CEPIK, Marco. **Espionagem e Democracia: agilidade e transparência como dilemas na institucionalização de serviços de inteligência**. Rio de Janeiro – RJ: editora FGV, 2003

Notas para aula de Inteligência
Prof. Rafael Ávila

Inteligência pode ser obtida por meio de fontes humanas (*humint*), da interceptação de comunicações e de outros sinais eletromagnéticos (*sigint*) e obtida através de imagens (*imint*).

Capítulo 1. Inteligência: dinâmicas operacionais

"Intelligence is concerned with that component of the struggle among nations that deals with information. Intelligence seeks to learn all it can about the world. But intelligence can never forget that the attainment of the truth involver a struggle with human enemy who is fighting back and that truth is not the goal but rather only a means toward victory" (Shulsky: 1992: 197).

Alvos e Objetivos da Inteligência: Política Externa; Defesa Nacional e Segurança Pública.

Inteligência é toda informação coletada, organizada ou analisada para atender as demandas de um tomador de decisões qualquer. (p.27)

Para a ciência da informação, inteligência é uma camada específica de agregação e tratamento analítico em uma pirâmide informacional, formada, na base, por dados brutos e, no vértice, por conhecimentos flexíveis. (p. 27-28)

A definição mais restrita de inteligência é, "a coleta de informações sem o consentimento, a cooperação ou mesmo o conhecimento por parte dos alvos da ação" (p.28). O termo, neste sentido, se assemelha a segredo ou informação secreta. Inteligência se diferencia da mera informação por sua capacidade explicativa e/ou preditiva.

Serviços de inteligência estão voltados para a compreensão de relações adversariais. Por isso, lidam com o estudo do outro e procura elucidar situações nas quais as informações mais relevantes são potencialmente manipuladas ou escondidas, em que há um esforço organizado por parte de um adversário para desinformar, tornar turvo o entendimento e negar conhecimento.

"Quanto mais ostensivas (públicas) as fontes de informação, quanto menos conflitivos os temas e situações, menos as análises de inteligência têm a contribuir para o processo de tomada de decisão governamental" (p. 29-30).

"Guerra Informacional (IW) – o conceito de IW passou a ser empregado para abarcar tanto a obtenção e a negação de informações de combate quanto a inteligência propriamente dita" (p.31-32).

Ciclo de Inteligência: 1. Requerimentos Informacionais; 2. Planejamento; 3. Gerenciamento dos meios técnicos de coleta; 4. Coleta a partir de fontes diversas; 5. Processamento; 6. Análise de

informações obtidas de fontes diversas; 7. Produção de relatórios, informes e estudo; 8. disseminação dos produtos; 9. Consumo pelos usuários; 10. *Feedback*. Deve-se destacar que isso é só uma metáfora sobre o processo de inteligência e que, efetivamente, não é assim que ocorre na prática.

Demanda informacional deriva de requerimentos informacionais segundo prioridades. Daí, parte-se para a coleta e análise. Ou seja, o que vai ser obtido em termos de informação é requisitado por uma agente tomador de decisão (policymakers). Destaca-se que, "na maioria das situações os policymakers não têm tempo nem clareza para especificar os tipos de informações de que necessitam ou irão necessitar para quais processos de tomada de decisão e implementação" (p.33). Neste sentido, e ainda que meio delicado, os serviços de inteligência deveriam antecipar algumas demandas ou preencher lacunas deixadas pela demanda. Por isso, é preciso com que se trabalhe ao mesmo tempo com **Princípios de Iniciativa** [o órgão avalia informações que seriam úteis ao usuário – *pushes*] e **responsividade** [coleta e análise de informações solicitadas diretamente pelos usuários – *pulls*].

Coleta e Processamento

As atividades especializadas de coleta absorvem entre 80 e 90% dos investimentos governamentais na área de inteligência nos países centrais do sistema internacional (p. 35).

1. *Humint* (*human intelligence*) para as informações obtidas a partir de fontes humanas. Existem dois tipos de atores neste processo: os oficiais de inteligência e suas fontes. As fontes podem ser: pessoas comuns que tem "acesso" aos países; informantes *ad hoc* (exilados políticos, de partidos de oposição e etc.); fontes secretas (recrutados ou voluntários, *walk-ins e, por fim os defector-in-place*, aquele oficial de um governo ou líder de uma organização que decide mudar de lado e permanece em suas funções fornecendo informações para seus novos controladores). Os oficiais de inteligência podem operar por "cobertura oficial" ou não (no jargão em inglês, NOCs).

2. *Sigint* (*Signals Intelligence*) para as informações obtidas a partir da interceptação e decodificação de comunicações e sinais eletromagnéticos. Nela se insere a criptografia (uso de códigos e cifras para garantir a inviolabilidade do conteúdo das mensagens) e a criptologia (decifração e/ou decodificação de mensagens interceptadas). Atualmente, a disciplina da inteligência de sinais divide-se em dois campos complementares, chamados de *comint* (*communications intelligence*), obtida através de interceptação, processamento e pré-análise das comunicações de governos, organizações e indivíduos, excetuando-se o monitoramento das transmissões públicas de rádio e televisão, as quais caem na área de *Osint* e; de *elint* (*eletronics intelligence*), obtida através de interceptação, processamento e pré-análise de sinais eletromagnéticos não-comunicacionais, emitidos por equipamentos civis e militares, com exceção das emissões decorrentes de explosões nucleares, as quais caem na área de especialização de *Masint*. "Desde o advento do telégrafo sem fio, do rádio e, principalmente , das comunicações via satélite, a interceptação de sinais eletromagnéticos transmitidos pelo ar tornou fisicamente mais simples a coleta de informações, aumentando para os alvos potenciais a importância da medidas de segurança (comsec) e a necessidade de contramedidas eletrônicas (ECM) no caso dos sistemas militares. Existem atualmente 3 tipos principais de satélites de sigint: satélites para interceptação de sinais eletrônicos não-comunicacionais (ferrets); os satélites de interceptação de comunicações; os satélites de orbitação elíptica (em russo, conhecidos como *Molniya*).

3. *Imint* (*Imagery intelligence*) para as informações obtidas a partir da produção e interpretação de imagens fotográficas e multiespectrais. É uma das áreas mais recentes. Seu desenvolvimento moderno começou com os balões, passando por aviões e câmeras, até se chegar aos satélites no mundo contemporâneo. Ressalta-se que os "riscos diplomático-militares derivados da violação do espaço aéreo de nações soberanas em tempos de paz, e principalmente, a ameaça representada pelo aperfeiçoamento das contramedidas defensivas de detecção e interceptação dos aviões de espionagem levaram a maioria dos países a uma utilização relativamente restrita dos vôos clandestinos de reconhecimento fotográfico" (p.46). Os satélites tornaram-se cruciais. Hoje as imagens são obtidas operando em múltiplas bandas discretas do espectro eletromagnéticos (MSI, ou *multispectral imagery*) ou sensores que operam em bandas espectrais contíguas incluindo luz visível, infravermelho, termo-infravermelho, ultravioleta e ondas de rádio (HSI, ou *hyperspectral imagery*). As limitações do *Imint* são: 1) custos de obtenção; 2) a interpretação de imagens obtidas por satélites, aviões e drones é uma atividade essencialmente humana, que demanda pessoas com habilidades especiais, cuja formação é demorada e artesanal; 3) ainda não se pode ver o que está escondido ou ainda não foi construído.

4. *Masint* (*Measurement and signature intelligence*) para as informações obtidas a partir da mensuração de outros tipos de emanações (sísmicas, térmicas etc.) e da identificação de "assinaturas", ou seja, sinais característicos e individualizados de veículos, plataformas e sistemas de armas. Envolve a coleta e o processamento técnico de imagens hiperespectrais e multiespectrais até a interceptação de sinais de telemetria de mísseis estrangeiros sendo testados, passando pelo monitoramento de fenômenos geofísicos (acústicos, sísmicos e magnéticos), pela medição dos níveis de radiação nuclear na superfície terrestre e no espaço, pelo registro e análise de radiações não-intencionais emitidas por equipamentos eletrônicos e radares e pela coleta e análise físico-química de materiais (efluentes, partículas, resíduos, partes de equipamentos estrangeiros e etc.). 3 tipos de satélites norte-americanos carregam sensores dedicados à coleta de *masint*: a) os satélites do *Defense Support Program* (DSP) [detectam assinaturas espectrais associados a diferentes sistemas de mísseis]; b) os satélites *Navstar Global Positioning System* (GPS) são equipados com sistemas de detecção de explosões nucleares (Nudet); c) satélites metereológicos de uso militar (DMSP) são equipados com sensores para radiação eletromagnética e tracking de fragmentos de explosões nucleares na atmosfera.

5. *Osint* (*Open sources intelligence*) quando a obtenção de informações ocorre exclusivamente a partir de fontes públicas, impressas ou eletrônicas. Consiste na obtenção legal de documentos oficiais sem restrições de segurança, da observação direta e não-clandestina dos aspectos políticos, militares e econômicos da vida interna de outros países ou alvos, do monitoramento da mídia, da aquisição legal de livros e revistas especializadas de caráter técnico-científico, enfim, de um leque mais ou menos amplo de fontes disponíveis cujo acesso é permitido sem restrições especiais de segurança.

Análise e Disseminação

Pode-se dividir os produtos analíticos segundo a função esperada e o foco temporal (presente/passado/futuro). Resultava-se desse critério uma separação entre inteligência sobre fatos correntes (chamada de relatorial), inteligência sobre características básicas e estáveis (chamada descritiva) ou sobre tendências futuras (chamada de inteligência avaliativa ou prospectiva). Um quarto tipo especial seria a inteligência sobre ameaças mais ou menos imediatas, também chamada de alerta (*warning intelligence*). Outra forma de dividir é organizar a atividade de inteligência a partir de seus produtos finais: política; militar; científica e tecnológica; econômica e, mesmo; sociológica.

Em relação aos alvos da operações de inteligência, divide-se em: transnacionais (terrorismo, crime organizado), regionais (UE, Oceania), nacionais (China, Rússia) e subnacionais (grupos militantes armados).

A adaptabilidade das diferentes fontes de inteligência a inferências depende dos problemas analíticos a serem resolvidos (p. 54). Os produtos finais de inteligência vão desde sumários diários/semanais sobre temas correntes até estudos mais aprofundados sobre tendências e problemas delimitados a partir de critérios espaciais ou funcionais (p.55).

Disseminação tende a ser o elo mais sensível do ciclo de inteligência. Em boa parte porque a diversidade de usuários é muito grande, suas necessidades obedecem a ritmos temporais específicos e a situação torna-se mais complexa ainda, porque os próprios analistas de inteligência constituem um tipo de usuário dos coletores.

Segurança de informações (*infosec*) e contra-inteligência

A área de inteligência e a área de segurança exercem funções simétricas e mutuamente dependentes. Do ponto de vista operacional, enquanto a principal missão da área de inteligência é tentar conhecer o "outro", a principal missão da área de *infosec* é garantir que os "outros" só conhecerão o que quisermos que eles conheçam sobre nós mesmos.

A segurança informacional é formada por 3 componentes relativamente autônomos entre si: 1) contramedidas de segurança (SCM), que vão desde programas de classificação de segredos governamentais, armazenamento especial, regras de custódia e transmissão de documentos, restrições físicas de acesso aos prédios e arquivos para pessoas não autorizadas, (...) camadas de segurança eletrônica nas redes de computadores e uso de criptografias; 2) contra-inteligência (CI), que envolve a identificação das operações de coleta de inteligência de um adversário, da detecção e da neutralização dos meios intrusivos de obtenção de informações utilizados por um governo ou organização considerada hostil e; 3) segurança de operações (Opsec), que compreende o conjunto de procedimentos que visam identificar quais as informações sobre equipamentos, operações, capacidades e intenções seriam críticas para um adversário obter e, a partir dessa análise, propor um conjunto de medidas para negar ativamente tais informações ao adversário. Ela envolve medidas passivas e ativas, esta últimas conhecida como *deception operations*.

Embora a contra-inteligência envolva um leque bem mais amplo de atividades do que a contra-espionagem, esta, sim, voltada principalmente para prevenção, detecção, neutralização, repressão ou manipulação/infiltração de atividades hostis de espionagem, é precisamente essa dimensão ativa de contra-espionagem que distingue a contra-inteligência dos demais aspectos da segurança de

informações (*infosec*) e recomenda sua alocação sob responsabilidade dos serviços de inteligência externos e internos de uma país.

Os serviços de inteligência e contra-inteligência têm a responsabilidade de avaliar as ameaças, estudar as operações adversárias, fazer inferências operacionais e sugerir normas e técnicas de proteção que aumentam a segurança informacional das forças amigas.

Operações encobertas

Nos EUA são chamadas de CA (*covert actions*), na URSS eram chamadas de medidas ativas (*aktivnye meropriiatiia*) e na Inglaterra tem a alcunha de ações políticas especiais (*special political actions*).

Operações encobertas são utilizadas por um governo ou organização para tentar influenciar sistematicamente o comportamento de outro governo ou organização através da manipulação de aspectos econômicos, sociais e políticos relevantes para aquele ator, numa direção favorável aos interesses e valores da organização ou governo que patrocina a operação. Uma das características dessas operações é a negação de autoria (*plausible deniability*).

Quatro tipos de operações encobertas podem ser destacados: 1) aquele que envolve apoio a grupos já existente (ou de financiamento e a organização de grupos) para a condução de guerra subterrânea, operações paramilitares, guerrilhas, campanhas de contra-insurgência ou terrorismo. O envolvimento de um governo, nesses casos, pode variar desde o suporte financeiro e o fornecimento de armas até um engajamento mais direto em logística, treinamento, inteligência e etc; 2) aquele que envolve os chamados *wet affairs*, desde o apoio a golpes de Estado e tentativas de assassinatos de líderes das forças adversárias (ou de governantes) até incursões militares irregulares numa fronteira, sabotagem e perpetração de atos terroristas isolados; 3) aquele que envolve operações de sabotagem econômica e política contra forças adversárias ou, por outro lado, o fornecimento de assistência secreta a governos e forças aliadas; 4) aquele que abarca um conjunto de medidas para tentar influenciar as percepções de um governo ou mesmo de uma sociedade como um todo através de agentes de influência, desinformação, falsificação de dinheiro ou documentos, além dos vários tipos mais ou menos encobertos de propaganda.

A função da Inteligência

Seriam oito utilidades principais: 1) contribuir para tornar o processo decisório governamental nas áreas relevantes de envolvimento (PEX, defesa nacional e ordem pública) mais racional e realista; 2) que o processo interativo entre policymakers e oficiais de inteligência produzisse efeitos cumulativos de médio prazo, aumentando o nível de especialização dos tomadores de decisão e de suas organizações; 3) que a inteligência pudesse apoiar o diretamente o planejamento de capacidades defensivas e o desenvolvimento e/ou aquisição de sistemas de armas, de acordo com o monitoramento das sucessivas inovações e dinâmicas tecnológicas dos adversários; 4)que apoiasse diretamente as negociações diplomáticas em várias áreas; 5) que a inteligência fosse capaz de subsidiar o planejamento militar e a elaboração de planos de guerra; 6) que a inteligência pudesse alertar os responsáveis civis e militares contra ataques surpresa, surpresas diplomáticas e graves crises políticas internas que podem nunca ocorrer, mas para as quais os governantes preferem "assegurar-se" ao invés de arriscar; 7) deveriam monitorar os alvos e ambientes externos prioritários

para reduzir incerteza e aumentar o conhecimento e a confiança, especialmente no caso de implementação de tratados e acordos internacionais sem mecanismos de inspeção in loco; 8) serviriam para preservar o segredo sobre as necessidades informacionais, as fontes, métodos e fluxos e técnicas de Intel diante da existência de adversários interessados em obter tais coisas (p. 65).

Capítulo 2 Inteligência: perfil organizacional

Sistemas governamentais de inteligência consistem em organizações permanentes e atividades especializadas em coleta, análise e disseminação de informações sobre problemas e alvos relevantes para a política externa, defesa nacional e garantia da ordem pública de um país (p.85). São órgãos do Poder Executivo que desempenham atividades ofensivas e defensivas na área de informações.

O estado moderno e a função de inteligência

A criação dos serviços secretos (mais tarde conhecidos como serviços de inteligência) foi uma das respostas às necessidades mais gerais dos governantes em termos de redução dos custos de transação associado à obtenção de informações (p.88). os serviços de inteligência modernos teriam surgido com um dupla face, informacional e coercitiva a um só tempo (p. 89). A trajetória moderna dos serviços de inteligência é marcada por grandes descontinuidades entre os primeiros serviços secretos surgidos no contexto do absolutismo e as inúmeras organizações que configuram atualmente os sistemas nacionais de inteligência e segurança.

Origens: diplomacia, guerra e policiamento

Diplomacia e inteligência externa

Os serviços de inteligência exterior são “clássicos”, pois têm como característica comum o fato de serem os principais responsáveis pela espionagem propriamente dita e também pela coleta de informações a partir de fontes ostensivas fora do território nacional.

Guerra e inteligência de defesa

Em comparação com a linha evolutiva derivada da diplomacia secreta dos séculos XVI e XVIII, pode-se dizer que a inteligência militar acrescenta à conspiração e à espionagem uma nova dimensão, a de coleta sistemática de informações básicas e menos perecíveis, seguida pela análise dos fatos e idéias novas, tendo como pano de fundo aqueles acervos informacionais, redundando na apresentação de relatórios de inteligência orientados para tornar mais racionais e “informadas” as decisões de comando (p.96).

Policiamento e inteligência de segurança

Esta se distingue das duas anteriores por sua ênfase nas chamadas ameaças internas à ordem existente. São derivadas de forças especializadas em manutenção da ordem interna, que desenvolveram técnicas e recursos de vigilância, infiltração, recrutamento de informações e interceptação de mensagens para a repressão política dos grupos considerados subversivos (p.99)

Organização de Sistemas Nacionais de Inteligência

Desenho organizacional envolve: 1. alguma instância central de coordenação; 2. uma ou mais agências de coleta de informação (normalmente imagens e sinais estão separados de *humint* e fontes ostensivas); 4. alguma instância central de análise; 5. unidades departamentais de análise com laços mais ou menos definidos com as organizações centrais de coleta de inteligência; 6. poderosos subsistemas de inteligência de defesa e de segurança; 7. algum órgão de formação e treinamento e; 8. órgãos mais ou menos colegiados para coordenação e instâncias de supervisão externa.

3 tipos básicos de sistemas nacionais de inteligência: a) anglo-saxão, caracterizado pela alta centralização de autoridade sobre as unidades do sistema, alto grau de interação analítica; b) modelo europeu continental, caracterizado por média centralização da autoridade sobre as unidades do sistema, média integração analítica dos produtos da Intel, alto envolvimento da atividade de inteligência com as instâncias de *policymaking*; c) um modelo asiático, caracterizado por baixa centralização da autoridade sobre as unidades do sistema, alta integração analítica dos produtos de Intel, médio envolvimento da atividade de inteligência com as instâncias de *policymaking*.

Na literatura a divisão é: modelo descentralizado com supervisão congressual (EUA) e modelo centralizado sem controle público (URSS).

Capítulo 3 Segurança Nacional, segredo e controle

Segurança seria então "uma condição relativa de proteção na qual se é capaz de neutralizar ameaças discerníveis contra a existência de alguém ou de alguma coisa com razoável expectativa de sucesso. Em termos organizacionais, segurança é obtida através de padrões e medidas de proteção para conjuntos definidos de informações, sistemas, instalações, comunicações, pessoal, equipamentos ou operações" (p.138).

Considerações Finais

Em 1999 foi aprovada pelo congresso a lei que criava a Agência Brasileira de Inteligência (ABIN) e o Sistema Brasileiro de Inteligência (Sisbin).

Lei no. 9.883/99, art. 1º. Parágrafo 2º. A atividade de inteligência visa 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". Segundo Cepik (p.207) esta definição é muito vaga. "Ela implica, no limite, a idéia absurda de que a inteligência está legalmente encarregada do provimento da onisciência para o governo brasileiro".