

Operações de Informação: um estudo sobre o desenvolvimento de doutrina aplicada à prevenção à fraude

Eduardo Amadeu Dutra Moresi
moresi@ucb.br

Universidade Católica de Brasília
QS 07 – Lote – EPCT - 71999-700 – Brasília – DF – Brasil

e

Gilson Libório de Oliveira Mendes
liborio@cgu.gov.br

Controladoria-Geral da União
SAS Quadra 01 - Bloco A – Sala 727 – 70070-905 - Brasília - DF - Brasil

RESUMO

O conceito de Operações de Informação (InfOp), no contexto militar, descreve a importância da informação e como ganhar a guerra de informação nas operações militares no século XXI. Identifica a informação como uma condicionante essencial do poder militar nos âmbitos estratégico, operacional e tático. O conceito integra três componentes fundamentais: informações e inteligência relevantes; sistemas de informações eficazes; e uma combinação de operações de influência e baseadas em efeito no processo decisório adversário. O objetivo é planejar a obtenção de informação relevante, por meio do uso de inteligência de fontes abertas, para emprego na atividade de comunicação social visando alcance de objetivos previamente definidos. Em consequência busca-se o domínio da informação, ou seja, obter um grau de superioridade informacional que permita a uma organização alcançar vantagem em uma disputa, ou controlar uma situação, negando, ao mesmo tempo, esses meios ao seu adversário. No âmbito empresarial, público e privado, poucos estudos foram realizados no sentido de apropriar conceitos doutrinários de Operações de Informação para emprego em Gestão Estratégica. Este é o foco do projeto de pesquisa, financiado pelo UNODC e em parceria com a CGU, que estuda a aplicação de conceitos de InfOp para a prevenção à fraude e à corrupção.

Palavras-chave: Operações de Informação, Prevenção à fraude, Inteligência de Fontes Abertas.

1. INTRODUÇÃO

A Controladoria-Geral da União (CGU) é o órgão do Governo Federal responsável por assistir direta e imediatamente ao Presidente da República do Brasil quanto aos assuntos que, no âmbito do Poder Executivo, sejam relativos à defesa do patrimônio público e ao incremento da transparência da gestão, por meio das atividades de controle interno, ouvidoria, auditoria pública, correição, combate e prevenção à corrupção. A CGU também deve exercer, como órgão central, a supervisão técnica dos órgãos que compõem o Sistema de Controle Interno e o Sistema de Correição e das unidades de ouvidoria do Poder

Executivo Federal, prestando a orientação normativa necessária [7].

O desafio de zelar pela boa aplicação do dinheiro público, pelo comportamento ético, legal e transparente dos gestores e o esforço em prevenir e combater à corrupção impõem à CGU, atuar, dentre outras competências, na fiscalização e detecção de possíveis fraudes com relação ao uso do dinheiro público federal, idealizando soluções com o intuito de prevenir novos acontecimentos.

O tema “prevenção e combate à corrupção” está diretamente relacionado ao exercício da cidadania e do controle social. As atividades exercidas pelos órgãos estatais de controle, a exemplo da CGU, são indispensáveis para o combate à corrupção. Portanto, devido à impossibilidade da presença sistemática e permanente dos órgãos institucionais em todas as frentes, a maximização do controle por parte destes órgãos passa a ser de fundamental importância.

É de se destacar também a crescente demanda da sociedade civil pela maior capacidade do Governo em aumentar a eficiência da máquina pública, estancar danos ao patrimônio do Estado advindos da má gestão das despesas. Capitalizadas pela mídia independente, essas demandas exigem respostas céleres, de forma a prevenir novos casos e aumentar a confiança da sociedade no poder público.

O fenômeno da sociedade da informação acarreta para o Estado Brasileiro um aumento de complexidade na fiscalização da gestão dos recursos públicos, dados a dimensão continental do Brasil e a forma descentralizada de execução dos programas governamentais. Muito embora o Governo detenha todos os dados de suas receitas e despesas, a complexidade, a dispersão das informações em diversos sistemas, das mais variadas plataformas tecnológicas e, o volume de informações resultantes da atuação dos gestores públicos, tornam a extração de informação e processamento de conhecimentos úteis, uma tarefa extremamente complicada se executada com meios tradicionais de investigação e auditoria.

Assim, o objetivo desse trabalho é apresentar um arcabouço conceitual que caracteriza a fraude e a corrupção como fenômenos complexos. Em seguida, desenvolve-se o referencial conceitual que fundamenta a aplicação de operações de informação na prevenção à fraude e à corrupção. Por fim,

apresenta-se o projeto de pesquisa focado em operações de informação.

2. FRAUDE – UM FENÔMENO COMPLEXO

Num sentido amplo, uma fraude é um esquema criado para obter ganhos pessoais, apesar de ter, juridicamente, outros significados legais mais específicos, que não são o foco da presente abordagem. Eisele [11] afirma que fraude é o ardil utilizado pelo sujeito no sentido de simular a ocorrência de um fato inexistente, ou ocultar a existência de um fato efetivamente ocorrido.

Uma fraude é qualquer crime ou ato ilegal para lucro daquele que se utiliza de algum logro ou ilusão praticada na vítima como seu método principal. Em Direito Penal [6], fraude é o crime ou ofensa de deliberadamente enganar outros com o propósito de prejudicá-los, usualmente para obter propriedade ou serviços dele ou dela injustamente. O Código Penal Brasileiro, em seu Capítulo VI, define estelionato e os diversos tipos de fraudes.

As Normas Internacionais de Auditoria [13] definem fraude como quaisquer atos ilegais caracterizados por engano, dissimulação ou violação da verdade. Estes atos não dependem da aplicação de ameaça de violência ou força física. Os erros por fraudes ou intencionais podem ser cometidos para: subtrair mercadorias, matérias-primas, produtos e resíduos; subtrair dinheiro; subtrair títulos; iludir o fisco, evitando o pagamento de impostos; dissimular atos sujeitos a penalidades; encobrir faltas de terceiros; alterar resultados para usufruir maiores percentagens em lucros; simular ocorrências; iludir a opinião de acionistas e autoridades monetárias etc [16].

As fraudes podem ser cometidas através de muitos métodos, incluindo fraude de correspondência, por meios de Tecnologia de Informações, fraude por telefone e fraude por internet. Atos que podem ser caracterizados como fraude criminal incluem:

- propaganda enganosa;
- roubo de identidade;
- falsificação de documentos ou assinaturas;
- apropriação de propriedade de outros sob custódia através da violação de confiança;
- fraude da saúde, vendendo produtos inócuos, como remédios falsos;
- criação de empresas falsas;
- insolvência de instituições bancárias e de seguro.

No setor público, as fraudes podem ser facilmente equiparadas, conceitualmente, com as fraudes internas nas grandes empresas. Em ambas são fatores recorrentes, determinantes e fundamentais a existência de oportunidades, a corrupção e o conflito de interesses. Por esta razão muitos dos métodos aplicados no combate às fraudes internas também servem, ou melhor serviriam se fossem aplicados, para o combate às fraudes no setor público [8].

Porém, existem algumas características peculiares do setor público e, sobretudo, algumas medidas de combate à fraudes, e conseqüentemente à corrupção e conflitos de interesses, que são especialmente aplicáveis ao setor público. Uma destas é a transparência na administração e a divulgação e acesso público as informações. Pereira (2010) afirma que cada vez mais a sociedade tem consciência de que as distorções e as fraudes ocorridas no setor público não são responsabilidades somente dos gestores públicos. Busca-se sempre punir os criminosos, os corruptos, mas o movimento por parte da sociedade, de denúncia e combate à corrupção, além disso, deve buscar mecanismos

efetivos, como uma legislação onde estejam tipificados crimes e sanções para aqueles que não cumprirem com deveres como ética, transparência, economicidade e celeridade durante os processos licitatórios.

O Código Penal (1940), em seu Título XI, define os crimes contra a Administração Pública: peculato (Art. 312); extravio, sonegação ou inutilização de livro ou documento (Art. 314); emprego irregular de verbas ou rendas públicas (Art. 315); concussão (Art. 319); corrupção passiva (Art.317); facilitação de contrabando ou descaminho (Art. 318); prevaricação (Art. 319); condescendência criminosa (Art. 320); advocacia administrativa (Art. 321); exploração de prestígio (Art. 332); corrupção ativa (Art. 333); etc.

Apesar não serem termos sinônimos, fraude e corrupção têm um espaço conceitual comum. A fraude busca a obtenção de vantagem por meio de atos ilegais, praticados por pessoas, grupos ou empresas. A corrupção é o comportamento daquele que se desvia das obrigações formais do cargo público (eletivo ou por indicação) por causa de vantagens pessoais, ganhos de riqueza ou de status [3]. Corrupção baseia-se no ato de corromper com a ética de algo, degradar a sociedade, violar com os direitos e deveres de todos.

Por outro lado, complexidade pode ser definida como aquela propriedade de uma expressão de linguagem que a torna difícil para formular seu comportamento global, mesmo quando obtida quase a informação completa sobre seus micro componentes e seus inter-relacionamentos [10].

Outra possibilidade é definir complexidade por meio da relação entre um sistema e um observador. O observador tem sempre a conotação de algum sistema vivo (uma pessoa) ou sistema composto por sistemas vivos (uma organização), não há referências à colocação de algum sistema artificial na posição de observador. Segundo Klir e Folger [14], qualquer descrição deve considerar dois princípios gerais de complexidade de sistemas:

- primeiro princípio geral de complexidade: uma medida de complexidade de um sistema deve ser proporcional à quantidade de informação necessária para descrever o sistema - por exemplo número de entidades (variáveis, estados, componentes);
- segundo princípio geral de complexidade: uma medida de complexidade de um sistema deve ser proporcional à quantidade de informação necessária para resolver qualquer incerteza associada ao sistema.

A idéia central da ciência em geral é que em um sistema complexo - seja uma simulação de computador, um ecossistema ou uma organização - os agentes interagem em modos simples mas freqüentes, afetando mutuamente um ao outro, para criar padrões de comportamento elaborados e inesperados, um fenômeno conhecido como emergência [9]. Então, a teoria da complexidade mantém o foco na natureza de interações entre agentes individuais em um sistema dinâmico complexo e monitora os seus efeitos. O importante é a resposta do sistema às mudanças externas.

A lição mais importante da teoria da complexidade é que sistemas complexos dinâmicos geram ordem criativa e se adaptam a mudanças em seus ambientes, por interações simples entre os seus agentes, e que pequenas mudanças podem conduzir freqüentemente a grandes efeitos. A ordem não é imposta por planejamento de cima para baixo, ela emerge de baixo para cima [15].

Nesse contexto, pode-se afirmar que fraude e corrupção são fenômenos complexos. A idéia de complexidade é a única que

torna possível tratar fenômenos como fraude e corrupção. À medida que os órgãos de fiscalização aprimoram seus mecanismos de combate à corrupção e de prevenção à fraude, os fraudadores e corruptos desenvolvem novos golpes. A complexidade impõe a observação de novos princípios para descrever a realidade. A perturbação da ordem vigente faz com que os atores busquem condições ideais de atuação, gerando um novo equilíbrio dinâmico.

3. OPERAÇÕES DE INFORMAÇÃO

A era da Internet, da globalização e do trabalho centrado em rede, impõe à atividade humana a tendência de se inserir mais em espaços do que em locais físicos, onde a informação e o conhecimento se difundem e se dispersam, ainda que associado a pessoas, processos e tecnologias. Essa nova realidade modificou drasticamente a delimitação de tempo e espaço da informação. A importância do instrumental da tecnologia da informação forneceu a infra-estrutura para modificações, sem retorno, das relações da informação com seus usuários. As transformações associadas à interatividade e à interconectividade no relacionamento dos receptores com a informação, mostram como tempo e espaço modificam as relações com o receptor [4]:

- interatividade ou inter-atuação multitemporal representa a possibilidade de acesso em tempo real, o que representa o tempo de acesso no entorno de zero, pelo usuário à diferentes fontes de informação; possibilita o acesso em múltiplas formas de interação entre o usuário e a própria estrutura da informação contida neste espaço. A interatividade modifica o fluxo: usuário - tempo - informação. Reposiciona os acervos de informação, o acesso à informação e a sua distribuição;
- inteconectividade reposiciona a relação usuário - espaço - informação; opera uma mudança estrutural no fluxo de informação que se torna multiorientado. O usuário passa a ser o seu próprio mediador na escolha de informação, o determinador de suas necessidades. Passa a ser o julgador da relevância da informação que procura e do estoque que o contém em tempo real, tempo igual a zero, como se estivesse colocado virtualmente dentro do sistema de armazenamento e recuperação da informação.

Todavia, as mudanças tecnológicas que tiveram lugar nas últimas décadas deram um lugar de destaque à utilização da informação no cotidiano das pessoas e das organizações. A informação passou a ser um elemento fundamental à vida das organizações sendo importante refletir sobre a sua importância, quanto aos diversos aspectos e setores que influencia.

Para compreender melhor toda essa mudança, pode-se reduzir essa nova realidade a três mundos: o mundo subjetivo dos sistemas cerebrais, o mundo objetivo dos sistemas materiais e o mundo dos sistemas simbólicos cibernéticos e informatizados. A realidade subjetiva dos conteúdos de informação, da sua geração e assimilação, a realidade objetiva dos seus equipamentos e seus instrumentos, e a realidade do ciberespaço, de tempo zero, da existência pela não presença, da realidade virtual. A figura 1 apresenta uma ilustração da intersecção desses três mundos e o Quadro 1 as respectivas descrições.

No relacionamento com uma estrutura de suporte da informação, um receptor realiza reflexões e interações, que lhe permitem evocar conceitos relacionados explicitamente com a informação recebida [5]. O receptor mostra aspectos de um pensamento que

é seduzido por condições quase ocultas, silenciosas, de um meditar próprio de sua privacidade ambientada no:

- contexto da informação;
- contexto particular do sujeito, no tempo e no espaço de interação com a informação;
- estoque de informação do sujeito;
- competência simbólica do receptor em relação ao sub-código lingüístico na qual a informação se insere;
- contexto físico e cultural do sujeito que interpreta a informação.



Figura 1 – Os três mundos da informação [4].

Nesse sentido, cabe esclarecer que as operações de informação ocorrem em uma nova dimensão – a virtual. A interatividade e a interconectividade estabelecem um novo ambiente em que as informações podem ser empregadas para influenciar, atacar ou defender pessoas, grupos ou organizações. Da mesma forma, os três mundos da informação permitem entender como esses novos tipos de relações se estabelecem entre pessoas, infra-estrutura tecnológica e aplicativos.

Outro aspecto a considerar é a realidade de uma organização, que consiste em três domínios principais [2]:

- o físico inclui os ambientes geral, que compreende os fatores políticos, sociais, demográficos, tecnológicos, legais, econômicas, e culturais, e tarefa, que compreende os concorrentes, clientes, fornecedores, e entidades reguladoras;
- o cognitivo que compreende a consciência individual e coletiva que existe nas mentes das pessoas;
- da informação que existe tanto no domínio físico quanto no cognitivo, incluindo a criação, a manipulação, a armazenagem e o compartilhamento de dados e informações.

Portanto, o domínio do espaço virtual pode ser caracterizado pelo uso da tecnologia da informação para armazenar, modificar e intercambiar dados e informações por intermédio de sistemas de redes e infra-estrutura física [12]. O espaço virtual consiste em elementos dos domínios físico (infra-estrutura de tecnologia da informação), cognitivo (a “mente” de qualquer sistema automático de tomada de decisão) e da informação (os dados e informações confinados à arquitetura física do ciberespaço).

A doutrina de Operações de Informação (InfOp) envolve o desenvolvimento de ações planejadas e executadas para afetar as informações e os sistemas de informação adversários e para defender os próprios sistemas de informação. Por conseguinte, uma estratégia de InfOp coerente, integrada à atuação de uma organização, é essencial para lidar com cenários adversos e incertos.

Quadro 1 – Descrição dos espaços dos três mundos da informação [4].

Identificador	Mundos da Informação	Exemplos
A	Espaço da Realidade Subjetiva	espaço das construções teóricas, dos conteúdos, dos processos de geração, interpretação e apropriação da informação.
B	Espaço da Realidade dos Objetos	espaço dos artefatos dos sistemas, dos computadores e das comunicações.
C	Espaço da Realidade do Ciberespaço	espaço dos símbolos cibernéticos, da interação ente os indivíduos e as máquinas.
1	Espaço de Interseção das realidades subjetivas e dos objetos	espaço das tecnologias de informação e comunicação, dos estoques de conteúdos e das redes.
2	Espaço de interseção das realidades subjetivas e do ciberespaço	espaço das construções dos agentes inteligentes para interação do homem com a máquina - os softwares.
3	Espaço de interseção das realidades dos objetos e do ciberespaço	espaço dos processos das comunicações e das redes interativas.
N	Espaço de interseção das realidades subjetivas, dos objetos e do ciberespaço	espaço das atividades de interatividade da interconectividade, da inteligência artificial, da realidade virtual e dos novos desenvolvimentos.

No âmbito militar, InfOp descrevem uma ação institucional dos Estados Unidos para desenvolver um conjunto de abordagens doutrinárias para as suas forças militares e diplomáticas visando a utilização e a operacionalização do poder da informação [1]. O alvo das InfOp é o tomador de decisão adversário e, portanto, o esforço principal será em coagir essa pessoa a realizar ou não uma determinada ação.

Alguns aspectos doutrinários, publicados nos manuais militares do Exército dos Estados Unidos da América FM 100-6 [17] e FM 3-13 [18], podem ser interpretados e aplicados no contexto organizacional. Os principais conceitos são:

- o emprego de InfOp permite que a organização aperfeiçoe a sua capacidade de controlar as informações disponíveis e relevantes (essenciais); proteger sua habilidade de avaliar, processar, integrar, decidir e agir, com relação àquela informação; e atacar a habilidade de seu adversário em potencial de avaliar, processar, integrar, decidir e agir, também em relação à mesma informação;
- o conceito de InfOp integra três componentes fundamentais: informações e inteligência relevantes; sistemas de informações eficazes; e uma combinação de operações de influência e baseadas em efeito no processo decisório adversário;
- o ambiente de informação global é definido como todos os indivíduos, organizações ou sistemas, que coletam, processam e disseminam informação para públicos nacionais e internacionais;

- o ambiente de informação organizacional, como um ambiente dentro do ambiente de informação global, compreendendo sistemas de informações e organizações que interagem ou competem em um mesmo segmento, tais como a mídia, instituições acadêmicas, organizações não governamentais (ONGs), empresas, etc;

- domínio da informação é definido como o grau de superioridade das informações que permite ao seu detentor empregar os seus sistemas de informações e seus meios para alcançar uma vantagem operacional em uma disputa, ou controlar uma situação por meio do emprego da informação.

Basicamente, existem três tipos de InfOp [1]:

- as operações de informação defensivas procuram assegurar o acesso permanente e a utilização efetiva da informação e dos sistemas de informação de forma a atingir objetivos planejados previamente;
- as operações de informação ofensivas procuram influenciar a informação e os sistemas de informação adversários, criando obstáculos na consecução de seus objetivos ou em resposta a uma ameaça específica;
- as operações de influência são definidas como operações que visam afetar a percepção e o comportamento de tomadores de decisão, grupos de pessoas ou população em geral.

No âmbito militar, as InfOp são vistas não apenas como um meio de melhorar ou complementar um ataque físico, mas como um meio de substituir a destruição física pela eletrônica [1]. No âmbito organizacional, as InfOp significam o emprego da informação para reforçar a imagem organizacional ou apoiar a ação organizacional de forma sincronizada em ambientes geograficamente distribuídos.

Por exemplo, para empresas que operam com transações on-line, a interrupção do serviço ou a adulteração de conteúdo de seu portal web certamente trará conseqüências materiais e perdas financeiras. Além das perdas financeiras, há o impacto na imagem organizacional, principalmente em sua credibilidade e na segurança das transações.

As InfOp não são vistas como uma nova atividade ou conjunto de atividades, mas, essencialmente, como uma forma sinérgica de coordenação. Destinam-se, fundamentalmente, em combinar a capacidade de inteligência de uma organização - coleta e análise de informações sobre o seu ambiente externo - com novas capacidades, particularmente aquelas relacionadas à comunicação organizacional.

Na visão antiga, a área de inteligência identificava as necessidades de informação, coletava e analisava informações, e disseminava o conhecimento produzido. Na visão mais atual, a área de inteligência deve atuar de forma sinérgica com a área de comunicação organizacional, planejando o emprego da informação no espaço informacional.

4. PROJETO DE PESQUISA

Nesse contexto a Universidade Católica de Brasília (UCB) em parceria com a Controladoria-Geral da União (CGU) delimitou um projeto de pesquisa denominado "Operações de Informação para apoiar a prevenção à fraude". Os recursos de financiamento do projeto são oriundos da Carta Acordo 2009/11/001 firmada entre a UCB e o Escritório Sobre Drogas e Crime (UNODC/Nações Unidas), no âmbito do Projeto de Realização do IV Fórum de Combate à Corrupção e Implementação de Ações Específicas de Combate à Corrupção – AD/BRA/05/S07.

O projeto tem o objetivo geral de propor um arcabouço doutrinário para emprego das Operações de Informação e de Inteligência de Fontes Abertas para apoiar a gestão estratégica da Secretaria de Prevenção à Corrupção e Informações Estratégicas (SPCI) da CGU.

Os objetivos específicos são:

- identificar as principais referências doutrinárias aderentes ao projeto;
- identificar, caracterizar e qualificar as fontes abertas no ciclo de inteligência;
- analisar a aplicação de conceitos doutrinários de operações de informação na prevenção à fraude e à corrupção;
- estudar as alternativas tecnológicas para análise de grandes volumes de dados;
- propor uma solução tecnológica aderente às demandas da CGU;
- propor as bases doutrinárias para a aplicação de Inteligência de Fontes Abertas para a CGU;
- propor as bases doutrinárias para a aplicação de Operações de Informação possibilite a gestão estratégica da informação na CGU.

Para alcançar esses objetivos, foram definidos o ambiente global de informação e a arquitetura do projeto, que estão apresentados, respectivamente, nas figuras 4 e 5. O ambiente de informação visa definir as necessidades doutrinárias, as principais fontes de informação e os grandes temas que orientarão o levantamento de necessidades de inteligência. A arquitetura do projeto divide-se em três camadas:

- infra-estrutura de Tecnologia da Informação – visa desenvolver plataforma tecnológica que permita o processamento de grandes volumes de informação de forma distribuída;
- produção de informação – estudar soluções de software para aplicação na análise de grandes volumes de dados (quantitativos e qualitativos) empregando técnicas de mineração de dados e de textos, coleta e processamento automático de informação e recuperação de informação não estruturada;
- operações de informação – desenvolvimento de doutrina apropriando conceito de Inteligência, Contra-Inteligência e Comunicação Organizacional para aplicação no contexto da prevenção à fraude e corrupção.

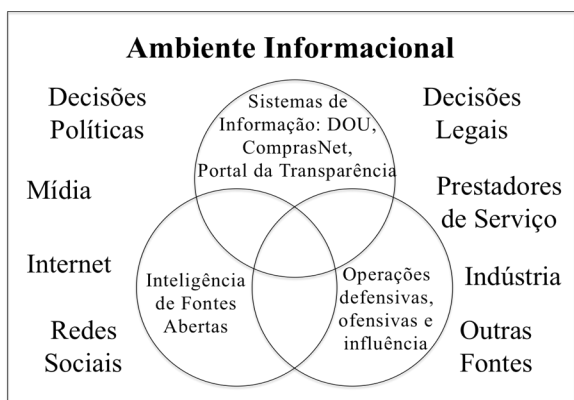


Figura 4 – Ambiente informacional do projeto.

5. CONCLUSÃO

O propósito desse trabalho é apresentar uma nova abordagem de emprego da doutrina de Operações de Informação. Essa doutrina tem origem no domínio militar e foi desenvolvida pelo Exército dos Estados Unidos da América, desde o conflito do Golfo, ocorrido em 1991. O arcabouço doutrinário apresenta outro

ambiente de embates – o informacional, onde a superioridade da informação pode ser decisiva em operações militares.

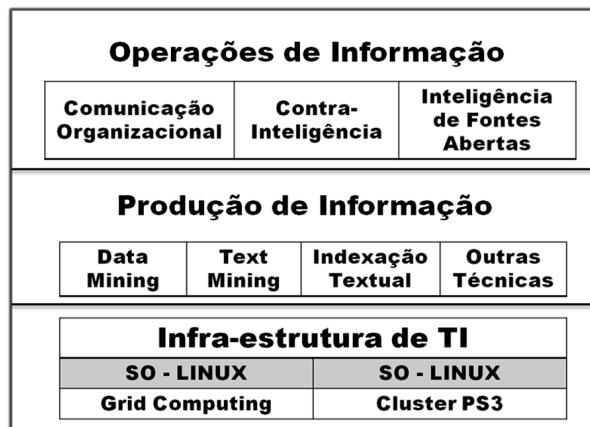


Figura 5 – Arquitetura do Projeto [15].

No âmbito das organizações, a evolução das tecnologias da informação e comunicação impôs uma nova realidade – o espaço virtual. Tanto as organizações públicas quanto as privadas passaram a interagir com essa nova realidade, que se apresenta em três domínios – o físico, o cognitivo e o da informação. Portanto, entender a informação como um novo domínio que pode influenciar pessoas, grupos ou outras organizações é o contexto que de aplicação da doutrina de operações de informação no âmbito não militar.

Além disso, o trabalho contextualizou a fraude e a corrupção como fenômenos complexos, ou seja, mostrou que o seu entendimento passa necessariamente pela assimilação de conceitos e princípios da teoria da complexidade. Enfatizou-se que, à medida que os órgãos de controle aperfeiçoam seus mecanismos de prevenção à fraude e combate à corrupção, os fraudadores e corruptos desenvolvem novas técnicas para praticarem os ilícitos, ou seja, estabelece um equilíbrio dinâmico.

Conclui-se, afirmando que o emprego da informação passa a não ser mais exclusividade das operações militares, podendo ser apropriada no domínio das organizações civis. Enxergar a realidade das fontes de informação como atores que realizam operações de informação ofensivas, defensivas e de influência permite interpretar suas mensagens de forma subliminar.

AGRADECIMENTOS

Esse trabalho é financiado pelo Escritório Sobre Drogas e Crime (UNODC/Nações Unidas), sendo executado na Universidade Católica de Brasília (UCB) em parceria com a Controladoria-Geral da União (CGU).

REFERÊNCIAS BIBLIOGRÁFICAS

- [1] P.D. Allen. Information Operations Planning, Boston: Artech House, 2007.
- [2] D.S. Alberts, J.J. Garstka, R.E. Hayes, D.A. Signori, Understanding Information Age Warfare, Washington, DC: CCRP Publication Series, 2001.
- [3] J. Andvig, O. Fieldstad, I. Amudsen, T. Sissener, T. Soreide, Research on Corruption: A Policy Oriented Survey. Bergen,

Norway: Chr. Michelsen Institute and Norwegian Institute of International Affairs, 2000.

- [4] A.A. Barreto, O tempo e o espaço da ciência da informação. Disponível em: <aldoibct.bighost.com.br/tempespa.htm>. Acesso em 25 jul 2010.
- [5] A.A. Barreto, A estrutura do texto e a transferência da informação. DataGramZero - Revista de Ciência da Informação - v.6 n.3 jun/2005.
- [6] Brasil, Código Penal, Decreto-Lei Nº 2.848, de 07 de dezembro de 1940.
- [7] Brasil, A CGU, Disponível em: <www.cgu.gov.br/CGU/>, Acesso em 12/12/2010.
- [8] R.A. Cezar, Corrupção e fraudes no setor público, Disponível em: <www.reflexoes.diarias.nom.br/CIDADANIA/CORRUPCAOEFRAUDESNOSETORPUBLICO.pdf, Acesso em 12 dez 2010.
- [9] G.A. Cowan, Complexity: metaphors, models, and reality, Reading, MA: Addison Wesley, 1994.
- [10] B. Edmonds, Syntactic measures of complexity. PhD thesis submitted to the University of Manchester, 1999.
- [11] A. Eisele, Crimes Contra a Ordem Tributária, 2 ed, São Paulo: Dialética, 2002.
- [12] T.P. Franz, IO Foundations to Cyberspace Operations: Analysis, Implementation Concept, and Way-Ahead for Network Warfare Forces, Master's thesis, US Air Force Institute of Technology, 2007.
- [13] IBRACON, Normas Internacionais de Auditoria, São Paulo: Atlas, 1998.
- [14] G.J. Klir, T.A. Folger, Fuzzy sets, uncertainty and information, New Jersey: Prentice Hall, 1988.
- [15] E.A.D. Moresi, Operações de Informação para apoiar a prevenção à fraude, In: Anais XV Congreso Internacional del CLAD, Republica Dominicana, 2010.
- [16] A.L. Sá, Curso de Auditoria, São Paulo: Atlas, 1998.
- [17] US Army, Field Manual 100-6, Department of the Army - USA, 1996.
- [18] US Army, Field Manual 3-13, Department of the Army - USA, 2003.