, Michael S.; BANGA, M.; NARASIMHAN, S. Hardware trojan attacks: threat analysis and countermeasures. In: *Proceedings of the IEEE,* v.102, p. 197–214, 2014.

BRASIL. *Política Nacional de Inteligência (PNI)*. Decreto n° 8.793/2016, Brasília-DF, 2016.

CARUZZO, A.; ZAWADZKI, M.; BELDERRAIN, M. *Proteção de Infraestruturas Críticas: desafios da previsão meteorológica como ferramenta de apoio aos Serviços de Inteligência. Revista* Brasileira de Inteligência, Brasília, ABIN, v.9, 2015.

CERT.BR. *Cartilha de Segurança para Internet:* Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. Disponível em: <cartilha.cert.br>. Acesso em: 01 out. 2017.

CHAKRABORTY, R. S.; SASHA, I.; PALCHAUDHURI, A.; NAIK, G. K.: *Hardware trojan insertion by direct modification of FPGA configuration bitstream*. IEEE Design and Test, 30(2), 2013.

CHAKRABORTY, R. S.; NARASIMHAN, S.; BHUNIA, S. *Hardware trojan: Threats and emerging solutions*. IEEE, 2009.

CLARKE, Richard A.; KNAKE, Robert K. *Guerra Cibernética:* A Próxima Ameaça à Segurança e o que Fazer a Respeito. São Paulo: Brasport, 2015.

FLOYD, Thomas L. *Digital Fundamentals*. 11 ed. England: Pearson, 2014.

GOERTZEL, K. M.: Integrated circuit security threats and hardware assurance countermeasures. In: *The Journal of Defense Software Engineering,* p. 33–38, 2013.

IQBAL, Asif: *Understanding Integrated Circuit Security Threats*. Disponível em: <sdm.mit.edu/news/news_articles/webinar_021014/iqbal_021014.pdf>. Acesso em:09 set. 2017.

KARRI, Ramesh; RAJENDRAN, Jeyavijayan; ROSENFELD, Kurt. *Trustworthy hardware: Identifying and Classifying hardware Trojans*. IEEE Computer Society, p. 39–46, 2010.

KING, S. T.; TUCEK, J.; COZZIE, A.; GRIER, C.; JIANG, W.; ZHOU, Y. Designing and implementing malicious hardware. In: *Proceedings of the 1st Usenix workshop on large-scale exploits and emergent threats,* 2008.

KRIEG, Christian; DABROWSKI, Adrian; HOBEL, Heidelinde; KROMBHOLZ, Katharina; WEIPPL, Edgar. *Hardware Malware*. Synthesis Lectures on Information Security, Privacy, and Trust. Williston, USA: Morgan & Claypool Publishers, 2013.

LI, He; LIU, Qiang; ZHANG, Jiliang. *A survey of hardware trojan threat and defense*. Integration, the VLSI journal, 2016.

MCCORMACK, Richard. *$600 Million Over 10 Years For IBM's 'Trusted Foundry' Chip Industry's Shift Overseas Elicits National Security Agency, Defense Department Response.* Manufacturing & Technology News, v. 11, n. 3 (Feb. 3, 2004). Disponível em: <www.manufacturingnews.com/news/04/0203/art1.html>. Acesso em: 16/10/2018.

MOEIN, Samer; GULLIVER, Thomas A.; GEBALI, Fayez; ALKANDARI, Abdulrahman. *A New Characterization of Hardware Trojans.* IEEE Access, 4:2721–2731, 2016.

PIKMA, T.: *Stealthy dopant-level hardware trojans.* In: Research Seminar in Cryptography, 2013.

QAMARINA, Nur; NOOR, Mohd; NUR, Nilam; SJARIF, Amir; HUDA, Nurul; MOHD, Firdaus; DAUD, Salwani M. Hardware Trojan Identification Using Machine Learning-based Classification. *Journal of Telecommunication, Electronic and Computer Engineering Result.* 9(3):23–27, 2017.

RAJENDRAN, J.; GAVAS, E.; JIMENEZ, J.; PADMAN, V.; KARRI, R. Towards a comprehensive and systematic classification of hardware trojans. In: *Proceedings of 2010 IEEE International Symposium,* p. 1871–1874. New York, USA, 2010.

RAWNSLEY, Adam. *Can DARPA Fix the Cybersecurity Problem From Hell?*. Disponível em: <www.wired.com/2011/08/problem-from-hell/>, 2011. Acesso em: 2017-11-22.

SANCHEZ, Julio: *Metodología para la Investigación en Marketing y Dirección de Empresas.* Ed. Pirámide: Madrid, 1999.

SHIYANOVSKII, Y; WOLFF, F; PAPACHRISTOU, C; WEYER, D; CLAY, W. *Exploiting Semiconductor Properties for Hardware Trojans.* ACM CoRR, p. 6, 2009.

SUBRAMANI, Kiruba S.; ANTONOPOULOS, Angelos; ABOTABL, Ahmed A.; NOSRATINIA, Aria; MAKRIS, Yiorgos. INFECT: INconspicuous FEC-based Trojan: A hardware attack on an 802.11a/g wireless network. In: Proceedings of the 2017 *IEEE International Symposium on Hardware Oriented Security and Trust,* HOST 2017, p. 90–94, 2017.

SWIERCZYNSKI, Pawel; FYRBIAK, Marc; KOPPE, Philipp; PAAR, Christof. FPGA Trojans Through Detecting and Weakening of Cryptographic Primitives. In: *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems,* 2015.

TEHRANIPOOR, Mohammad; KOUSHANFAR, Farinaz. A survey of hardware trojan taxonomy and detection. In: *IEEE Design and Test of Computers,* 27(1):10–25, 2010.

USA: *Discussion draft of the preliminary cybersecurity framework [report],* 2013.

VILLASENOR, J. *Compromised by design:* Securing the defense electronics supply chain. USA: Brookings Institute, 2013.

VILLASENOR, J: *Ensuring Hardware Cybersecurity.* Electrical Engineering, 2011.

VILLASENOR, J: *The hacker in your hardware.* Scientific American, 303(2):82–87, 2010.

WANG, Xiaoxiao; TEHRANIPOOR, Mohammad; PLUSQUELLIC, Jim. Detecting malicious inclusions in secure hardware: Challenges and solutions. In: *2008 IEEE International Workshop on Hardware-Oriented Security and Trust,* HOST, 1(July):15–19, 2008.

XIAO, K; FORTE, D.; JIN, Y.; KARRI, R.; BHUNIA, S.; TEHRANIPOOR, M. Hardware Trojans: lessons learned after one decade of research. In: *ACM Transactions on Design Automation of Electronic Systems,* 22(1):1–23, 2016.

YOSHIKAWA, M.; TAKEUCHIR, D.; KUMAKI, T. Reset Signal Aware Hardware Trojan Trigger. In: *ICAET,* 2014 (pp. 528–531).

INTELIGÊNCIA ECONÔMICA DE ESTADO: NECESSIDADE ESTRATÉGICA PARA O BRASIL

Delanne Novaes de Souza *

Resumo

O Brasil tem acumulado fracassos decorrentes não apenas de suas intrínsecas fraquezas produtivas como de sua incapacidade de definir seu papel no mundo, particularmente devido à inexistência de grande estratégia nacional no País, em especial de estratégia econômica capaz de promover, de modo integrado e competitivo, suas potencialidades nas relações internacionais. Com vistas a sanar esta grave falta de rumo econômico, o País deve criar e desenvolver mecanismo de modo a orientar e construir consensos para aperfeiçoar sua inserção econômica internacional. Inteligência Econômica de Estado (IEE) e Sistema de Inteligência Econômica (SIE) coordenado, dinâmico, adaptável e transparente, que se aproveite das experiências minimamente consolidadas dos atores econômicos já integrantes do Sistema Brasileiro de Inteligência (Sisbin) e que integre outros órgãos fundamentais às políticas públicas econômicas do País, como o Instituto de Pesquisa Econômica Aplicada (Ipea), do Ministério do Planejamento, Desenvolvimento e Gestão (MPOG), aliados ao fortalecimento da IEE no âmbito da Agência Brasileira de Inteligência (Abin), órgão central do Sisbin, podem ser importantes elementos deste mecanismo.

Palavras-chaves: inteligência econômica; sistema de inteligência econômica; desenvolvimento econômico; estratégia nacional.

NATIONAL ECONOMIC INTELLIGENCE: STRATEGIC NEED FOR BRAZIL

Abstract

Brazil has accumulated setbacks not only from its intrinsic productive weaknesses, but also from its incapacity to define its role in the world, particularly due to the inexistence of a national grand strategy in the country, especially an economic strategy capable of promoting, in an integrated and competitive way, its potentialities in the international relations. In order to cope with this serious lack of economic direction, the country should create and develop a mechanism to guide and build consensus to improve its international economic integration. A National Economic Intelligence (IEE) and a coordinated, dynamic, adaptable and transparent National Economic Intelligence System (SIE), which takes advantage of minimally consolidated experiences of economic actors already members of the Brazilian Intelligence System (Sisbin) and that integrates other key agencies to economic policies of the country, such as the Institute for Applied Economic Research (IPEA) of the Ministry of Planning, Development and Management (MPOG), together with the strengthening of the IEE area under the Brazilian Intelligence Agency (Abin), the central organ of the Sisbin, may be important components of this mechanism.

Keywords: *economic intelligence; economic intelligence system; economic development; national strategy.*

---

* Mestre em Estudos Estratégicos (*National Defense University,* Estados Unidos), mestre em Relações Internacionais (Universidade Federal Fluminense) e bacharel em Economia (Universidade Federal do Rio de Janeiro).

Artigo recebido em Julho/2018
Aprovado em Setembro/2018

Introdução

Entre os objetivos estratégicos do Brasil, o desenvolvimento nacional ocupa posição ímpar, como preconiza o Art. 3º da Constituição Federal de 1988 (BRASIL, 2000). Trata-se de necessidade de Estado que, aliada à solução pacífica de conflitos na geopolítica mundial, configura objetivo imperioso ao Brasil. Infelizmente, porém, o país, em especial em alguns setores estratégicos, isto é, aqueles fundamentais ao seu desenvolvimento e garantes de sua soberania, encontra-se sem rumos plenamente definidos, circunstância grave que decorre da ausência de projeto de futuro coordenado, capaz de impulsionar seu potencial de forma orientada e dinâmica.

Como apontam Kalout e Degaut no Relatório de Conjuntura da Secretaria de Assuntos Estratégicos da Presidência da República (2017, p. 12), o Brasil tem avançado agenda pontual, sujeita a conjunturas, sem definir objetivos de longo prazo de modo integrado. Em que pese objetivos de longo prazo avançados por meio de planos estratégicos setoriais, entre outros, o energético, e de empresas específicas, como os da Petrobras e da Eletrobras, não há clareza sobre o modo como se articulam no contexto de objetivos nacionais econômicos de longo prazo.

Em sentido econômico, o País acumula série de insucessos internacionais, não obstante os ganhos em temas agropecuários em painéis da Organização Mundial de Comércio (OMC), entre os quais aqueles no âmbito das seguintes esferas: Rodada Doha, da OMC; relação bilateral com parceiros potenciais, prejudicada pelo Mercosul, o que ensejou apenas três acordos de livre comércio (Israel, Palestina e Egito) e dois acordos preferenciais (Índia e União Aduaneira da África Austral); tratados sobre investimentos estrangeiros, tendo sido superado por vários países emergentes, como Chile, Argentina, Peru, África do Sul, México e Colômbia; BRICS (Brasil, Rússia, Índia, China e África do Sul), caracterizado, salvo a experiência incipiente do Banco de Investimentos, por competição e desinteresse, como evidencia o baixo montante de investimentos externos diretos no Brasil dos demais países-membros; destaque da China como parceiro comercial (um quarto do *superávit* comercial brasileiro), com pauta de exportações menos diversa e concentrada em *commodities,* situação distinta do comércio com os Estados Unidos da América (EUA), antes dessa primazia da China o maior parceiro comercial do Brasil, e órgão de apelação do Sistema de Solução de Controvérsias da OMC (SSC)[1], com perda de vagas.

Sublinha-se que entre as dez maiores economias do mundo em 2016, Brasil, Índia, Rússia e Indonésia, não estão entre as dez maiores exportadoras de mercadorias. Além de ser exceção no *ranking* de maiores exportadores entre as maiores economias do mundo, entre todos os membros da OMC, de 2014 a 2016, o Brasil é o país que detinha a menor participação do comércio

1 Ver também BENJAMIM, Daniela Arruda (2013) O Sistema de Solução de Controvérsias da OMC. Brasília: Fundação Alexandre de Gusmão, 1995.

internacional no PIB – 12,1% [2], o que sinaliza baixa alavancagem das exportações e do comércio exterior como um todo como fator de crescimento e desenvolvimento nacional, ainda que, em 2016, de acordo com os dados mais recentes do *World Trade Statistical Review* (2017), tenha sido o terceiro maior exportador de produtos agrícolas e de alimentos do mundo, atrás apenas de União Europeia (UE) e dos EUA, representando, respectivamente, 4,9% e 5% das exportações mundiais[3].

Tabela 1 – As dez maiores economias do mundo, segundo o Produto Interno Bruto (PIB) com base na paridade do poder de compra da moeda, com destaque (em negrito) para as que também não são as maiores exportadoras do mundo)

POSIÇÃO	PAÍS
1	China
2	EUA
3	**Índia**
4	Japão
5	Alemanha
6	**Rússia**
7	**Brasil**
8	**Indonésia**
9	Reino Unido
10	França

Fonte: Banco Mundial

2 A União Europeia (UE), formada por 28 países – nos períodos em foco, não havia ocorrido o chamado Brexit –, foi considerada como bloco. Detém 16,8% de participação do comércio exterior em sua economia. Ressalta-se que os dados mais atuais referentes a alguns países compreendem o período 2013-2015. São eles, em ordem decrescente de participação: Congo, Omã, Guiana, Trinidad e Tobago, Djibouti, Zimbábue, Gabão, Gâmbia, República Democrática do Congo, Laos, Chade, Venezuela, Camarões, Iêmen, Myanmar e República Centro-Africana. Ademais, os dados afetos a dois países – Serra Leoa e Guiné – são do período 2012-2014. Não há dados disponíveis sobre a participação do comércio internacional no PIB na base da OMC de dois países-membros: Cuba e Liechtenstein.

3 Ver também MOREIRA e ARAÚJO JR. ,2011.

Tabela 2 – As dez maiores economias exportadoras do mundo (*merchandise trade*)

POSIÇÃO	PAÍS	VALOR (US$ BI)	PARTICIPAÇÃO (%)
1	China	2098	13,2
2	EUA	1455	9,1
3	Alemanha	1340	8,4
4	Japão	645	4
5	Países Baixos	570	3,6
6	Hong Kong	517	3,2
7	França	501	3,1
8	República da Coreia	495	3,1
9	Itália	462	2,9
10	Reino Unido	409	2,6

Fonte: Dados obtidos do *World Trade Statistical Review* 2017, da OMC

Acrescente-se que de 2004 a 2014 o crescimento das exportações para dezoito países africanos onde se abriram embaixadas nos últimos anos configura acréscimo de apenas 0,38% na pauta de exportação do Brasil e o fato de que apenas 9% do total da pauta de exportações e 6% do total de importações do Brasil se concentrarem no Mercosul. Comparativamente, as exportações da Aliança do Pacífico representaram 47% do total registrado na América Latina (KALOUT; DEGAUT, 2017, p. 20-4). Destaca-se que o Brasil ocupa a 45ª posição no *ranking* de 139 países e governos mais preparados para enfrentar riscos globais, entre outros, como crise financeira, conforme pesquisa do Fórum Econômico Mundial (WEF, da sigla em inglês) (ANGELIS, 2013, p. 319).

Tais insucessos não decorrem apenas das dificuldades inerentes às relações econômicas internacionais, mas também de ser o País incapaz de definir seu lugar no mundo além da meta clara de ganho de mercados do setor agropecuário, e de suas intrínsecas fraquezas produtivas[4] . De modo a tentar sanar esta ausência de rumo econômico, é imprescindível que o País crie e desenvolva mecanismo capaz de

4 Ver também Waltz, sobre forças produtivas intrínsecas de um país como propulsor de seu próprio desenvolvimento, em que este chamou teorias reducionistas das relações internacionais (teorias marxistas internacionais, como a teoria de Lênin sobre o imperialismo como fase ulterior do capitalismo, entre outras) (WALTZ,1979. p. 19-38).

orientar com solidez e consenso sua inserção econômica internacional. Um Sistema de Inteligência Econômica (SIE) coordenado, dinâmico e transparente pode ser importante elemento deste mecanismo. (ZELIKOW, 1997).

No Brasil, há iniciativas importantes, como aquelas no âmbito da Diplomacia Comercial do Ministério das Relações Exteriores (MRE) e Ministério da Indústria, Comércio Exterior e Serviços (MDIC), por meio da Agência de Promoção de Exportações do Brasil (Apex-Brasil), em especial, entre os sete programas desta, por intermédio de Inteligência de Mercado e Estratégia de Negócios; o Instituto de Pesquisa Econômica Aplicada, do Ministério do Planejamento, Desenvolvimento e Gestão (Ipea/MPOG), com o seu estudo *Brasil 2035: cenários para o desenvolvimento;* e o Ministério da Agricultura, Pecuária e Abastecimento (MAPA), com suas *Projeções do Agronegócio.*

Além de tais iniciativas, há aquelas setoriais privadas, como as das federações de indústrias nos estados; Confederação Nacional da Agricultura (CNA), e a Confederação Nacional da Indústria (CNI). Não há no país, todavia, estrutura integrada de Inteligência Econômica de Estado (IEE), isto é, Inteligência de Estado para apoiar o desenvolvimento econômico nacional.

Países que têm se destacado na geoeconomia[5] (ARENAS, 2014, p. 10) mundial, como Alemanha, China, Coreia do Sul, EUA, França, Japão, Reino Unido (RU), Rússia e Suécia se pautam na IEE como vetor fundamental de desenvolvimento econômico, conforme a Espanha percebeu ao pensar e tentar conceber seu SIE.

Contrariamente, porém, a qualquer exercício de sobreposição de ideias e sistemas estrangeiros no Brasil, a experiência de tais países apenas serve como fonte de inspiração relevante da Inteligência aplicada à economia. Há que se considerar, por conseguinte, que a criação e o desenvolvimento da IEE no Brasil devem se fundamentar na cultura e em necessidades específicas nacionais, bem como respeitar, por questões de economicidade e bom senso, ainda mais em período de crise econômica, social e política, estruturas já formadas que podem bem servir como guia para a consecução deste propósito.

Este artigo visa apontar a importância da IEE para o desenvolvimento econômico nacional e propor ideias preliminares sobre a criação de um SIE no País e seus integrantes, aproveitando-se de estrutura já minimamente consolidada do Sistema Brasileiro de Inteligência (Sisbin). Para isso, está dividido da seguinte forma: na primeira parte, trata-se de definir o que se entende por IEE neste trabalho; em seguida, alude-se à IEE de alguns países, em particular a de alguns daqueles acima citados; na terceira parte, abordam-se problemas associados à IEE, em especial os afetos à priorização – ineficiente e corrompida – pelo Estado, de determinados setores da iniciativa privada, e meios de contorná-los; propõe-se a criação de um SIE, e aponta-se conjunto focal de subáreas econômicas a serem acompanhadas pela Inteligência. Na última parte, tecem-se considerações finais.

5 Ver também conceito avançado por Edward Luttwak e Pascal Lorot.

Afinal, que é IEE?

A literatura internacional sobre inteligência econômica, como ferramenta de Inteligência de Estado no âmbito do campo econômico, não obstante seja escassa[6], é repetitiva e, na maioria das vezes, estritamente programática, caso, por exemplo, dos estudos espanhóis acerca do tema (ESPANHA, 2016). E, apesar de casos de atuação da IEE, pouco se sabe quanto ao emprego efetivo de Serviços de Inteligência para fins econômicos. No Brasil, a literatura sobre o assunto é rara, como sublinhou Ribeiro (2016, p. 10).

A Inteligência, como ferramenta de auxílio à tomada de decisões econômicas, em geral, é tratada de modo amplo, em que o conceito se confunde ora com Inteligência Competitiva (CI, da sigla em inglês), ora com *Business Intelligence* (BI), os quais se relacionam à gestão do conhecimento para a ação estratégica no âmbito empresarial privado[7]. Ou, como evidencia produção em academias militares (Academia Militar da Romênia, país onde cada vez mais se produz sobre a temática), vincula-se à gestão de recursos em contexto militar, seja em tempos de paz ou de guerra.

Ribeiro (2016, p. 32-44), em seu esforço de delimitar o conceito no aspecto estatal e sugerir uma "rede inicial de atores" de IEE no Brasil, talvez no único trabalho no País que trata do tema de modo específico, expõe levantamento bibliográfico em que revela a diversidade do emprego conceitual da inteligência econômica e como esta se confunde com métodos de gestão empresarial. A autora aponta que em pesquisa realizada em junho de 2016, na Biblioteca Digital de Teses e Dissertações, que reúne teses e dissertações defendidas no Brasil e por brasileiros no exterior, por meio do assunto "Inteligência Econômica", não se recuperou nenhum resultado. Nem no Google Acadêmico se encontrou qualquer tese ou dissertação em busca realizada no mesmo período. Em sua pesquisa para defesa de dissertação, apenas 37,5% dos documentos que a economista analisou entendiam inteligência econômica como atividade de Inteligência de Estado com vistas ao desenvolvimento econômico (RIBEIRO, 2016, p. 34-5).

IEE, distintamente de tais ferramentas de auxílio à tomada de decisões estratégicas no setor privado, é Inteligência de Estado para fins de desenvolvimento econômico, o que se coaduna com um conjunto de ações coordenadas de busca, tratamento, difusão e proteção das informações úteis aos diferentes atores econômicos (MARTRE, 1994, p. 3). Em âmbito estatal, favorece a competitividade de uma nação frente às demais. Em todos os países em que há SIE

6 Potter (1998, p. 29) aponta que na literatura ostensiva sobre o assunto, há muito menos informações sobre análise comparativa entre SIEs que sistemas de Inteligência de modo geral.

7 De acordo com o Financial Times, BI é método de inteligência usado por empresas em que se tratam dados brutos (quantitativos) a fim de se ter melhor compreensão de suas atividades internas. Geralmente requer uso de técnicas específicas, por meio de *hardware e software*, como *Big Data, OLAP (online analytical processing), data mining e DSS (decision support systems)*. Objetiva detectar padrões de comportamento de modo a antecipar comportamentos futuros. Por sua vez, CI analisa dados externos às atividades da empresa, tendo foco qualitativo, de modo a obter vantagem estratégica em determinado nicho concorrencial. Já a Inteligência Financeira, está relacionada à prevenção e combate a práticas ilegais – lavagem de dinheiro e financiamento do terrorismo – no sistema financeiro nacional e internacional. Tais tipos de Inteligência, portanto, não devem ser confundidas com IEE.

de razoável capacidade de atuação, traço comum é a sinergia entre o Estado e empresas privadas de setores estratégicos[8], selecionados segundo os interesses de desenvolvimento e cultura de cada país. Observa-se que a definição de Martre deve ser relacionada à especificidade de cada país quanto aos setores econômicos e empresas a serem contemplados.

Frisa-se que embora se costume, particularmente quanto à atuação dos EUA em IEE, realçar o papel desta no que concerne à obtenção de dado negado, quase 90% do estoque de dados econômicos se concentram em bancos de dados, imprensa, publicações especializadas, seminários e Internet, isto é, fontes abertas. Os 10% restantes são geralmente obtidos por meio de fontes "fechadas", que podem demandar práticas desonestas *(grey information)* ou ilegais *(black information)* (IVAN, 2013, p. 187-8).

Entre as várias linhas de ação em que o Estado pode atuar como produtor de IEE estão as seguintes: formação de opinião e consciência do papel da informação no processo econômico; assistência durante a criação de capacidades específicas, educação e treinamento de especialistas; desenvolvimento de plataformas de cooperação nos vários setores econômicos; criação de parceria estratégica no gerenciamento da informação e conhecimento, e consultoria (IVAN, 2013, p. 191-2).

Ressalta-se que neste trabalho a IEE se alinha a referenciais *estratégicos* de Inteligência no Brasil: a Lei nº 9.883, de 7 de dezembro de 1999, que instituiu o Sisbin; o Decreto nº 8.793, de 29 de junho de 2016, que fixou a Política Nacional de Inteligência (PNI); a Estratégia Nacional de Inteligência (ENINT), e os fundamentos doutrinários da Doutrina Nacional da Atividade de Inteligência, com a especificidade de estar voltada para assessorar decisores nacionais quanto ao desenvolvimento econômico. No âmbito da PNI, Inteligência é

> [...] atividade que objetiva produzir e difundir conhecimentos às autoridades competentes, relativos a fatos e situações que ocorram dentro e fora do território nacional, de imediata ou potencial influência sobre o processo decisório, a ação governamental e a salvaguarda da sociedade e do Estado.

IEE é, portanto, tal atividade dirigida especificamente ao processo decisório nacional econômico.

Além de objetivar garantir a segurança nacional quanto aos aspectos econômicos, a IEE hoje está em patamar mais básico quanto a seu foco de atuação, como preconiza o *Intelligence Services Act* do RU, de 1994, ao incluir no rol de atribuições dos Serviços de Inteligência a promoção do bem-estar econômico do Reino Unido (PORTEOUS, 1998, p. 81-83). Percebe-se, pois, que bem-estar econômico seja menos restrito que segurança econômica associada à segurança nacional. No que diz respeito à relação entre estas se realça que no advento de a economia nacional

8 Na literatura especializada, referem-se a alguns destes setores, aqueles intensivos em tecnologia e capital, entre eles o de microeletrônica, telecomunicações, computadores, biotecnologia, aeroespacial, nuclear, químico e farmacêutico, como os detentores de *enabling technologies*, haja vista tornarem o país mais competitivo no mundo (POTTER, 1998).

inviabilizar a prosperidade da população e as instituições que garantem harmonização de interesses sociais (defesa, saúde, educação, pensões, etc.), o Estado perde sua razão de existir, tornando-se um "estado falido", o nível máximo de insegurança para o Estado, segundo *matriz de segurança* do *Watson Institute for International Studies* (IVAN, 2013, p. 194).

Ou, conforme a tipologia de Martre (1994, p. 84), a inteligência econômica pode ser primária e secundária (*green e yellow zones,* a depender da obtenção mais ou menos pública do dado), por meio da coleta de dados de fontes abertas como centros estatísticos, sistemas *on line, think tanks,* universidades, bibliotecas, associações de comércio, imprensa e publicações especializadas; tática *(red zone)*, isto é, quando obtém dados e informações mais privilegiados e sensíveis, por intermédio de contatos pessoais, simpósios fechados, dados mais protegidos de empresas, e clandestina *(black zone)*, quando coleta informação classificada.

Não se pode desprezar que ameaças a empresas de setores estratégicos, cuja seleção se deve vincular a uma grande estratégia nacional ou a uma estratégia nacional econômica subordinada àquela, públicas ou privadas, podem configurar ameaça ao interesse nacional, devendo, se assim o for, ser objeto de tratamento pelo Estado.

Vulnerabilidades e ameaças que tenham impactos macroeconômicos, como, por exemplo, nas políticas monetária e fiscal, e práticas abusivas de comércio internacional também devem ser foco de consideração pelo Estado. Este deve, portanto, atuar, ademais das áreas que impactem a macroeconomia do País, também nos aspectos microeconômicos que possam afetar a competitividade de empresas estratégicas, como corrupção de empresas estrangeiras competidoras, e na construção e fortalecimento de regimes internacionais[9], como os relacionados ao mercado financeiro internacional; investimentos externos diretos; comércio internacional; propriedade intelectual; indicadores financeiros e *ratings*; bem como em campanhas internacionais de desestabilização, as quais podem prejudicar diversas políticas públicas (REVEL, 2010; PORTEOUS, 1998, p. 11, 104-108).

Fator importante no que diz respeito à IEE é o fato de o Estado, em que pese ampla gama de empresas privadas que atuam em Inteligência no campo econômico, ser dotado de capacidade única de coleta. Serviços de Inteligência são particularmente úteis ao assessorar a tomada de decisões no Estado por meio de análise sobre questões econômicas não disponíveis em fontes abertas, como na detecção de tentativas de influência estrangeira nos interesses econômicos internacionais do país.

O Escritório de Avaliações Nacionais (ONA, da sigla em inglês), coordenador da comunidade de Inteligência da Austrália, defendeu sua atuação em IEE com base no objeto de acompanhamento: compreensão de capacidades e intenções que competidores e adversários do país

9 Assim, todo o marco regulatório vinculado à proteção do meio ambiente, emissões de carbono, riscos nucleares, garantias mínimas aos trabalhadores, trabalho infantil, preservação de estoques de peixes, segurança alimentar torna-se objeto de acompanhamento da IE (IVAN, 2013, p. p. 192).

buscam esconder. Além disso, os Serviços podem desenvolver atividades de modo a influenciar eventos, comportamento e formulação de política econômica de países estrangeiros, inclusive por meio de campanhas de desinformação, influência encoberta em decisões econômicas, e, talvez o aspecto mais polêmico, obter e difundir inteligência comercial e tecnológica para atores comerciais (PORTEOUS, 1998, p. 88, 107).

Outros campos passíveis de acompanhamento pela IEE são as negociações comerciais e aqueles associados à segurança cooperativa que podem impactar economicamente o país, como migrações, crime internacional, doenças, direitos humanos, e crises humanitárias (POTTER, 1998, p. 4).

A IEE e os SIES no mundo

A demanda de Inteligência para a tomada de decisões pelo Estado está intimamente ligada ao modelo de sociedade, estilo de vida, ética, aspectos jurídicos, tradições, identidade cultural e nível de desenvolvimento de cada país. Como dito, portanto, a criação e o desenvolvimento da IEE no Brasil devem se fundamentar na cultura e necessidades específicas nacionais.

Como evidência desta especificidade, história, geografia, língua e cultura geral predispõem os canadenses a serem aparentemente mais coletivos que os americanos, mas não os faz unificados na gestação de um propósito nacional, como ocorre na Alemanha e Japão. O Canadá não tem cultura de compartilhamento de informação. Ademais, a história política do Canadá é marcada por períodos de centralização e descentralização, efeito da resistência provinciana a tentativas de se racionalizar suposto sistema de inteligência econômica. Também no país inexiste cultura de inteligência econômica no setor privado, por dificuldade de compartilhar informações e sensibilizar funcionários quanto ao modo de coleta de informação por agentes externos às empresas, bem como falta de consciência destas da importância do assunto (IVAN, 2013, p. 184; POTTER, 1998, p. 22).

A cultura impacta não só tecnicamente na criação e desenvolvimento de IEE, como em aspectos morais relativos ao tema. Quanto maior o sentimento de propósito nacional, maior a possibilidade de os atores econômicos do país "aceitarem" os dilemas morais que podem advir da inteligência econômica. O senso de competitividade como objetivo nacional, assim, será prevalecente quanto aos meios de obtenção e produção de Inteligência. De modo similar, países mais propensos à intervenção do Estado na economia tenderão a ter menos resistência quanto ao emprego da IEE em assuntos comerciais, como ocorre no caso de assistência estatal aos chamados "campeões nacionais" (POTTER, 1998, p. 67; PORTEOUS, 1998, p. 100).

Este traço cultural também está presente na chamada *"co-opetition"*, inserida no contexto da geoeconomia. Como Potter (1998, p. 4) defende, japoneses, alemães e franceses veem poucas inconsistências ou dilemas morais ao coletar e reunir inteligência econômica um do outro, aberta ou clandestinamente, enquanto mantêm consenso político em matérias como arranjos de segurança comum, e liberalização do comércio

internacional e investimentos.

Em alguns países, com maior senso estatal e coletivista, o SIE caracteriza-se pela atuação do Estado na proteção e criação de indústrias nacionais ("campeões nacionais"). Participam diretamente como ator no mercado, bem como provêm o setor privado, por meio de canais regulares e formais, de serviços e informação. Em outros países, há grande complementariedade entre os setores público e privado, sem que haja qualquer ator que exerça liderança efetiva na provisão de inteligência econômica. Ademais, quanto mais aberta a economia de um país, mais se tende à provisão de informações abertas, caso dos países da Organização Econômica para Cooperação e Desenvolvimento (OECD), nos quais, em razão disso, há pletora de fornecedores de inteligência econômica privada (POTTER, 1998, p. 56-7).

Outros dois aspectos importantes são o senso de competitividade nos países e a predisposição dos Estados em se engajar em inteligência. Assim, a competitividade entre as firmas japonesas é característica no mercado doméstico, enquanto tendem a cooperar na economia internacional. Já o Canadá e os EUA são relutantes; o RU, bem menos, enquanto a prática é considerada normal no Japão, Alemanha e França (POTTER, 1998, p. 66).

Segundo Martre (1994, p. 13), SIEs são modelos, pois satisfazem a três condições: a prática de inteligência econômica é permanente, contínua quanto ao emprego de técnicas, e perene no uso de estratégias. SIEs são geralmente compostos de instituições de Estado, das quais os Serviços de Inteligência são um dos componentes, que coletam, analisam, e difundem conhecimento de modo a proteger e promover a segurança econômica nacional (POTTER, 1998, p. 1), e diversos outros entes privados, a depender do país.

Um SIE é visto como conjunto de práticas e estratégias de interpretação da informação útil, desenvolvida e compartilhada no seio de uma nação entre seus diferentes níveis de organização: Estado, organizações governamentais, autoridades locais, empresas, sistema educacional, associações profissionais, sindicatos, entre outros. Deve ter três finalidades: a) desenvolver capacidades de interpretação e compreensão do meio pelos diferentes agentes econômicos; b) produzir conhecimentos compartilhados e ajustar ações coletivas adaptadas aos desafios da organização; e c) executar estratégias de influência, para promover modelo de desenvolvimento socioeconômico nacional nos mercados externos, de modo a valorizar o poder de negociação do Estado no seio das relações internacionais (CLERC, 1999).

A rede social de IEE soma-se às contribuições de uma série de atores (universidades, centros de inovação, fundações, associações) sobre a qual um observador está atento para sinalizar pontos fortes que podem agregar valor à dinâmica de desenvolvimento de uma rede nacional (GÓMEZ; RAMÍREZ, 2008).

Além dos pioneiros Alemanha, Japão e Suécia, outros países se destacam no que tange à IEE, como China, França, EUA e RU, sempre pautados por sua cultura, necessidades específicas e estratégia de

inserção internacional. Alguns deles, como a Espanha, que não conta com SIE plenamente estabelecido, os EUA, o RU, o Canadá e a Rússia, contam com atuação do Serviço de Inteligência – o Centro Nacional de Inteligência (CNI); a Agência Central de Inteligência (CIA); o Serviço Secreto de Inteligência (SIS, ou MI6, das siglas em inglês), por meio da *Section VII;* o Serviço Canadense de Inteligência de Segurança (CSIS, da sigla em inglês) e o Centro de Segurança das Telecomunicações (CSE, da sigla em inglês), e o Serviço de Inteligência Externa russo (SVR, da sigla transliterada do russo), por sua Diretoria de Inteligência Econômica.

O Japão foi o primeiro país a usar a IEE de modo a estimular o desenvolvimento econômico, com o fim de preservar sua independência econômica frente a potências ocidentais. A IEE japonesa caracteriza-se pelo papel garantidor do Estado na gestão estratégica do conhecimento, por meio do Ministério do Comércio Internacional e Indústria (MITI, da sigla em inglês), que oferece aos setores econômicos estratégicos do país estudos especializados do Instituto de Proteção Industrial (IIP, da sigla em inglês) e auxílio ao corpo diplomático, por meio do Centro de Informação e Investigação.

Caracteriza-se por profundo sentimento coletivo patriótico, visão de longo prazo associada à análise prospectiva, inserção comercial específica por país, política de comunicação seletiva da informação, aliada à prática de desinformação. O Japão dispõe de forte capacidade em análise de IEE de fontes abertas. Adota a chamada *"glocalization"*, isto é, proteção do mercado doméstico e, também, expansão do comércio exterior, já mencionada (ARENAS, 2014). Como se trata de IEE caracterizada por compartilhamento de informações, as empresas japonesas são relutantes em obter inteligência econômica aberta de consultorias, sejam elas nacionais ou estrangeiras.

Outros importantes atores são o Escritório de Pesquisa da Informação, do Gabinete do Primeiro Ministro (CIRA) ou Escritório de Inteligência, encarregado de enviar relatórios semanais de todo o mundo para tal gabinete; a Organização de Fomento ao Comércio Exterior do Japão (JETRO), e grandes corporações japonesas que operam no exterior. Há também entendimento tácito entre os conglomerados japoneses *(keiretsu)* de modo a evitar que se destruam domesticamente, mas sim a pensar em competição econômica no longo prazo, o que potencializa a solidariedade entre eles em relação aos negócios internacionais. O SIE japonês evidencia forte consenso e cooperação entre os principais atores econômicos quanto às iniciativas, abertas ou encobertas, necessárias ao fortalecimento da economia (POTTER, 1998, p. 57-8).

Em 1991, a pedido da CIA, graduandos americanos produziram relatório intitulado *Japan 2000*, no qual argumentaram que o "milagre japonês" decorreu de estratégia eficiente em obter informação econômica. Em poucos anos, segundo o documento, o Japão tornou-se uma das maiores potências econômicas do mundo, apesar de sua infraestrutura ter sido destruída na Segunda Guerra Mundial.

Diferentemente dos SIEs americano e canadense, o sistema de IEE da Alemanha

é similar ao japonês. Caracteriza-se por centralização do fluxo de informações provenientes de órgãos estatais; uso sistemático de redes de emigrantes e descendentes alemães no exterior; 6.000 câmaras de comércio; sindicatos; províncias; informação de empresas privadas, como bancos, companhias comerciais e de seguro, grandes grupos industriais, sociedades de transporte; e sentimento coletivo de patriotismo econômico. Como atores centrais há rede de decisores nos níveis federal e outros níveis de governo, e rede industrial. Como no caso japonês, o SIE alemão está baseado em meta estratégica nacional reconhecida pelos principais entes econômicos. Um fator histórico importante é a atuação do setor privado junto ao governo por meio de câmaras de comércio, algo que remonta à Liga Hanseática. Daí ser o setor privado o *hub* do SIE e não o governo. É fundamental o papel do Círculo Interministerial para a Proteção da Economia, criado em 2008 (POTTER, 1998, p. 60-61).

Foco especial tem sido dado a empresas e governos estrangeiros, especialmente da França, do RU, dos EUA e do Leste Europeu, de forma a proteger a Alemanha no que tange à Inteligência destes países. Marcante é a requisição dos melhores Oficiais de Inteligência do Serviço Externo da Alemanha, o BND, e da Polícia Federal Criminal (BKA, da sigla em alemão), para gerenciar a coleta de dados econômicos. Talvez uma fraqueza do SIE alemão seja a tendência a concentrar como fontes de informação os institutos de pesquisa, fornecedores privados de informação e redes comerciais alemãs.

Diferentemente dos SIEs da Alemanha e do Japão, o SIE dos EUA é descentralizado, em razão do individualismo reinante no sistema político e econômico do país. Assim, alianças entre empresas no estilo japonês *(keiretsu)* foram historicamente curtas. As grandes empresas americanas, em decorrência de seu poder financeiro, têm sido capazes de desenvolver intensa inteligência competitiva (MARTRE, 1994). Potter destaca, por exemplo, que o orçamento para a inteligência competitiva da General Motors excedia, na década de 1990, o do Serviço de Inteligência Externa da França (POTTER, 1998). Diante da dispersão e concentração nas empresas e da necessidade de se organizar o fluxo de inteligência econômica no governo federal, a IEE ganhou forte impulso durante o governo de Bill Clinton (1993-2001), que passou a contar com estrutura estatal focada na busca de vantagens competitivas para empresas americanas em determinados setores industriais. Em 1993, criou-se o Conselho Econômico Nacional (NEC, da sigla em inglês), órgão máximo de assessoria econômica presidencial[10], que ocupa o mesmo nível que o Conselho de Segurança Nacional (SANDOVAL, 2006, p. 20). Já no início da década de 1990, sucessivos diretores da CIA, entre eles William Webster e R. James Woolsey, indicavam a IEE como de importância fundamental para a comunidade de Inteligência dos EUA (DÍAZ, 2014, p. 356). Desde então, as empresas passaram a cooperar mais com o governo no sentido de criar e desenvolver estratégia internacional de negócios. Em 1996 votou-se o *Economic Espionage Act,* de modo a proteger os segredos dos negócios americanos.

10 O presidente recebe, diariamente, além de relatório de segurança, relatório de IEE.

A atuação da CIA salientou-se, entre outros eventos, nas negociações bilaterais EUA-Japão sobre automóveis em 1994, quando agentes da Agência estavam entre os negociadores comerciais americanos, de modo a avaliar a pressão que estes podiam exercer sobre suas contrapartes japonesas. De igual modo, um ano antes, durante a Rodada Uruguai de comércio, a CIA proveu o governo das conversas de membros que negociavam o acordo comercial, especialmente franceses, e da Comissão Europeia. Ademais, ilustra ajuda a atores comerciais nos EUA episódio envolvendo a Hughes Aircraft, quando, em abril de 1993, esta decidiu não participar do Bourget Air Show após alerta da CIA de que a companhia estava sendo espionada pelo Serviço de Inteligência francês. O presidente da Hughes tinha sido informado que a empresa estava numa lista de 49 companhias americanas objeto de ação da Inteligência da França.

A França, ao analisar a perda de competitividade de sua inserção internacional no mundo, publicou, em 1994, o Informe Martre, referência maior da IEE do país[11], que estimulou a criação do Comitê para a Competitividade e Segurança Econômica (CCSE), similar ao NEC dos EUA, subordinada ao Primeiro-Ministro. O Informe apontou a necessidade de pesquisa coordenada, processamento e difusão de Inteligência a atores econômicos estratégicos. Posteriormente, em 2003, publicou-se o Informe Carayon, que fortaleceu a IEE como questão de Estado e criou um SIE dirigido por alto funcionário subordinado a um comitê sob responsabilidade de representante do Primeiro Ministro. Em tal comitê estavam representados o Presidente da República, o Primeiro Ministro, os Ministros do Interior, de Relações Exteriores, de Defesa e de Economia. Em 2009, o alto representante passou a ser o delegado interministerial para assuntos de IEE (D2IE), encarregado de elaborar a política pública francesa de IEE (RODRÍGUEZ, 2016). Participam do sistema órgãos estatais, empresas de Inteligência estratégica e câmaras de comércio, que avançam os quatro pilares prescritos no Informe Martre: fomentar a participação de empresas; otimizar o fluxo de informações entre os setores público e privado; construir base de dados adaptada às necessidades de usuários; e fomentar a formação e a educação em IEE. A IEE na França tem permitido a empresas como Airbus, Renault, Total, PSA-Citröen, Areva, Air France, entre outras, importantes contratos no Irã e países da América Latina. Ressalta-se que se menciona a IEE francesa até mesmo no Livro Branco de Defesa da França.

SIE no Brasil: uma proposta inicial e problemas potenciais associados à IEE nas relações entre o estado e o setor privado

No Brasil, não há grande estratégica nacional ou estratégia econômica nacional que alie interesses nacionais ou interesses nacionais econômicos específicos, o que desfavorece, embora não incapacite, a criação e o

11 Para análise histórica da IEE francesa, ver GIUSEPPE, Gagliano. *Economic Intelligence Culture in France*. Disponível em: <moderndiplomacy.eu>. Acesso em: 21 out. 2017.

desenvolvimento de SIE integrado. De modo geral, portanto, setores estratégicos da economia nacional não são selecionados[12] de modo a orientar o Estado a fomentar empresas e interesses para promover melhor inserção internacional do País, com vistas a seu desenvolvimento econômico e social.

Deve-se ter em mente que a existência de colegiado como o SIE brasileiro, em que as orientações estratégicas gerais seriam discutidas de modo coordenado e transparente, pode contribuir para o necessário enfraquecimento de práticas desleais na economia nacional, as quais podem desencadear corrupção e escolha ineficiente de setores a serem objeto de incentivos, por meio de contratos com o setor público, financiamento estatal e até mesmo sociedades entre o Estado e empresas privadas, o que pode, por sua vez, levar à internacionalização de companhias de área duvidosamente estratégica, causando perda de capacidade em desenvolvimento do País, como bem destacou o economista José Roberto Mendonça de Barros MENDONÇA DE BARROS (2017).

Como guia inicial para este fim, no âmbito do Sisbin, entre os atuais 39 órgãos de 16 ministérios ou instituições de nível ministerial, pode-se já identificar o aparato estatal da comunidade de Inteligência vinculado às políticas públicas econômicas. Sugere-se, por natural atuação estratégica na área econômica do País, ademais de já a compor o Sistema, incluir, além da Secretaria-Geral, as seguintes Subsecretarias-Gerais do MRE: Assuntos Econômicos e Financeiros; Meio Ambiente, Energia, Ciência e Tecnologia; e Cooperação Internacional, Promoção Comercial e Temas Culturais. Além dos órgãos do Ministério da Fazenda (MF) já participantes, a Comissão de Valores Mobiliários (CVM). E, ainda, o MDIC, com sua Câmara de Comércio Exterior (CAMEX) e o Instituto Nacional de Propriedade Industrial (INPI), juntamente com sua Secretaria-Executiva; os adidos agrícolas do Ministério da Agricultura, Pecuária e Abastecimento (MAPA); e o MPOG, a contemplar também o Ipea e o Banco Nacional de Desenvolvimento Econômico e Social (BNDES).

Além destes, haja vista a sinergia entre o Estado e outros atores relevantes na condução da economia nacional, necessária a um SIE, sugerem-se como integrantes do SIE brasileiro as seguintes instituições: Apex-Brasil, de cujo Conselho Deliberativo participam o MRE, o MAPA, o MDIC, a Secretaria-Executiva do Programa de Parcerias de Investimentos (PPI), e o BNDES; a CNI; a Agência Brasileira de Desenvolvimento Industrial (ABDI); a CNA; o Serviço Brasileiro de Apoio às Micro e Pequenas Empresas (Sebrae); a Associação de Comércio Exterior do Brasil (AEB); a Fundação Centro de Estudos do Comércio Exterior (FUNCEX); a Petrobras; as empresas ligadas à Indústria de Defesa Nacional, tendo por marcos a Política Nacional de Defesa (PND) e a Estratégia Nacional de Defesa (END); universidades; e *think tanks,* como a Fundação Getúlio Vargas (FGV).

12 A PNI sinaliza apenas de modo genérico tais setores, ao aludir que se deve proteger e impulsionar interesses nacionais econômico-financeiros e científico-tecnológicos.

Assim, no âmbito do Sisbin, o SIE brasileiro contaria com os seguintes participantes:

MINISTÉRIO	ÓRGÃO
1 - Gabinete de Segurança Institucional da Presidência da República (GSI/PR)	• Agência Brasileira de Inteligência
2 - Casa Civil (CC/PR)	• Secretaria-Executiva (SE/CC/PR)
3 - Ministério da Defesa	• Subchefia de Inteligência de Defesa (SC-2/MD)
4 - Ministérios das Relações Exteriores	• Secretaria-Geral (SG/MRE); • Subsecretaria-Geral de Assuntos Econômicos e Financeiros; • Subsecretaria-Geral de Meio Ambiente, Energia, Ciência e Tecnologia; • Subsecretaria-Geral de Cooperação Internacional, Promoção Comercial e Temas Culturais;
5 - Ministério da Fazenda	• Secretaria-Executiva do Conselho de Controle de Atividades Financeiras (SE/COAF/MF) • Secretaria da Receita Federal do Brasil (RFB/MF); • Banco Central do Brasil (BCB/MF); • Comissão de Valores Mobiliários (CVM/MF);
6 - Ministério do Trabalho	• Secretaria-Executiva
7 - Ministério da Ciência, Tecnologia, Inovação e Comunicações	• Gabinete do Ministro de Estado (GAB/MCTI);
8 - Ministério da Agricultura, Pecuária e Abastecimento	• Secretaria-Executiva (SE/MAPA);
9 - Ministério dos Transportes, Portos e Aviação Civil	• Secretaria-Executiva (SE/MTPAC);
10 - Ministério das Minas e Energia	• Secretaria-Executiva (SE/MME);
11 - Ministério da Indústria, Comércio Exterior e Serviços	• Câmara de Comércio Exterior (CAMEX); • Instituto Nacional de Propriedade Industrial;
12 - Ministério do Planejamento, Orçamento e Gestão	• Instituto de Pesquisa Econômica Aplicada (Ipea); • Banco Nacional de Desenvolvimento Econômico e Social

Fonte: adaptado pelo autor (quadro de integrantes do Sisbin)

De modo geral, os atores econômicos estatais envolvidos no desenvolvimento do SIE brasileiros, seriam de três níveis:

1. Nível 1: Grandes coletores de dados, que necessitam de mais profundo processamento, como o MRE, que não coleta dados de modo sistemático, e o MDIC, por meio da Secretaria de Comércio Exterior (Secex), cujo foco de atuação é o aparato técnico relativo à operacionalidade do comércio exterior (questões documentais aduaneiras, etc.), e acordos comerciais específicos;

2. Nível 2: Órgãos que não coletam dados de modo sistemático para a IE, mas que possuem forte capacidade de processamento, como o Banco Central do Brasil (BCB) e o Tesouro Nacional, do MF; e

3. Nível 3: Coletores e grandes demandantes de dados, como o MAPA, cuja requisição necessita ser constantemente orientada.

À Abin, órgão central do Sisbin, poderia caber a coordenação do SIE no contexto de sua experiência no âmbito do Sistema, oferecendo aos atores públicos fundamentais no campo econômico plataforma de coordenação e desenvolvimento de consensos, e também cumprir a tarefa de proporcionar maior integração com órgãos nacionais precipuamente atuantes nas políticas públicas econômicas, e de prospecção de cursos, inclusive de pós-graduação, em centros especializados no tema, como aqueles de universidades francesas e espanholas, bem como em *think tanks,* como o *Eurasia Group* que, em parceria com a *NYU Stern School of Business,* da Universidade de Nova Iorque (NYU, da sigla em inglês), possui cursos como o *Global Political Risk and its Impact on Business* que, tangentes à área, podem enriquecer a formação dos Oficiais de Inteligência.

Como áreas de acompanhamento do SIE para o Brasil, em razão das necessidades inerentes a sua melhor inserção no mundo e capacidades produtivas, sugerem-se as seguintes:

a) Comércio internacional, tanto no que se refere às negociações internacionais, como na análise de práticas desleais de comércio (agricultura, etc.);

b) investimentos externos;

c) sistema financeiro internacional, não só em sentido macroeconômico, como especificamente no que concerne a indicadores de investimento e formulação de *ratings,* os quais são formulados por comitês deliberativos privados;

d) aspectos macroeconômicos de países que afetem mais fortemente a economia internacional, em particular as políticas monetária e fiscal;

e) desenvolvimento em ciência e tecnologia estrangeira em setores estratégicos, entre eles aqueles relacionados à indústria nacional de defesa;

f) energia;

g) práticas desleais de setores e empresas competidoras estrangeiras de seus equivalentes no país;

h) propriedade intelectual;

i) marcos regulatórios ou regimes internacionais de comércio, investimentos, propriedade intelectual;

j) campanhas internacionais de desestabilização;

k) desinformação de modo a favorecer interesses estrangeiros;

l) influência e interferência externas;

m) desinformação; e

n) estudos acerca da concorrência internacional em setores e empresas estratégicos.

Considerações finais

À parte dos sucessos no setor agropecuário, o Brasil tem fracassado em muitos aspectos de sua inserção econômica internacional, em particular por não saber o que efetivamente quer, pode e deve fazer para se desenvolver. Contudo, a ausência de grande estratégia nacional ou, no que se refere à economia, de estratégia econômica nacional, apesar de enfraquecer a construção de projeto futuro do Brasil no seio de suas relações econômicas internacionais de modo competitivo, dando ensejo assim a seu desenvolvimento, não deve prejudicar a tarefa árdua, mas necessária, de se criar mecanismo capaz de coordenar e gerar consenso sobre os caminhos que o País quer e precisa seguir, sob pena de se ver perdido e com a soberania ameaçada por interesses estrangeiros. A criação e o desenvolvimento do SIE brasileiro, embora aqui propostos de modo preliminar, sujeito, portanto, a revisões de toda ordem e aprofundamento futuro, são parte de tal mecanismo.

Nas bases criativas do SIE brasileiro, como aludido, persistem desafios, os quais podem ser superados, entre outras medidas, por meio de transparência e diálogo no âmbito do SIE, entre eles o da priorização indevida de empresas na economia nacional, de setores de valor estratégico duvidoso. Discussões transparentes sobre que setores selecionar como objeto de fomento econômico estatal, amparadas tanto na PNI como na ENINT, podem mitigar tais práticas.

Por fim, passível de futura pesquisa, entre outros desafios político-institucionais e técnicos, resta desenvolver forma de integrar à estrutura de SIE atores privados, como empresas, fundações, universidades e *think tanks* fundamentais ao Sistema.

Referências

ANGELIS, Cristiano Trindade. Uma proposta de um modelo de inovação e inteligência governamental. In: *Revista de Administração e Inovação,* São Paulo, v. 10, n.3, p. 297-324, jul./set. 2013.

ARENAS, Eduardo Olier. Strategic Intelligence and Economic Security. In: ESPANHA. Ministry of Defence. *Strategic Dossier 162 B Economic Intelligence in a Global World.* Spanish Institute for Strategic Studies, 2014.

BENJAMIM, Daniela Arruda. *O Sistema de Solução de Controvérsias da OMC*. Brasília: Fundação Alexandre de Gusmão, 1995.

BRASIL. Brasil: um país em busca de uma grande estratégia. *Relatório de conjuntura n. 01*. Presidência da República, Secretaria-Geral da Presidência, Secretaria Especial de Assuntos Estratégicos. Brasília: 2017.

_____. Constituição (1988). *Constituição da Republica Federativa do Brasil*. Org. de Alexandre de Moraes. 16.ed, São Paulo: Atlas, 2000.

_____. Gabinete de Segurança Institucional. Agência Brasileira de Inteligência. *Doutrina Nacional de Inteligência: fundamentos doutrinários.* Brasília: Abin, 2016.

_____. Decreto no 8.793, de 29 de junho de 2016. Fixa a Política Nacional de Inteligência. *Diário Oficial da República Federativa do Brasil,* Poder Executivo, Brasília, DF.

_____. Lei no 9.883, de 7 de dezembro de 1999. Institui o Sistema Brasileiro de Inteligência, cria a Agência Brasileira de Inteligência – Abin e dá outras providências. *Diário Oficial da República Federativa do Brasil,* Poder Executivo, Brasília, DF.

CLERC, Philippe. Inteligência econômica: desafios atuais e perspectivas. In: *A Informação: tendências para o novo milênio.* Brasília: IBICT, 1999. P. 130-143.

DÍAZ, Gustavo. De la cooperación a la competición: la inteligencia económica en el marco de la estrategia de seguridad nacional 2013. *UNISCI Discussion Papers,* No 35, 2014.

ESPANHA. Ministerio de Defensa. El sistema de inteligéncia económica en España. Documento de Trabajo 07/2016. In: *Plan Anual de Investigación 2016*. Instituto Español de Estudios Estrategicos

_____. *Strategic Dossier 162 B Economic Intelligence in a Global World.* Spanish Institute for Strategic Studies, 2014.

GARCÍA, Jesús Santiago Fernández. Situación de la inteligência económica en España. In: ESPANHA. Ministerio de Defensa. El sistema de inteligência económica en España.

Documento de Trabajo 07/2016. *Plan Anual de Investigación 2016*. Instituto Español de Estudios Estrategicos.

GIAMBIAGI, Fabio & PORTO, Cláudio (2011) 2022: *propostas para um Brasil melhor no ano do bicentenário.* Rio de Janeiro: Editora Elsevier, 2011.

GÓMEZ, Andrés Montero; RAMÍREZ, José Martin. *Inteligencia económica como vector internacional de seguridad.* Madrid: Real Instituto Elcano, 2008. (Documento de Trabajo, n. 18/2008).

IVAN, Valeriu. Economic Intelligence. In: *Journal of Knowledge Management, Economics and Information Technology,* Special Issue, December 2013.

_____ . *Economic Intelligence: Instrument for Achieving Romania's Economic Security.* In: *International Scientific Conference Strategies XXI the complex and dynamic nature of the Security Environment.* v.1 Bucharest - Romania 2015.

_____*Models of Competitive Intelligence on the State Level. Common Elements and Carachteristic Landmarks. The 11th International Scientific Conference "Defense Resources Management in the 21st century".* Brasov, Nov. 10th 2016.

MARTRE, Henri. *Intelligence économique et stratégie des enterprises.* Paris: La Documentation Française, 1994. Disponível em: <www.ladocumentationfrancaise.fr/var/storage/rapports-publics/074000410.pdf>. Acesso em: out. 2017.

MENDONÇA DE BARROS, José Roberto. *JBS: vale a pena um campeão nacional?* Disponível em: <economia.estadao.com.br/noticias/geral,jbs-vale-a-pena-um-campeao-nacional-imp-,636 021> . Acesso em: 17 nov. 2017.

MOREIRA & ARAÚJO JR. Comércio Exterior e Crescimento: Diagnóstico e uma Agenda para 2022. In: GIAMBIAGI, Fabio e PORTO, Cláudio (2011) *2022: propostas para um Brasil melhor no ano do bicentenário.* Rio de Janeiro: Editora Elsevier, 2011

PORTEOUS, Samuel D. Economic and Commercial Interests and Intelligence Services. In: Potter, Evan H. (ed.) *Economic Intelligence & National Security.* Ottawa: Carleton University Press & The Centre for Trade Policy and Law, 1998. p. 79-128.

POTTER, Evan H. (ed.) *Economic Intelligence & National Security.* Ottawa: Carleton University Press & The Centre for Trade Policy and Law, 1998.

REVEL, Claude. *Economic Intelligence: An Operational Concept for a Globalised World.* Disponível em: em <www.realinstitutoelcano.org/wps/portal/web/rielcano_en/contenido? WCM_GLOBAL_CONTEXT=/elcano/elcano_in/zonas_in/defense+security/ari134-2010>. Acesso em: 16 nov. 2017.

RIBEIRO, Anna Carolina M. L. *Sistema Brasileiro de Inteligência Econômica: reflexões para o estabelecimento de uma rede inicial de atores*. Dissertação de Mestrado de Economia a Brasília: UnB, 2016.

RODRÍGUEZ, Jorge Vilas. *Francia y la Inteligencia Económica: una cuestión de Estado*. Documentos de Trabajo 2/2016. Madrid: Centro de Análisis y Prospectiva, Gabinete Técnico de la Guardia Civil, 2016.

SANDOVAL, Mario. La Inteligencia Económica: La Función y El papel del Gobierno. In: *Puzzle*-Año 5. ed, n. 2 mayo-jul. 2006. Barcelona: 2006.

WALTZ, Kenneth. Reductionist Theories. In: *Theory of International Politics. Berkeley*. University of California, 1979. p. 19-38.

ZELIKOW, Phillipe. American economic intelligence: past practice and future principles. *Intelligence and National Security,* v. 12, no. 1, p. 164-177, 1997.

A AGENDA LEGISLATIVA DA ABIN: ANÁLISE DAS PROPOSIÇÕES SOBRE ATIVIDADE DE INTELIGÊNCIA DE ESTADO NO CONGRESSO NACIONAL DE 1997 A 2017.

Lívia Sales *
Luiz Antônio P. Valle **

Resumo

Este artigo identifica proposições legislativas apresentadas no âmbito do Congresso Nacional no período de 1997 a 2017 sobre Atividade de Inteligência de Estado (AI), desde o recebimento pelo Congresso da Mensagem Presidencial nº 1.053, de 19 de setembro de 1999, que Institui o Sistema Brasileiro de Inteligência, cria a Agência Brasileira de Inteligência (Abin), e dá outras providências, a qual iniciou sua tramitação na Câmara dos Deputados como Projeto de Lei nº 3.651/1997, até o final da Sessão Legislativa de 2017. Os principais resultados indicam que os assuntos sobre AI têm dificuldades de serem pautados com prioridade, devido à quantidade de matérias no Congresso para serem deliberadas, o que exige uma atuação dos segmentos interessados junto aos parlamentares para que o assunto focado passe à frente da fila, notadamente no esclarecimento acerca da importância da temática para a soberania nacional, uma vez que no País inexiste uma cultura de inteligência adequada. Portanto, a celeridade na tramitação das propostas e seu resultado final dependem fundamentalmente da influência sobre o Parlamento daqueles que têm interesse no assunto objeto da matéria, o que requer estratégia específica para cada proposta e uma conjuntura que incentive a vontade política do Congresso na defesa de determinadas pautas.

Palavras-chaves: Agência Brasileira de Inteligência, Poder Legislativo, Atividade de Inteligência de Estado (AI).

ABIN LEGISLATIVE AGENDA: ANALYSIS OF LEGISLATIVE PROPOSALS ON STATE INTELLIGENCE AT THE BRAZILIAN CONGRESS FROM 1997 TO 2017

Abstract

This article identifies legislative issues regarding State Intelligence Activity (IA), presented at the Brazilian Congress from 1997 to 2017, since the reception by Congress of Presidential Message No. 1.053 of September 19, 1999 - which "establishes the Brazilian Intelligence System, creates the Brazilian Intelligence Agency (Abin), and gives other provisions", which began its proceedings in the House of Representatives as Bill No. 3.651/1997, until the end of the 2017 legislative session. The main results indicate that IA issues are hardly prioritized, due to the amount of issues in the Congress to be deliberated, which requires that the interested segments interact with the parliamentarians to put a specific issue on the Congress calendar, and especially to explain the importance of the theme for national sovereignty, since in the country there is still the lack of IA culture. The speed with which proposals are processed and their final outcome depend crucially on the influence of those who have an interest in the subject matter on the Parliament, which requires a specific strategy for each issue and an environment that encourages the political will of the Congress to defend certain timetables.

Key-words: Brazilian Intelligence Agency, Legislative Power, State Intelligence Activity (IA)

---

* Bacharel em Ciência Política (UnB/DF) e Especialista em Inteligência Estratégica em curso promovido pela Adesg/MT.

** Especialista em Política Estratégica e bacharel em Administração de Empresas (Bennett/RJ)

Artigo recebido em setembro/2018
Aprovado em setembro/2018

Introdução

Segundo (CEPIK, 2004, p. 68) "[...] a existência de serviços de inteligência institucionalizados, isto é, legítimos e efetivos, é condição necessária para um Estado democrático garantir a segurança dos cidadãos e promover o interesse público".

Considerando-se a importância desta premissa, este artigo tem como objetivo identificar propostas que marcaram a agenda do Parlamento no que diz respeito a Atividade de Inteligência de Estado (AI), por meio de pesquisa sobre as proposições legislativas, apresentadas no âmbito do Congresso Nacional, no período de 1997 a 2017, desde o encaminhamento da Mensagem Presidencial nº 1.053, de 19 de setembro de 1997, que "Institui o Sistema Brasileiro de Inteligência, cria a Agência Brasileira de Inteligência (Abin), e dá outras providências", até o final da sessão legislativa de 2017.

A aprovação pelo Legislativo desta Mensagem, que tramitou como Projeto de Lei (PL) nº 3651/1997, foi ratificada pelo Presidente da República e sancionada sem vetos, nos termos da na Lei nº 9.883, de 7 de dezembro de 1999, que prevê o exercício da atividade de Inteligência de Estado no Brasil pela Agência Brasileira de Inteligência (Abin), atualmente vinculada ao Gabinete de Segurança Institucional da Presidência da República (GSI/PR).

Esta lei simbolizou o primeiro passo recente na implantação de um Sistema De Inteligência, subordinado ao primeiro escalão da República, para reposicionar a atividade, sendo também o marco referencial que norteia toda a regulamentação da AI em vigor no País.

Mesmo após a introdução desta nova legislação, é possível identificar que ela não teve o mote de tornar a AI mais conhecida e compreendida. Segundo o Relatório Final da Comissão Parlamentar de Inquérito (CPI) do Senado, conhecida como "CPI da Espionagem", apresentado em 2014, p. 87: "[...] Pouco se conhece e pouco se discute sobre os serviços secretos e seu trabalho. De fato, quase três décadas após o fim do período militar no Brasil, a Atividade de Inteligência ainda é vista como algo ilegítimo e relacionado à ditadura".

Metodologia aplicada

A metodologia aplicada para este artigo consistiu na pesquisa de proposições legislativas sobre AI, na rede mundial de computadores, na base de dados dos sites institucionais da Câmara dos Deputados (CD), do Senado Federal (SF) e do Congresso Nacional (CN) e na análise do processo de tramitação das matérias no âmbito do Congresso.

Entende-se como proposição legislativa[1] toda a matéria sujeita à deliberação do Congresso, tais como: propostas de

1 Brasil. Congresso Nacional. Senado. Regimento Interno (1892). Disponível em: <www25.senado.leg.br/web/atividade/regimento-interno>. Acesso em: 18 out. 2018 Brasil. Congresso Nacional. Câmara dos Deputados. Regimento Interno. Disponível em: www.camara.gov.br/internet/legislacao/regimento_interno/RIpdf/RegInterno.pdf. Acesso em: 18 out. 2018

emenda à Constituição, projetos de lei, requerimentos, indicações, proposta de fiscalização.

Para a coleta de dados, realizou-se pesquisa por palavras-chave que mencionam expressamente a Abin e/ou AI nas ementas das proposições; em seguida, analisou-se individualmente cada proposta com o objetivo de verificar se a matéria atendia à pertinência temática escolhida.

Para efeitos do escopo delineado para esse artigo, não foram computadas proposições que discorrem sobre a legislação de Atividade De Inteligência executadas por outros órgãos da administração pública federal, como, por exemplo, órgãos vinculados à Segurança Pública e às Forças Armadas. Estes poderão ser objeto de outro artigo no futuro.

O Congresso Nacional e a Atividade de Inteligência

A Constituição Federal estabelece o Poder Legislativo, exercido pelo Congresso Nacional, composto pela Câmara dos Deputados e pelo Senado Federal, para desempenhar as funções de representação, fiscalização e controle (arts. 44 a 69).

As competências e o funcionamento de cada uma, respeitadas as diretrizes da Constituição, estão previstas em seus respectivos regimentos. Normalmente as Casas atuam separadas, uma funciona como iniciadora e a outra como revisora. Quando o Congresso se reúne, aplica-se o regimento comum, como, por exemplo, para apreciação vetos.

Os legisladores, além da função de discutir e votar projetos de lei, também possuem prerrogativas para realizar audiências públicas, convocar e convidar Ministros de Estado para prestarem informações, aprovar/desaprovar o orçamento e a indicação de autoridades, acompanhar a execução das políticas públicas governamentais, fiscalizar os atos do Poder Executivo e, inclusive, sustar atos normativos do Executivo que extrapolem o poder regulamentar ou os limites da competência legislativa.

No que se refere à fiscalização da AI, a Lei nº 9.883/1999, determinou que "[ ] controle e fiscalização externos da Atividade De Inteligência serão exercidos pelo Poder Legislativo na forma a ser estabelecida em ato do Congresso Nacional" (art. 6º).

Conforme previsto no artigo supracitado, o Congresso Nacional instalou em 21 de novembro de 2000 a Comissão Mista de Controle das Atividades de Inteligência (CCAI), composta por seis senadores e seis deputados, regulamentada pela Resolução do Congresso Nacional nº 2, de 22 de novembro de 2013, originária do Projeto de Resolução do Congresso (PRN) nº 02/2008. Nas competências da CCAI previstas nesta Resolução, destaca-se o exame preliminar de todas as matérias sobre esta temática que sejam apresentadas no Parlamento.

A tramitação legislativa e a análise dos dados

No Legislativo, toda nova proposta integra-se ao banco de dados da Casa iniciadora, que contém todas as proposições apresentadas e seu respectivo status. Para se ter uma ideia

deste quantitativo apenas na Câmara dos Deputados, considerando-se o período de 1997 a 2017 delimitado para essa pesquisa, foram apresentados, segundo o *site* da CD: 42.387 projetos de lei (PLs), destes 18.928 encontram-se em tramitação; 76.342 requerimentos (REQs), dos quais 11.010 ainda não tiveram seu curso encerrado; e 23.622 Requerimentos de Informação (RICs), e destes ainda possuem 1.165 em trâmite; ou seja, são 142.351 proposições legislativas.

Estes dados fornecem uma noção do volume de matérias que circulam no Congresso Nacional sobre os mais variados assuntos, demonstrando a necessidade de monitorar a rotina de trabalho das Casas, com a finalidade de identificar matérias de interesse e planejar estratégias para influenciar o Legislativo na formulação da pauta.

Portanto, a celeridade na tramitação das propostas e seu resultado final dependem fundamentalmente da influência a ser exercida sobre o Parlamento por aqueles que têm interesse no assunto objeto da matéria em trâmite, o que requer estratégia específica para cada proposição e uma conjuntura que incentive a vontade política do Congresso na defesa de determinados temas. Para ilustrar esta questão, importa citar que, das matérias apresentadas que chegaram a seu deslinde, ou seja, viraram norma jurídica, apenas 18,75% (3 dentro de um universo de 16) tratam da AI propriamente, as demais cuidam de questões vinculadas a administração, tais como: carreira, estrutura hierárquica, fiscalização e orçamento.

Ademais, a grande quantidade de matérias em curso também resulta em uma disseminação diluída sobre as etapas do processo legislativo nos meios de comunicação, redundando em desinteresse da maioria da sociedade no que se refere ao impacto do que se delibera para a vida cotidiana.

Isto posto, vamos nos deter na parte da legislação atinente ao tema. Dentre as propostas analisadas para este artigo, destaca-se o marco referencial para a AI no país, o PL nº 3651/1997, de autoria do Poder Executivo, que dispõe sobre a criação da Abin, o qual, após os trâmites, transformou-se na Lei nº 9.883, de 7 de dezembro de 1999.

Ressalta-se que o PL nº 3651/1997 tramitou por 789 dias nas duas Casas. No Senado, quando tramitava há mais de dois anos, recebeu emenda substitutiva global, que, ao ser aprovada, exigia a aprovação da Casa iniciadora para seu prosseguimento. Foi neste momento que ela conseguiu um embalo para finalizar seu exame no legislativo. A emenda foi aprovada no Senado, passados 3 dias úteis foi recebida na Câmara e aprovada no dia seguinte.

Esta situação demonstra a inércia do Congresso ante um assunto de relevante importância e interesse para o Poder Executivo.

Somente após essa longa caminhada para se criar um órgão específico para Atividade de Inteligência de Estado, foi possível iniciar a regulamentação, o planejamento e a estrutura administrativa do órgão, o que representou um período de insegurança jurídica para o País em um contexto geopolítico sempre conturbado e repleto de ameaças com potencial ofensivo variado.

No que se refere às proposições sobre AI, analisou-se informações sobre a tramitação de 152 matérias na Câmara dos Deputados, 46 no Congresso Nacional e 78 no Senado. No Gráfico 1 abaixo, podemos ver sua distribuição no período.

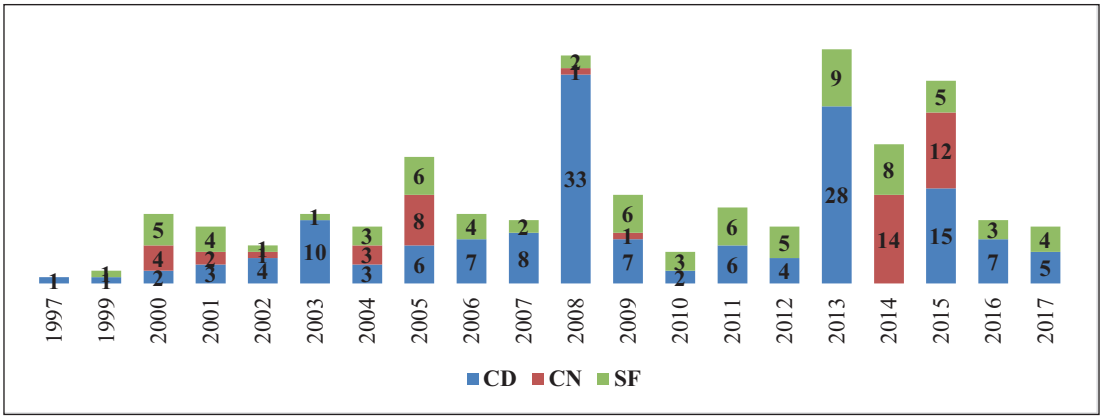


Gráfico 1 – Quantitativo de proposições apresentadas por ano e Casa Legislativa
Fonte: *sites* CD, SF & CN 2017

Comparativamente ao volume total de proposições legislativas citadas no início deste tópico, observa-se que, mesmo após a sanção da Lei nº 9.883/99, não houve incremento significativo na quantidade de propostas apresentadas.

No Congresso (CN), o ano de 2014 apresentou a maior quantidade de propostas; na Câmara dos Deputados (CD), foram os anos de 2008 e 2013, no Senado (SF) foram 2013 e 2014.

Nota-se uma concentração de proposições no período de 2013 a 2015, tendo o ano de 2008 como um ponto fora da curva, todos com mais de 20 matérias.

No Congresso, em 2014, a CCAI se destacou como a autora do maior número de propostas, em decorrência da aprovação de seu regimento no final de 2013, que permitiu a execução de suas atividades.

No ano de 2008, alguns fatos noticiados pelos meios de comunicação sobre espionagem marcaram a agenda da Câmara, com destaque para as denúncias que indicavam a participação de agentes da Abin em escutas telefônicas em operações da Polícia Federal, dentre as principais, uma conhecida como *Satiagraha,* e escutas ilegais de autoridades do Supremo Tribunal Federal (STF). A divulgação de trechos de conversas que vieram a público gerou desconforto na relação entre os Poderes, o que contribuiu para o afastamento do Diretor Geral da Abin (em 2008) até a conclusão das investigações. Neste contexto, o Parlamento também respondeu à sociedade com a apresentação de diversas proposições voltadas ao fortalecimento do controle sobre a Atividade de Inteligência.

No período de 2013 a 2015, as agendas da Câmara e do Senado repercutiram o vazamento de informações divulgadas por Edward Snowden, ex-prestador de serviços

para a Agência Nacional de Segurança dos EUA (NSA), sobre a espionagem de diversas autoridades mundiais pelo serviço secreto dos Estados Unidos da América (EUA), bem como de algumas empresas como, por exemplo, a Petrobrás, o que surpreendeu o alto escalão do governo federal, tendo inclusive sido instalada uma CPI no Senado para investigar esta questão, que, em seu relatório final, identificou diversos pontos com necessidade de inovação legislativa em prol da segurança da AI no Brasil.

Outro tópico que influenciou a agenda parlamentar nesta ocasião foi a apresentação de requerimentos e a realização de audiências públicas sobre as ações de Inteligência voltadas para a segurança na realização de grandes eventos, uma vez que houve o advento da Copa do Mundo em 2014 e as Olimpíadas na cidade do Rio de Janeiro em 2016. Este tema, bem como seus desdobramentos (segurança na fronteira, recrutamento de jovens pelo Estado Islâmico, etc.) gerou uma movimentação legislativa não usual, o que também contribuiu para que fossem debatidas perspectivas para a AI e a necessidade de adequações na legislação vigente.

Os parlamentares também identificaram que a AI, devido a sua importância estratégica, também precisava constar na Carta Magna. Para atingir este objetivo apresentaram quatro (4) propostas de emenda à Constituição (PECs) – duas na CD e duas no SF, das quais três (3) destas não conseguiram agilidade no trâmite e foram arquivadas ao final da legislatura.

A PEC remanescente tramita no Senado sob o nº 62/2012 e aguarda parecer da relatoria. Há pouca inovação no conteúdo do texto apresentado, considerando-se que a legislação infralegal vigente já trata a maior parte dos aspectos abordados na proposta. Isto posto, será necessária uma atualização da proposição.

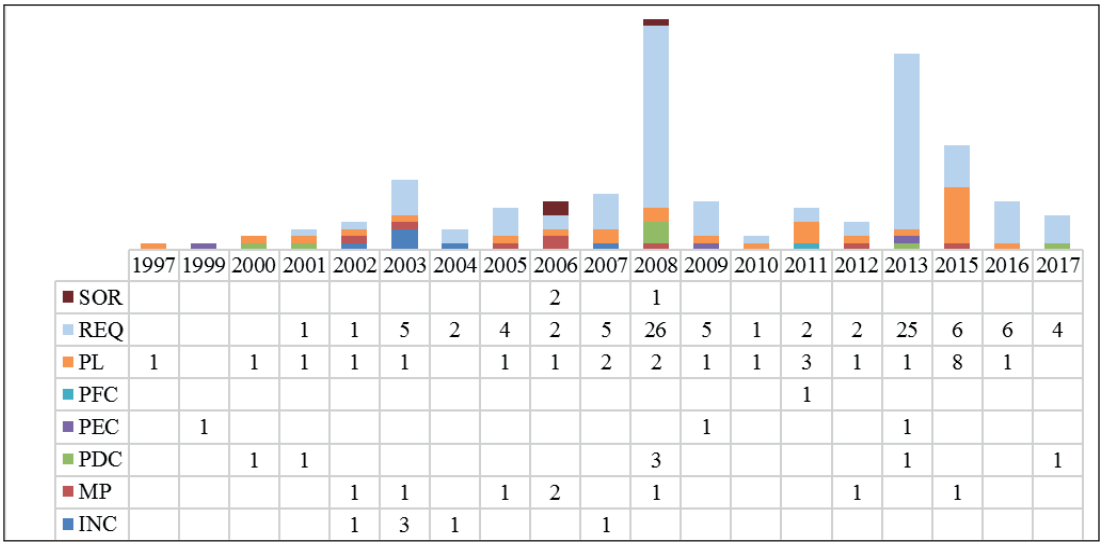
Ainda sobre o período analisado, o Parlamento também discutiu diversas propostas sobre carreiras, gratificações dos servidores e a estrutura da Abin, principalmente por meio de Medidas Provisórias, provavelmente com a finalidade de agilizar a implementação da estrutura administrativa da Agência, nos anos que sucederam a sanção da Lei nº 9.883, de 7 de dezembro de 1999, cujas aprovações dependeram de forte atuação da Casa Civil da Presidência da República e do líder do governo na articulação por prioridade na aprovação destas pautas.

Neste aspecto, destaca-se que compete ao Parlamento referendar ou emendar propostas que dispõem sobre as atribuições dos órgãos públicos, uma vez que compete ao Presidente da República privativamente, nos termos do art. 61 da CF, a iniciativa de leis desta natureza. Porém, o Congresso tem também apresentado propostas neste sentido como uma maneira de expressar sua vontade política, mesmo sabendo que a proposta está eivada de vício de iniciativa e que provavelmente será arquivada no Legislativo.

Contudo, no período analisado, não foi identificada apresentação de proposta específica sobre a Atividade de Inteligência, no que tange ao fortalecimento do arcabouço legal/institucional, que tenha tramitado com a urgência e a relevância que o recurso da

medida provisória permite. Por exemplo, a Lei nº 13.575, de 26 de dezembro de 2017, que cria a Agência Nacional de Mineração (ANM) e extingue o Departamento Nacional de Produção Mineral (DNPM), foi originária da MP nº 791/2017, um assunto relevante e estratégico que teve tramitação extremamente célere; diferentemente, a proposição que criou a Abin tramitou como projeto de lei ordinário.

O encaminhamento de proposições sobre AI ao Congresso, respeitando-se as prerrogativas previstas no art. 61 da Constituição, requer a realização de estudos técnicos prévios pelos órgãos da administração pública federal e posterior encaminhamento à Casa Civil para conhecimento, análise da conveniência e da oportunidade e decisão do Presidente da República (PR) A habilidade do Gabinete de Segurança Institucional (GSI) da PR no encaminhamento das articulações junto ao Executivo, notadamente no diálogo junto à Casa Civil na defesa de suas prioridades é essencial para que os objetivos no legislativo sejam atingidos.



	1997	1999	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2015	2016	2017
SOR									2		1								
REQ				1	1	5	2	4	2	5	26	5	1	2	2	25	6	6	4
PL	1		1	1	1	1		1	1	2	2	1	1	3	1	1	8	1	
PFC														1					
PEC		1										1				1			
PDC			1	1							3					1			1
MP					1	1		1	2		1				1		1		
INC					1	3	1			1									

Gráfico 2 – Tipo de proposição[2] apresentada por ano na Câmara dos Deputados.
Fonte: *site* CD 2017

2 Os significados das siglas apresentadas estão dispostos no Anexo I.

Observando-se, em detalhe, o quantitativo de proposições por tipo apresentada na Câmara, conforme o Gráfico 2 em 2008 e 2013, chama a atenção o quantitativo de requerimentos, os quais estão principalmente direcionados às atividades da CPI com a finalidade de investigar escutas telefônicas clandestinas/ilegais, conforme denúncia publicada na Revista "Veja", edição 2022, nº 33, de 22 de agosto de 2007 sobre a CPI da ESCUT), que teve 17 requerimentos aprovados, sendo 9 requerimentos de convocação para a Abin.

Nesta situação, observa-se que, por um lado, compete ao Legislador fiscalizar o Executivo e apresentar respostas à sociedade com transparência, mas, por outro, ele também precisa garantir o cumprimento de medidas que protejam a produção de conhecimento e o anonimato das fontes. O significativo número de audiências realizadas nesta CPI trouxe à tona a identidade de vários servidores da Abin, não somente ao Parlamento como para a toda a comunidade internacional, o que pode ser interpretado como uma falha na condução e na apuração de denúncias que envolvam conhecimentos sensíveis e estratégicos.

Nesse contexto sobre a preservação da identidade do servidor e da atividade da Agência, observou-se que matéria relevante foi proposta, o PL nº 6.873/2006, que, em sua justificativa, considera fundamental proteger a identidade dos profissionais para que o Sistema Brasileiro de Inteligência (Sisbin) possa cumprir seus objetivos e ainda informa que, nos EUA, é crime, desde 1992, a divulgação da identidade de funcionários da inteligência. Entretanto, o PL nº 6.873/2006 foi, surpreendentemente, arquivado ao final da legislatura, em janeiro de 2007, sem ter sido apreciado por nenhuma comissão. Considerando-se que a matéria foi apresentada em abril de 2006, provavelmente entrou na fila de espera e ficou à mercê de um articulador político forte para seu impulsionamento, pois que era ano eleitoral, e havia outras pautas ou houve algum ator que estrategicamente atuou para seu engavetamento.

Nem sempre os interesses, ou entendimento, dos parlamentares convergem com o do Executivo, denotando a absoluta importância da articulação junto aos congressistas. Como exemplo dos prejuízos que a ausência de uma ação de esclarecimento pode causar, destaca-se, no ano de 2008, o momento no qual os legisladores reagiram às declarações do então Diretor Geral da Abin Paulo Lacerda na CPI ESCUT, e propuseram dois projetos de decretos legislativos (PDCs nº 861/2008 e nº 1.322/2008) para sustar o Decreto nº 6.540, de 19 de agosto de 2008, que dispõe sobre o Sisbin e o compartilhamento de informações entre seus integrantes. Alegavam que o Chefe do Executivo havia extrapolado seu poder. Para alguns deputados, o referido decreto havia sido publicado com a finalidade de regularizar a suposta denúncia do uso indevido de agentes da Abin pela Polícia Federal durante a Operação Satiagraha, para outros ressoava que o Executivo estaria restabelecendo o antigo Serviço Nacional de Informação (SNI). Fica demonstrado que as leituras divergentes, por parte dos parlamentares, podem gerar reações indesejáveis. Estes PDCs acabaram arquivados.

Ainda no mesmo ano, destacou-se o requerimento REQ-CSPCCO 122/2008

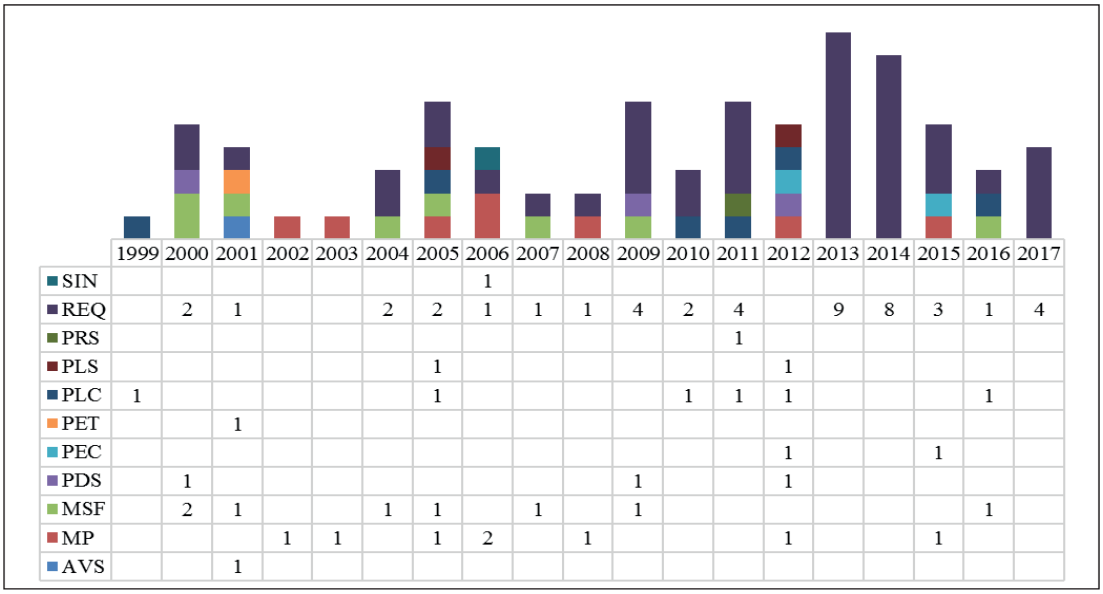
para a instalação de uma subcomissão para acompanhar atividades de Inteligência, informação e contrainformação do Governo Federal, no âmbito da Comissão de Segurança Pública e Combate ao Crime Organizado (CSPCCO), que foi retirada de tramitação a pedido do autor, quando este foi questionado por outro parlamentar, durante a apreciação do requerimento, sobre a necessidade da medida, uma vez que já existia a CCAI. Muitas vezes, há disputas na arena do Congresso quanto à autoria de propostas relevantes que possam fortalecer a imagem do Parlamentar.

Na época, tramitavam os PRNs nos 008/2001 e 02/2008, que dispõem sobre as finalidades, o funcionamento e a composição da CCAI com conteúdos idênticos, mas que tramitaram autonomamente por conveniência da relatoria. O primeiro, após dezessete anos, ainda se encontra em tramitação; o segundo foi aprovado, nos termos do substitutivo da relatoria, e transformou-se na Resolução no 02/13 do Congresso. Nesse caso, é possível que sejam realizadas ações para o arquivamento do PRN no 008/2001.

Nota-se ainda que as normas de funcionamento da CCAI foram aprovadas tardiamente, somente em 2013. O motivo para a demora é que ela passou mais de 1.000 dias na Mesa Diretora da Câmara, que teve de designar relatores mais de uma vez, o que, consequentemente, refletiu na demora da apresentação do parecer.

O grande número de requerimentos em 2013 deve-se a audiências públicas e convocação de ministros para apresentarem esclarecimentos sobre as informações divulgadas por Edward Snowden, bem como sobre as ações de monitoramento e contrainteligência realizadas pela Abin.

Outra temática presente nas proposições identificadas na pesquisa foi sobre o porte de arma aos agentes operacionais da Agência e a isenção de impostos para aquisição de equipamentos de segurança. Sobre este assunto, destacam-se o PL 7.528/2010, que foi arquivado ao final da legislatura sem ter sido apreciado por nenhuma comissão, o PL 5.982/2009, aprovado e enviado ao Senado e os PLs 553/2015, 1.263/2015 e 1.401/2015, que tramitam apensados (em um conjunto de 95 proposições) ao PL 3.722/2012 e aguardam inclusão na Ordem do Dia do Plenário. Desta feita, parece-nos oportuno sugerir que este último projeto seja objeto de uma vigorosa ação de monitoramento quanto às possíveis movimentações e inclusões de novos apensados, bem como uma efetiva ação, se necessária, a fim de evitar surpresas inesperadas ou desagradáveis ao final do trâmite legislativo. Cabe ressaltar que o arquivamento do PL 7.528/2010 provavelmente deveu-se ao fato de ter sido apresentado poucos meses antes do encerramento do período legislativo e seu autor não ter sido reeleito para o período seguinte.



	1999	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017
SIN								1											
REQ		2	1			2	2	1	1	1	4	2	4		9	8	3	1	4
PRS													1						
PLS							1							1					
PLC	1						1					1	1	1				1	
PET			1																
PEC														1			1		
PDS		1									1			1					
MSF		2	1			1	1		1		1							1	
MP				1	1		1	2		1				1			1		
AVS			1																

Gráfico 3 – Tipo de proposição apresentada por ano no Senado Federal[3]
Fonte: *site* SF 2017

No Senado, das oito Mensagens enviadas pelo Poder Executivo, conforme demonstrado no Gráfico 3, sete foram sobre a indicação do Presidente de República para o cargo de Diretor Geral da Abin, sendo todas aprovadas pelo Plenário. O que demonstra que o Parlamento também se corresponsabiliza pela condução dos assuntos sobre AI no Brasil.

Em complemento às propostas aprovadas na Câmara, o PL 5.982/2009, que dispõe sobre o porte de arma aos agentes, mesmo fora de serviço, tramitou no Senado como o PLC 87/2011 e foi objeto de veto presidencial total em 2013, por contrariedade ao interesse público. A então Presidente Dilma alegou que a matéria implicaria a circulação de maior quantidade de armas de fogo, em desacordo com o Estatuto do Desarmamento, e que há possibilidade de requisição de porte para a defesa pessoal conforme a necessidade de cada agente.

Ora, este veto mostrou-se impróprio, uma vez que, em todos os países desenvolvidos, os agentes de Inteligência possuem porte de arma, mesmo fora do serviço, pois o risco de vida a que se expõem os acompanha permanentemente. Ademais, neste caso, os agentes da Abin ficaram em desvantagem em relação aos Agentes de Inteligência Militar (AIM) e das Polícias (Militar, Civil, PF e PRF), que, por força da função, podem portar armas de fogo a qualquer momento.

Importa destacar que, no ano de 2013, o Senado aprovou a criação da chamada "CPI da Espionagem", destinada a investigar a denúncia de existência de um sistema de espionagem, estruturado pelo governo dos EUA, com o objetivo de monitorar *e-mails,* ligações telefônicas, dados digitais, além

3 Informações sobre as siglas apresentadas estão disponíveis no anexo I.

de outras formas de captar informações privilegiadas ou protegidas pela CF. O Relatório Final aprovado pela CPI, informa, na p. 135, que:

> Assim, diante do problema e da constatação de fragilidade em que se encontram a sociedade e o Estado brasileiro, percebe-se, no âmbito da Inteligência, a necessidade de mais investimentos e do aprimoramento do aparato brasileiro de contrainteligência. Apenas com mais contrainteligência e com o fomento a uma cultura de inteligência, segurança e proteção ao conhecimento, no setor público e na área privada, é que os brasileiros conseguirão fazer frente à ameaça da espionagem internacional.

O relatório supracitado possui outras recomendações, das quais destaca-se a importância de se realizar ampla reforma na legislação sobre AI, mediante comissão temporária no Senado, além de sugerir a apresentação de proposta com a finalidade de regulamentar o fornecimento de dados de cidadãos ou empresas brasileiras a organismos estrangeiros. O documento ressalta a necessidade de legislação específica para o uso de meios e técnicas sigilosas, a proteção dos profissionais e os procedimentos de aquisições e contratos; busca, ainda, respaldo na Lei de Acesso à Informação (LAI) na salvaguarda de assuntos sigilosos de interesse do Estado.

Considerações finais

Este artigo analisou a apresentação e a deliberação de matérias sobre a AI, no período de 19/9/1997 a 31/12/2017 no Congresso Nacional.

A pesquisa demonstra que as proposições sobre AI tiveram pouco destaque na agenda do Congresso Nacional, considerando-se o quantitativo total das matérias apresentadas. Identificou-se que houve avanços na legislação sobre as carreiras dos servidores da Abin, principalmente por meio de edição de medidas provisórias, pois o Estado precisava estruturar a recém-criada Agência. Contudo, a mesma celeridade não ocorreu com outras propostas que dispõem especificamente sobre a política da AI.

A leitura dos dados também demonstra a necessidade de se aprimorar a legislação referente às atividades desenvolvidas pela Abin para que ela possa ter um adequado suporte ao exercer seu papel previsto na legislação em vigor, primordialmente no que concerne à necessidade de sigilo e segurança na atividade.

Para a consecução deste objetivo, verificou-se a necessidade de uma maior articulação intragovernamental na construção de consensos no Executivo, como também na habilidade do GSI/PR junto à Casa Civil para o adequado encaminhamento de novas propostas ao Congresso, considerando-se que, constitucionalmente, a iniciativa é privativa do Presidente da República. No Legislativo, a aprovação de matérias encaminhadas pelo Executivo dependerá de um ambiente favorável nas relações entre os poderes, como também da atuação do líder do Governo na priorização das matérias na pauta legislativa.

A adequação da celeridade do rito legislativo para a apreciação, pelo Congresso, das propostas estratégicas da AI também é uma necessidade imperiosa, visto que alguns projetos não conseguiram tramitar em tempo conveniente.

A análise das proposições selecionadas delimitou um escopo específico para a Atividade de Inteligência de Estado, mas, durante a coleta de dados, também foi identificada a tramitação de matérias correlatas à AI em outros segmentos, principalmente nas Forças Armadas e na Segurança Pública, o que requer estudos futuros.

Dentre estas matérias, destacaram-se as propostas que dispõem sobre alterações no estatuto do desarmamento, que teve extensa agenda no Congresso e foi objeto de um plebiscito. Contudo é um tema que ainda requer análise de todas as proposições em tramitação no Congresso e estudos comparados para que seja apurado o impacto destas medidas na atuação da Abin.

Nas propostas identificadas, tampouco foram encontradas proposições sobre uma legislação específica que disponha sobre as exceções para licitações e prestação de contas voltadas para a Atividade de Inteligência de Estado no Brasil, tendo em vista que a proteção do conhecimento é uma medida essencial de soberania contra possíveis ações de interesses contrários. A adoção destas medidas encontra resistência, possivelmente, devido ao histórico de corrupção no governo, o que impõe uma transparência que prejudica a incorporação de um regime de exceção para a AI.

A valorização da Atividade de Inteligência na pauta do Congresso também depende da conscientização da sociedade e dos parlamentares sobre a importância da temática para a segurança nacional.

A resultante final do trâmite no Parlamento dos projetos afetos aos assuntos relacionados à Atividade de Inteligência de Estado dependerá também, de forma significativa, da capacidade de o GSI/PR e a Abin exercerem adequada influência no Congresso Nacional na defesa de seus objetivos, dentro dos mais eficientes modelos de atuação atualmente em voga.

Apesar da relevância para a segurança e a soberania nacional, a priorização no Congresso dos temas afetos à AI somente ocorrerá se for realizado um intenso e eficaz trabalho de assessoria parlamentar, com a consequente disseminação de uma cultura ou consciência sobre os diversos ângulos da atividade, o que contribuirá decisivamente para dinamizar o processo de tomada de decisão e refletirá em uma atuação do Parlamento menos reativa aos fatos midiáticos e mais efetiva na defesa dos interesses nacionais.

Referências

BRASIL. Congresso Nacional. Câmara dos Deputados. **Regimento interno da Câmara dos Deputados** [recurso eletrônico]: aprovado pela Resolução nº 17, de 1989, e alterado até a Resolução nº 20, de 2016. 18. ed. Brasília: Câmara dos Deputados, Edições Câmara, 2017. (Série textos básicos; n. 141 PDF).

_____. **Lei nº 9.883, de 7 de dezembro de 1999.** Institui o Sistema Brasileiro de Inteligência, cria a Agência Brasileira de Inteligência – Abin, e dá outras providências. Disponível em: </www.planalto.gov.br/ccivil_03/Leis/L9883.htm>. Acesso em: 10 fev. 2018.

_____. Presidência da República. **Cronologia de criação dos órgãos de inteligência de estado no Brasil.** Disponível em: <www.Abin.gov.br/institucional/historico>. Acesso em: 10 jun. 2018

_____. Congresso Nacional. **Comissão Mista de Controle das Atividades de Inteligência.** Disponível em:<legis.senado.leg.br/comissoes/comissao;jsessionid=F5E4562C68BCC71628B8 EA625158478C?0&codcol=449>. Acesso em: 8 mar. 2018.

_____. Congresso Nacional. Câmara dos Deputados. ***Relatório Final da Comissão Parlamentar de Inquérito com a finalidade de investigar escutas telefônicas clandestinas/ilegais, conforme denúncia publicada na revista "Veja", edição 2022, nº 33, de 22 de agosto de 2007.*** Disponível em: <www2.camara.leg.br/atividade-legislativa/comissoes/ comissoes-temporarias/parlamentar-de-inquerito/53a-legislatura-encerradas/cpiescut/relatorio-final-aprovado-1>. Acesso em: 16 mar. 2018.

_____. Congresso Nacional. **Regimento Comum do Congresso Nacional** [recurso eletrônico]: Resolução do Congresso Nacional nº 1 de 1970, alterada até o Ato da Mesa do Congresso Nacional nº 1 de 2015, e legislação correlata. 2. ed. Brasília: Câmara dos Deputados, Edições Câmara, 2015. (Série textos básicos; n. 101).

_____. Congresso Nacional. Senado Federal. ***Regimento Interno:*** Resolução nº 93, 1970. Brasília: Senado Federal, 2011.

_____. Congresso Nacional. Senado Federal. **Relatório Final nº 1 de 2014,** *da Comissão Parlamentar de Inquérito destinada a investigar a denúncia de existência de um sistema de espionagem, estruturado pelo governo dos Estados Unidos, com o objetivo de monitorar e-mails, ligações telefônicas, dados digitais, além de outras formas de captar informações privilegiadas ou protegidas pela Constituição Federal.* Disponível em: <legis.senado.leg.br/sdleg-getter/documento?dm=3857843&disposition=inline>. Acesso em:17 mar. 2018.

CEPIK, Marco. **Regime Político e Sistema de Inteligência no Brasil:** Legitimidade e Efetividade como Desafios Institucionais. Rio de Janeiro: DADOS; Revista de Ciências Sociais. V. 48, n. 1, 2005, p. 67 - 113.

GONÇALVES, Joanisval Brito. **Quem Vigia os Vigilantes?** O controle da atividade de inteligência no Brasil e o papel do Poder Legislativo.in: Revista da Informação Legislativa, Brasília, v. 47, n. 187, p. 125-136, julho/set. de 2010. Disponível em: <www2.senado.leg.br/bdsf/handle/id/198697>. Acesso em: 12 fev. 2018.

Anexo I

Lista de siglas

AI – Atividade de Inteligência de Estado

AVS – Aviso, em trâmite no Senado

CD – Câmara dos Deputados

CN – Congresso Nacional

CCAI – Comissão Mista de Controle das Atividades de Inteligência

INC – Indicação da Câmara dos Deputados

MP – Medida Provisória

MSF – Mensagem do Senado Federal

MSG – Mensagem do Congresso Nacional

PDC – Projeto de Decreto Legislativo, em trâmite na Câmara

PDS – Projeto de Decreto Legislativo, em trâmite no Senado

PEC – Proposta de Emenda à Constituição

PET – Petição

PFC – Proposta de Fiscalização da Câmara

PL – Projeto de Lei da Câmara

PLC – Projeto de Lei da Câmara, em trâmite no Senado

PLN – Projeto de Lei do Congresso Nacional

PLS – Projeto de Lei do Senado

PRN – Projeto de Resolução do Congresso Nacional

PRS- Projeto de Resolução do Senado

REQ – Requerimento

SF – Senado Federal

SIN – Sindicância

SOR – Sugestão de emenda ao Orçamento