

# **Espionagem e democracia**



MARCO A.C. CEPÍK

# Espionagem e democracia



ISBN — 85-225-0437-7

Copyright © Marco A. C. Cepic

Direitos desta edição reservados à  
EDITORAS FGV

Praia de Botafogo, 190 — 14º andar  
22253-900 — Rio de Janeiro, RJ — Brasil  
Tels.: 0800-21-7777 — 0-XX-21-2559-5543  
Fax: 0-XX-21-2559-5532  
e-mail: editora@fgv.br  
web site: www.editora.fgv.br

Impresso no Brasil / Printed in Brazil

Todos os direitos reservados. A reprodução não autorizada desta publicação, no todo ou em parte, constitui violação do copyright (Lei nº 5.988)

1ª edição — 2003

*Revisão de originais:* Renato Barraca

*Editoração eletrônica:* Cristiana Ribas

*Revisão:* Fatima Caroni e Marco Antônio Corrêa

*Capa:* Studio Creamcrackers

Ficha catalográfica elaborada pela Biblioteca  
Mario Henrique Simonsen/FGV

Cepik, Marco

Espionagem e democracia: agilidade e transparéncia como dilemas na institucionalização de serviços de inteligência / Marco A. C. Cepik.  
— Rio de Janeiro : Editora FGV, 2003.  
232p.

Versão revisada de parte da tese do autor (doutorado — IUPERJ),  
aprovada em 2001 com o título: Serviços de inteligência: agilidade e  
transparéncia como dilema de institucionalização.

Inclui bibliografia.

1. Serviço de inteligência. 2. Segurança nacional. I. Fundação Getúlio Vargas. II. Título.

CDD – 355.45

# **Sumário**

<b>Agradecimentos</b>	<b>7</b>
<b>Prefácio</b>	<b>9</b>
<b>Introdução</b>	<b>13</b>
<b>Capítulo 1</b>	<b>27</b>
<b>Inteligência: dinâmicas operacionais</b>	
O que é inteligência?	27
O ciclo da inteligência	32
Segurança de informações e contra-inteligência	56
Operações encobertas	61
A função da inteligência	64
<b>Capítulo 2</b>	<b>85</b>
<b>Inteligência: perfil organizacional</b>	
O Estado moderno e a função de inteligência	86
Origens: diplomacia, guerra e policiamento	91
Lógica de expansão dos sistemas de inteligência	102
Organização dos sistemas nacionais de inteligência	111
A agilidade como dilema	119
<b>Capítulo 3</b>	<b>137</b>
<b>Segurança nacional, segredo e controle</b>	
Segurança nacional	138
Segredo governamental	151
Controle externo	158
A transparência como um desafio	186
<b>Considerações finais</b>	<b>207</b>
<b>Referências bibliográficas</b>	<b>213</b>



## Agradecimentos

Este livro é uma versão revisada de parte de minha tese de doutorado em ciência política, aprovada no Iuperj em 2001. Repito aqui os agradecimentos que eu já fiz na própria tese, acrescentando meu reconhecimento pelo trabalho de Maria Celina D'Araujo, do Cpdoc, e de Cristina Mary Paes da Cunha, coordenadora editorial da Editora FGV.

Fiz a tese e este livro, barcos de papel, para a Eliane e para os nossos filhos, Hannah e Arthur, como parte de nossa travessia. Só o fiz porque os três me ensinaram que a alegria é o justo, e diz a lenda que teses concluídas tornam a vida mais alegre. Junto com eles, Otto, Janisse, Olga, Carla, Ana Paula, Brune, Fabiano, Matheus e Thiago foram acrescentando valores e significados a uma vida errante (milonga de oito cidades até agora) e que seria, sem eles, errada. Meus agradecimentos também para Rosalva Machado e a família de Belo Horizonte. Além da família, quem no Brasil poderia honestamente esquecer os amigos, espalhados pelo mundo e conectados, mais pela vida do que pela internet. Cada um pode ter certeza de que não me esqueci.

No Rio de Janeiro, meu profundo agradecimento a Maria Regina S. Lima, minha orientadora no Iuperj, e para Domício Proença Jr., co-orientador e coordenador do Grupo de Estudos Estratégicos (GEE) da Coppe/UFRJ. Nos Estados Unidos, pude contar com o apoio e o diálogo crítico mantidos com Edward Platt, meu supervisor quando fui *visiting scholar* no Departamento de Ciência Política da Indiana University of Pennsylvania (IUP), em 1997-98. Por sua vez, Thomaz Guedes da Costa acompanhou esta pesquisa desde o início e me confiou seu apoio em momentos decisivos. Também gostaria de agradecer o diálogo constante mantido com Russell Swenson e com Thomas Bruneau, bem como os comentários de Margaret Hayes e de Bruce Berkowitz. Na Grã-Bretanha, tenho uma dívida imensa com Michael Herman (Oxford), e gostaria também de agradecer aos professores Peter Gill (Liverpool John Moores University), Andrew Hurrell (Oxford) e Charles Jones (Cambridge).

Na América Latina, gostaria de agradecer os comentários e diálogos mantidos sobre esses temas ao longo dos últimos anos com vários pesquisadores, em especial com Adrián Bonilla (Equador), Elsa Llenderrozas, Mariano

Bartolomé e José Manuel Ugarte (Argentina), Manuel Gallardo, Carlos Gutiérrez e Guillermo Holzmann (Chile) e Ana Tager (Guatemala).

Ao longo dos anos, ensinaram-me muito, e sou especialmente grato a Antonio Mitre, Bruno Lazzarotti, Bruno Reis, Carla Ferreira, Carlos Aurélio Faria, Carlos Ranulfo F. Melo, Edgar Pontes de Magalhães, Elisa Reis, Eugênia Bossi, Eugênio Diniz, Fábio Wanderley Reis, Francisco Gaetani, Gustavo Torres, José Luiz Ratton Jr., José Miguel Martins, José Eisenberg, Juliana Bemfica, Luiz Cláudio Barros, Luiz Dulci, Mauro Mosqueira, Paulo Vizentini, Otávio Dulci, Priscila Antunes, Renato Lessa, Rômulo Paes de Sousa, Salvador Raza, Sigrid Frahia (*in memoriam*) e Vera Alice Cardoso.

As boas condições de trabalho e o estímulo intelectual que permitiram a realização deste e de outros textos eu devo ainda aos colegas do Departamento de Ciência Política da UFMG, aos meus alunos e orientandos, aos colegas e professores do Iuperj, aos pesquisadores e gestores da Fundação João Pinheiro-MG, aos colegas e diretores da Prodabel, bem como ao CNPq e à Capes.

Na verdade, para cada pessoa eu teria muitas palavras de agradecimento e poderia relembrar muitos momentos. Mas já é hora de passar ao texto e seguir adiante, assumindo as responsabilidades de praxe e isentando a todos pelos equívocos e defeitos deste livro.

## Prefácio

Os temas relativos às instituições, políticas governamentais e organizações na área de segurança nacional não têm despertado o mesmo interesse analítico nos cientistas sociais, pelo menos no caso do Brasil, que outras questões sociais e políticas. As razões são várias, mas estão associadas ao contexto pregresso recente de autoritarismo militar e ao otimismo liberal que costuma grassar em situações de mudança, como aquela representada pelo fim dos regimes de exceção, de que poderíamos também eliminar essas instituições de nossas estruturas políticas. A consequência da baixa popularidade desses temas é que estes são deixados a seus operadores ou simpatizantes, resultando em análises no mais das vezes superficiais e enviesadas.

O livro de Marco Cepik não corre nenhum desses riscos. Trata-se de um estudo muito competente, apoiado em bibliografia internacional, e que enfrenta com argúcia analítica os problemas e as tensões envolvidas na convivência, nem sempre harmoniosa, entre o aparato estatal e suas demandas de segurança e informação, e as instituições e processos políticos próprios a um contexto democrático. Escrito originariamente como parte de sua tese de doutorado, o livro tem no binômio agilidade e transparência o eixo de sua argumentação. A relação entre os dois termos é tratada como permeada de tensão, mas não redutível a um de seus pólos. O argumento do autor afasta-se quer de uma demanda tecnocrática, que sacrificaria a transparência e o controle democrático pela eficiência dos serviços de inteligência, quer da defesa de teses ultraliberais que simplesmente proporiaiam a eliminação dos últimos e do próprio Estado, sem oferecer uma alternativa institucional à questão de como lidar com as ameaças à segurança de uma comunidade política qualquer.

Na verdade, como argumenta Cepik, os problemas de agilidade são inerentes à própria natureza das atividades dos serviços de inteligência, em função da contradição potencial entre a demanda por aumento das informações disponíveis sobre determinado assunto e/ou indivíduo e a simultânea necessidade de protegê-las da indiscrição alheia. Da mesma forma, são notórias as dificuldades envolvidas no controle de tarefas complexas, interdependentes e multifacetadas como são aquelas implementadas

pelos aparatos estatais contemporâneos em qualquer uma das áreas cobertas pelas políticas governamentais.

De fato, a premissa normativa que informa o desenho institucional preferido pelo autor é obter os maiores valores em cada um dos termos daquele binômio, em cada contingência específica, sem que nenhum deles se sobreponha ao outro. Mas para que se projete algum desenho organizacional que possa maximizar tanto a agilidade quanto o controle democrático, é preciso antes conhecer o que são e o que fazem os serviços de inteligência, tarefa a que se propõe o livro.

Com base em uma extensa pesquisa bibliográfica e documental, o livro analisa a dinâmica operacional, os desenhos organizacionais e os diversos mecanismos de controle público das atividades de segurança. A discussão sobre o ciclo de atividades de inteligência leva o leitor aos diversos circuitos de operação das atividades nessa área, expondo as engrenagens responsáveis pela expansão das operações de inteligência calcada nos desenvolvimentos tecnológicos das comunicações, bem como na inércia burocrática que preside a regulação pública da informação. Da mesma forma como não existe uma racionalidade inerente a essa expansão, já que é fruto das decisões e não-decisões de atores relevantes, em face das definições nacionais de segurança e limites da tecnologia disponível, também se mostra estreito o limite entre o legal e o não-legal, multiplicando-se as dificuldades para o controle efetivo das atividades nessa área.

A análise dos desenhos organizacionais de diversas experiências nacionais demonstra as descontinuidades organizacional e institucional que têm caracterizado a evolução desse campo de atividades no Estado moderno. A pesquisa desvenda o que consiste, na prática, o núcleo duro do Estado, no exercício de suas funções coercitivas que são parte de sua constituição enquanto aparato estatal. O estudo empírico da evolução organizacional desse campo não apenas desautoriza aquelas teses que consideram o Estado uma arena ou um campo de forças onde competem interesses diversos, como também aquelas que entendem os aparatos coercitivos como uma herança atávica de um passado absolutista. Curioso, igualmente, é que os mesmos fenômenos que, contemporaneamente, são apontados como impulsionadores do declínio do Estado e da soberania, pela maior permeabilidade das fronteiras que implicam, tais como o terrorismo, o crime organizado, o narcotráfico, a imigração ilegal e a ameaça de espionagem, são também responsáveis pela expansão da estrutura de inteligência sob o comando estatal.

O capítulo final sobre os problemas conceituais na definição de segurança e os mecanismos de controle público vincula analiticamente dois campos de pesquisa que, convencionalmente, têm estado separados: os estudos estratégicos e a análise das instituições e dos processos políticos. Como qualquer conceito polissêmico, o de segurança nacional é contestado, sendo várias as suas definições e evidentes os conflitos entre elas. Além de apresentar as razões para uma avaliação presciente dos limites práticos resultantes do atual movimento nos estudos internacionais contemporâneos de “securitização” de temas e problemas não relacionados ao uso potencial da força, o capítulo examina os limites dos diversos mecanismos existentes nas democracias contemporâneas de supervisão e controle externo sobre as atividades de inteligência. Três aspectos ressaltam do quadro examinado: a ausência dos temas correlatos da informação e do segredo na reflexão política contemporânea, seja de natureza teórica ou empírica; a relação inversa entre ampliação conceitual da segurança e desenhos organizacionais que maximizem o grau de controle público sobre aquela atividade; e, por fim, a inexistência de associação negativa entre agilidade e controle democrático: por que, sendo os serviços de inteligência uma das atividades mais difíceis de serem controladas nas democracias modernas, esses serviços governamentais não são mais ágeis nesses mesmos contextos políticos?

O livro demonstra que o tema da segurança vincula conceitual e institucionalmente os planos interno e externo, simultaneamente, expondo as contradições e tensões entre o sistema anárquico de Estados e as experiências nacionais democráticas. Se o sistema de Estados aumenta as demandas por segurança e informação de cada unidade nacional, também crescem as exigências de controle e supervisão que caracterizam a formação e a implementação de políticas governamentais em contextos democráticos. No plano mundial, o fim da Guerra Fria, ainda que tenha eliminado uma fonte significativa de instabilidade do sistema internacional, não tornou o mundo mais pacífico e menos violento, já que são múltiplas as razões para as incertezas que caracterizam a ordem mundial contemporânea. Ademais, a porosidade das fronteiras nacionais potencializa e multiplica as fontes de insegurança, com repercussões nas políticas públicas das unidades nacionais. No caso brasileiro, com o fim do regime militar e a instauração de uma nova ordem constitucional, os serviços de segurança foram objeto de regulação pública, com a aprovação pelo Congresso Nacional do Sistema Brasileiro de Inteligência, em 1999.

Em vista dos novos desafios internacionais e das profundas transformações na estrutura institucional brasileira, o livro de Marco Cepik constitui uma excelente oportunidade para que a sociedade e a opinião pública do país possam saber mais sobre esse objeto cinzento, cuja maior e sempre necessária transparência depende da existência de instituições estáveis de fiscalização e controle só encontráveis em contextos democráticos.

*Maria Regina Soares de Lima*, PhD  
Professora do Instituto Universitário de Pesquisas do  
Rio de Janeiro (Iuperj) e do Instituto de  
Relações Internacionais (IRI) da PUC-Rio

## Introdução

Em suas *Lezione americane: sei proposte per il prossimo millennio* (1988), Italo Calvino situava a rapidez e a visibilidade entre os valores literários que deveriam ser cultivados em nossa época.<sup>1</sup> Rapidez e visibilidade correspondem, *grosso modo*, aos dois valores políticos discutidos neste livro: a agilidade e a transparência. No caso dos serviços de inteligência, agilidade e transparência sintetizam ainda os dilemas mais persistentes no processo de institucionalização dessas organizações no Estado contemporâneo.<sup>2</sup>

Para Calvino, a rapidez a ser valorizada em nosso tempo não poderia ser exclusivamente aquele tipo de velocidade inspirada por Mercúrio, o deus de pés alados, leve e desenvolto. Através de Mercúrio se estabelecem as relações entre os deuses e os homens, entre leis universais e casos particulares, entre a natureza e as formas de cultura. Hoje, escreve Calvino, a velocidade de Mercúrio precisaria ser complementada pela persistência flexível de Vulcano, um “deus que não vagueia no espaço, mas que se entoca no fundo das crateras, fechado em sua forja onde fabrica interminavelmente objetos de perfeito lavor em todos os detalhes – jóias e ornamentos para os deuses e deusas, armas, escudos, redes e armadilhas”.<sup>3</sup>

Da combinação entre velocidade, persistência, relevância, precisão e flexibilidade surge a noção contemporânea de agilidade, transformada em *mot juste* de nosso tempo. Uma agilidade que vem se tornando um lugar-comum, senão na vida prática das organizações, pelo menos nos discursos. Empresas, governos, universidades, exércitos e indivíduos querem ser ágeis. Também os serviços de inteligência querem ser ágeis, uma exigência cada vez mais decisiva para justificar sua própria existência no mundo de hoje.

Serviços de inteligência são agências governamentais responsáveis pela coleta, pela análise e pela disseminação de informações consideradas relevantes para o processo de tomada de decisões e de implementação de políticas públicas nas áreas de política externa, defesa nacional e provimento de ordem pública. Essas agências governamentais também são conhecidas como serviços secretos ou serviços de informação. Embora o uso de espiões e informantes especializados remonte à antigüidade em áreas tão dispersas quanto a China, o Oriente Próximo e o Império Romano, a atividade de inteligência adquiriu uma nova escala operacional como função social organizada, profissio-

nal e permanente com o surgimento do Estado moderno na Europa. Mesmo então, os serviços de inteligência, tal como os conhecemos hoje, só começaram realmente a institucionalizar-se no século XX. Por institucionalização entende-se aqui o processo através do qual organizações e procedimentos adquirem estabilidade e valor.<sup>4</sup>

Após o final da Guerra Fria, em muitos países foi debatida a própria necessidade e o papel desses serviços, o que poderia indicar que seu crescente peso institucional fora, na verdade, apenas um fenômeno passageiro, um subproduto das duas guerras mundiais e da própria Guerra Fria. Durante a primeira metade da década de 1990, os serviços de inteligência tiveram de fato seus orçamentos reduzidos de forma significativa, ao mesmo tempo em que o novo contexto internacional tornava-se mais volátil e, por conseguinte, as demandas por informações tornavam-se mais exigentes e diversificadas. Por outro lado, a emergência e o crescimento vertiginoso das novas tecnologias de informação e comunicação (TICs) possibilitaram o surgimento de empresas privadas que ofertam informações sobre temas de segurança em escala global, competindo em muitas áreas com os próprios serviços de inteligência pela atenção e pelos recursos orçamentários dos governantes. A resposta dos serviços de inteligência a esses desafios tendeu inicialmente a ser reativa, adaptando-se aos novos orçamentos e ao novo cenário internacional.<sup>5</sup>

Contudo, na medida em que se aproximava o começo do século XXI e os serviços de inteligência continuavam sendo uma parte estável da maquinaria governamental dos países, a resposta típica aos desafios da nova realidade internacional tendeu a deslocar-se para uma discussão muito mais *low profile* sobre as condições de eficiência e efetividade dos serviços de inteligência no cumprimento de suas missões.<sup>6</sup>

No caso norte-americano, por exemplo, Frederick T. Martin (1999:317-352) afirma que há uma crescente convergência entre os projetos de modernização tecnológica coordenados pelo Pentágono e pelo Escritório do Diretor Central de Inteligência (DCI).<sup>7</sup> No contexto de uma competição mais direta com outros provedores de informações, recursos mais escassos e situação internacional cambiante, a busca por agilidade corresponderia a uma estratégia baseada em três eixos integrados:

- velocidade – os processos de coleta, análise e disseminação de informações relevantes para a segurança nacional deveriam operar com ciclos temporais mais curtos para atender às mudanças bruscas de atenção e prioridade dos usuários, sejam eles *policymakers*, legisladores ou comandantes militares;
- capacidade – como as tecnologias de coleta e produção de dados brutos ultrapassaram imensamente a capacidade de processamento, produção e disseminação de inteligência “finalizada”, um aumento de capacidade nessas

áreas torna-se decisivo para que as organizações de inteligência possam acrescentar *inputs* de maior valor agregado aos processos decisórios da área de segurança nacional;

■ flexibilidade – na medida em que as crises e temas de política externa aparecem e desaparecem sem muito aviso prévio, sobrepondo-se à agenda cada vez mais exigente dos governantes, as relações de custo e benefício dos recursos investidos nas organizações de inteligência envolvem pressões crescentes por maior flexibilidade e também por maior integração entre as várias agências.

Embora o livro de Frederick Martin lide extensamente com as inúmeras dificuldades tecnológicas e de cultura organizacional para a realização desse conceito de “agilidade” nas agências de inteligência norte-americanas, os problemas decorrentes das próprias características operacionais e da organização das atividades de inteligência são largamente subestimados.<sup>8</sup> Deixei então percorrer um caminho distinto, procurando entender como as próprias características operacionais e o *design* organizacional da atividade de inteligência afetam suas chances de institucionalização no Estado contemporâneo.<sup>9</sup>

Esse é, de modo geral, um problema pouco explorado pela literatura especializada.<sup>10</sup> Siglas como CIA, KGB, Mossad e SIS são relativamente familiares para o público, mas o conhecimento médio sobre suas atividades e estruturas organizacionais restringe-se a alguns fatos pitorescos ou imagens distorcidas pela mídia e pela literatura ficcional.<sup>11</sup>

Nesse sentido, um outro traço persistente da trajetória dos serviços de inteligência é justamente sua relativa opacidade, o manto de segredo que cerca suas atividades.<sup>12</sup> Como a transparéncia dos atos governamentais é um dos requisitos mais valorizados da prática política contemporânea (e a principal promessa não cumprida da democracia), não é de se estranhar que a mera existência de serviços de inteligência gere desconfiança e insegurança nos cidadãos dos próprios países que têm organizações desse tipo. A visão negativa que os cidadãos tendem a ter dos serviços de inteligência de seus próprios países faz da transparéncia um enorme desafio no processo de institucionalização dessas atividades. Para introduzir o tema, voltemos um instante ao texto de Italo Calvino.

Segundo Calvino, a visibilidade como um valor literário envolve não apenas a capacidade de ver a realidade do mundo e dela partir para a criação escrita de uma estória. Calvino estava mais preocupado justamente com a perda contemporânea da capacidade de imaginar visualmente conteúdos e significados para então tentar expressá-los através da escrita. Numa época em que a literatura já não se refere à tradição, mas sim à originalidade e à invenção, a capacidade de imaginação individual *in absentia* é decisiva e vem

sendo afetada negativamente pela saturação de imagens pré-fabricadas. Esse fenômeno torna imperativo o que Calvino chama de “pedagogia da imaginação”, uma educação que nos torne capazes de expressar verbalmente e através da escrita as visões polimorfas obtidas através dos olhos e da alma.

Embora a idéia de visibilidade em Calvino seja incomensurável em relação à idéia de transparência como dilema de institucionalização, ela é sugestiva, pois evoca o tipo de ambigüidade e desafio com que se tem de lidar na abordagem do fenômeno da transparência dos atos governamentais. Ambigüidade que se expressa, inclusive, pelo fato de transparência poder significar simultaneamente visibilidade e invisibilidade.

Na área de informática, por exemplo, transparência é uma metáfora óptica utilizada para destacar a propriedade invisível das interfaces, que garante que os usuários possam usar recursos e resolver problemas sem que tenham que passar por (“visualizar”) todas as etapas e operações intermediárias realizadas pelos sistemas.<sup>13</sup> De modo geral, as chamadas atividades-meio do Estado (em que se incluem as atividades de provimento de informações para a tomada de decisões) seriam, nesse sentido, transparentes para os cidadãos, que olhariam através delas para visualizar e controlar os atos dos governantes em relação aos fins considerados desejáveis pela comunidade política (*polity*). Entretanto, o gigantismo burocrático, a ineficiência e a corrupção tornam o meio administrativo opaco e os próprios atos governamentais invisíveis. Daí que a transparência como um princípio republicano e democrático seja associada não à valorização da invisibilidade do meio, mas sim à busca da capacidade – por parte do cidadão – para visualizar e julgar por si mesmo o que os governos estão fazendo nas várias esferas de ação política. Essa capacidade de fazer uso do próprio entendimento (o *Sapere aude*, na sua versão kantiana) é que dá sentido à transparência e a aproxima da visibilidade educada, tal como expressa valorativamente por Calvino.

Para David Luban (1996:154-198), a transparência dos atos, normas e políticas governamentais é uma condição necessária para a manutenção da confiança popular (*trust*) que sustenta as instituições democráticas e legitima as pretensões dos governantes de obtenção de colaboração e obediência dos governados. O princípio de publicidade (transparência) é uma proposição de tipo moral e também um princípio de desenho institucional. Nenhuma agência ou área de atuação governamental, para manter-se consistente com o princípio da transparência, deveria ser construída segundo linhas de funcionamento que dependessem do segredo para sua efetividade e eficácia.

No entanto, serviços de inteligência são justamente organizações que dependem do segredo sobre seus métodos de atuação e suas fontes de informação para operar de forma eficaz. Na medida em que o processo de institucionalização desse tipo de organização implica não apenas um esfor-

ço para tornar-se estável (o que depende da agilidade), mas também uma busca por reconhecimento e valor aos olhos dos cidadãos (o que depende da transparência), não se pode simplesmente contornar o problema de forma pragmática, dizendo que a existência de segredos governamentais e de serviços de inteligência constitui exceções a uma regra ou princípio.<sup>14</sup>

Na verdade, o segredo governamental e as atividades de inteligência são compatíveis com o princípio da transparência somente quando a justificação de sua existência puder ser feita, ela própria, em público. Nesses termos, a proposição de Luban fornece um interessante ponto de partida para a análise das complexidades, tensões e condições de possibilidade associadas à transparência como um desafio de institucionalização.

Além de discutir por que e como as características operacionais e os contornos organizacionais dos serviços de inteligência dificultam a busca por agilidade, decidi estudar também como esses mesmos contornos organizacionais e características operacionais limitam a transparência das atividades governamentais nas áreas ligadas ao provimento de segurança. Embora as duas dimensões normativas apresentem-se como desafios na trajetória de qualquer organização, regra ou procedimento e, no limite, configurem um duplo dilema de institucionalização, não se trata aqui de reiterar o argumento tecnocrático sobre a existência de um mecanismo de *trade-off* entre agilidade e transparência, através do qual ganhos em uma dimensão só seriam possíveis a expensas da outra.

As implicações autoritárias daquele tipo de argumento são muito claras ao sugerirem, por exemplo, que a eficiência governativa dependeria largamente do segredo e do insulamento burocrático. Ou, pelo ângulo inverso, que ganhos institucionais em transparência limitariam necessariamente a agilidade das organizações. Embora seja razoável supor que o segredo é um requisito funcional mais ou menos importante para a eficácia e a eficiência de certas ações governamentais, isso não elimina o problema da justificação pública (transparência) acerca da própria necessidade daqueles segredos. Por outro lado, embora se possa sustentar que a legitimidade (transparência) constitui, em maior ou menor medida, uma das condições que garantem a eficiência e a eficácia (agilidade) da ação governamental, seria igualmente equivocado supor que todos os problemas de agilidade poderiam ser resolvidos através de ganhos institucionais em transparência. Nesse sentido, trata-se realmente de duas dimensões com exigências próprias e muito complexas nos processos de institucionalização, em especial no caso das organizações de força e nos serviços de inteligência do Estado.

O duplo dilema da agilidade e da transparência no processo de institucionalização de serviços de inteligência é, portanto, o fio condutor que unifica e confere lógica expositiva ao texto.

Vale notar, porém, que a pesquisa bibliográfica e documental foi conduzida a partir de um leque relativamente mais amplo de perguntas: 1. O que é e como funciona a atividade de inteligência? 2. Por que surgiram e por que, na maioria dos países, existem diversas agências governamentais de inteligência? 3. Como o conceito de segurança nacional e a instituição do segredo governamental estão relacionados com a atividade de inteligência? 4. Quais são os instrumentos disponíveis e os limites do controle externo sobre os serviços de inteligência num Estado democrático?

Como será possível observar ao longo do livro, uma resposta satisfatória para essas questões está longe de ser obtida, tanto do ponto de vista teórico quanto prático. Creio, entretanto, que este estudo contribui para estabelecer o debate num patamar mais elevado em termos de rigor analítico e atenção à evidência empírica.

O texto está dividido em três grandes capítulos, em que são analisados diversos aspectos relacionados ao duplo desafio da agilidade e da transparência no âmbito das atividades governamentais de inteligência e segurança.<sup>15</sup> Os dois primeiros capítulos concentram-se no tema da agilidade e são escritos *ex parte principis*, ou seja, do ponto de vista da preocupação típica dos governantes para com a utilidade, a capacidade e a eficiência dos serviços de inteligência. O terceiro capítulo trata da transparência e é redigido *ex parte populi*, ou seja, do ponto de vista da preocupação típica dos cidadãos de uma comunidade política democrática para com os limites e funções do Estado.

O capítulo 1 estabelece os parâmetros iniciais para a discussão. Nesse capítulo, a atividade de inteligência é definida de forma mais precisa como um tipo de conflito informacional. Também são analisadas as áreas de fronteira entre o trabalho de inteligência e outros tipos de atividade informacional (especialmente as chamadas informações de combate).

A noção de ciclo de inteligência, discutida na segunda parte do capítulo, refere-se à especialização funcional entre as diversas disciplinas de coleta de informações e as etapas posteriores de análise e disseminação. Essas disciplinas de coleta são definidas segundo as fontes típicas a partir das quais as informações são obtidas. As três áreas mais importantes são a inteligência obtida a partir de fontes humanas (*humint*), inteligência obtida a partir da interceptação de comunicações e de outros sinais eletromagnéticos (*sigint*) e a inteligência obtida a partir de imagens (*imint*).<sup>16</sup> Ainda na segunda parte do capítulo são apresentadas as categorizações mais comuns utilizadas para estruturar as várias etapas do ciclo.

As características operacionais dessas e de outras disciplinas especializadas de coleta, bem como os problemas de integração entre as várias etapas do ciclo, permitirão ao leitor uma visão mais sistemática da dialética entre inteligência e segurança que estrutura toda a dinâmica

operacional dos serviços de inteligência contemporâneos, inclusive a área de contra-inteligência. Nesse capítulo também é discutido o conceito de operações encobertas e sua relação com as atividades de inteligência. Nas considerações finais do capítulo são sintetizadas as restrições impostas pela própria natureza das operações de inteligência à busca por agilidade, resultando dessa discussão uma conclusão preliminar sobre a utilidade relativa da atividade de inteligência para os governantes.

O capítulo 2 também parte dos fundamentos, mas o foco já não é operacional e sim organizacional. O capítulo começa mostrando como os serviços de inteligência modernos surgiram no contexto dos Estados absolutistas europeus, procurando generalizar os tipos de requisitos funcionais que os novos governantes aparentemente pretendiam atender ao criarem tais organizações. Esses requisitos eram, basicamente, a necessidade de reduzir custos na obtenção de informações e o desejo de ampliar sua capacidade de dominação (*enforcement*). Essa dupla função dos serviços de inteligência, simultaneamente informacional e coercitiva, fica evidente quando se consideram, na segunda parte do capítulo, as três matrizes que deram origem aos serviços de inteligência, a saber, a diplomacia, o fazer a guerra e o policiamento. A partir dessas três marizes, o “crescimento institucional” descontínuo desses serviços culminou na formação, já bem adiantado o século XX, de sistemas nacionais de inteligência.

Esse processo, discutido na terceira seção do capítulo, envolveu dois movimentos complementares. De um lado, houve uma expansão horizontal no número de agências como resultado da especialização funcional ao longo das etapas do ciclo de inteligência. De outro, houve uma expansão vertical do sistema através da formação de subsistemas de inteligência militar e policial. A formação dos sistemas nacionais de inteligência acompanhou os contornos mais gerais da evolução do Estado em cada país. Na quarta seção do capítulo são utilizados os casos dos Estados Unidos e da Grã-Bretanha para exemplificar como matrizes doutrinárias e históricas similares dão origem a sistemas nacionais de inteligência ainda assim peculiares. Apesar das enormes disparidades entre as realidades nacionais, estima-se que as atividades de inteligência das maiores potências do sistema internacional empregavam, em 1995, mais de 1 milhão de pessoas e custavam aos governos mais de US\$100 bilhões por ano.<sup>17</sup>

Considerando então o peso relativo dos serviços de inteligência no Estado contemporâneo, a seção final foi dedicada a uma tentativa de sincretizar as principais conclusões sobre desenho organizacional e agilidade, enquadrando-as a partir de uma versão revisada do novo institucionalismo.

Por último, mas não em último lugar, o capítulo 3 analisa a relação entre segurança nacional, segredo governamental e controle externo das ati-

vidades de inteligência. Na primeira seção do capítulo discutem-se o conceito de segurança nacional e os problemas decorrentes da tensão entre segurança individual e segurança estatal. Mesmo reconhecendo que o Estado moderno é simultaneamente uma fonte de segurança e de ameaça para os indivíduos, considero que a natureza mesma do sistema internacional e das sociedades nacionais torna a segurança coletiva irredutível ao bem-estar dos indivíduos. Isso nos obriga a conviver da melhor forma possível (e freqüentemente da pior forma imaginável) com a tensão inerente ao conceito de segurança nacional. Na parte final dessa primeira seção adoto provisoriamente a perspectiva da “teoria dos complexos de segurança” como uma alternativa às posições autoritárias, liberais e pós-modernas na análise de problemas de segurança.

Essa tomada de posição me permite, na segunda seção do capítulo, discutir de forma mais consistente a *rationale* e os problemas do segredo governamental. Esse tipo de segredo é concebido como uma forma de regulação pública de fluxos informacionais que demanda, portanto, justificação pública sobre sua necessidade prática e validade moral. Uma vez estabelecida a regulação, os segredos de Estado não se manteriam secretos se contassem apenas com a discrição dos indivíduos que partilham a informação sigilosa, ou se contassem apenas com a indiferença alheia. Nesse sentido, o restante da seção discute três processos complementares que, segundo a literatura especializada, são utilizados para se tentar garantir a efetividade do segredo governamental: procedimentos de classificação, controles de acesso e punições em caso de revelação não autorizada. Os riscos associados ao uso excessivo e injustificado do segredo governamental são discutidos de forma mais concreta na terceira seção do capítulo, que trata dos mecanismos de controle externo das atividades de inteligência e segurança.

Embora a mídia e os poderes Judiciário e Executivo exerçam alguma supervisão e controle, a seção discute principalmente o papel do Congresso, seus mecanismos de supervisão (*oversight*), os (poucos) incentivos que os parlamentares têm para participar do controle externo das áreas relacionadas à segurança nacional e as consequências que tudo isso tem para o princípio de transparência.

Nas considerações finais do livro são reapresentados brevemente os fundamentos da tensa relação entre inteligência e democracia, bem como os argumentos sobre os desafios da transparência e sua possível aplicação para o Brasil.

Aliás, embora os chamados *intelligence studies* sejam uma área de pesquisa acadêmica relativamente consolidada no plano internacional, no Brasil esse é um dos primeiros trabalhos que analisam a existência, as características operacionais e organizacionais e os problemas de institucionalização de serviços de inteligência.<sup>18</sup> Atualmente existem diversas iniciativas internacionais de pes-

quisa em andamento, tanto no âmbito da seção de estudos sobre inteligência da International Studies Association (ISA), quanto no âmbito do British Study Group on Intelligence, da Canadian Association for Security and Intelligence Studies (Casis), do Consortium for the Study of Intelligence (Georgetown University), do Harvard's Intelligence and Policy Program (John Kennedy School of Government) e do International Intelligence History Group (IIHG, com sede na Alemanha), para mencionar apenas alguns grupos.<sup>19</sup>

De modo geral, pode-se situar os estudos de inteligência como uma especialização no âmbito dos *strategic studies*, os quais podem ser definidos como o campo de estudos que tem por objeto principal de análise os fenômenos associados ao “uso da força para compelir o outro à nossa vontade”.<sup>20</sup> No Brasil, os próprios estudos estratégicos ainda são pouco consolidados como área acadêmica de pesquisa, praticamente inexistindo no âmbito de programas de pós-graduação em relações internacionais e ciência política.<sup>21</sup> Nesse contexto rarefeito, destacam-se institucionalmente o Grupo de Estudos Estratégicos (GEE) da Coppe/UFRJ e o Núcleo de Estudos Estratégicos (NEE) da Unicamp.<sup>22</sup>

Serviços de inteligência não podem ser definidos como um tipo puro de organização de força do Estado, uma vez que cumprem funções primordialmente informacionais. Por outro lado, na medida em que também desempenham algumas funções coercitivas e, principalmente, na medida em que mesmo suas funções informacionais são parte de interações conflitivas mais amplas, adaptam-se mais à abordagem *stricto sensu* dos estudos estratégicos. Afinal, as organizações de inteligência militar são consideradas agências de suporte ao combate, e mesmo as organizações civis de inteligência fazem parte da institucionalidade de segurança dos Estados, pois derivam sua razão de ser da obtenção, da análise e da disseminação de informações relevantes para os processos decisórios e para a implementação de políticas públicas nas áreas de política externa, política de defesa e provimento de ordem pública.<sup>23</sup>

Nesse sentido, este livro sobre serviços de inteligência também tem por objetivo contribuir para o avanço e a consolidação dos estudos estratégicos no Brasil.

## Notas

1. Na verdade, apenas cinco das seis Charles Eliot Norton Poetry Lectures na Universidade de Harvard chegaram a ser escritas por Calvino antes de morrer. Essas cinco *lezione americane* é que foram publicadas postumamente em 1988. Os seis valores literários destacados por Calvino seriam a leveza, a rapidez, a exatidão, a visibilidade, a multiplicidade e a consistência. Cf. Calvino (2000).

2. Para uma discussão sobre a interface empírico-normativa nas teorias sobre *design institucional*, ver Goodin (1999:1-53).

3. Calvino (2000:64-65).

4. Essa é uma definição minimalista de institucionalização retirada da obra de Samuel P. Huntington (1975), publicada originariamente em 1968, muito criticada por sua generalidade. Segundo Huntington, sistemas políticos institucionalizados seriam aqueles em que as regras e as organizações públicas são não apenas estáveis, mas também efetivamente interiorizadas (valorizadas) por parte dos membros da coletividade. Devidamente depurado de quaisquer traços etnocêntricos e de ênfases excessivas na questão do “grau de governo”, o recurso à categoria de institucionalização permite um amplo programa de pesquisas sobre várias dimensões do problema da acomodação institucional do convívio social em sociedades complexas, marcadas pela diversidade de interesses conflitantes e pela multiplicidade de fins legítimos estabelecidos pelos atores.

No caso dos serviços de inteligência tomados enquanto objeto de investigação das ciências sociais, duas linhas de pesquisa seriam possíveis a partir da noção de institucionalização: a primeira, claramente mais ambiciosa e significativa, poderia tentar analisar o papel desempenhado por essas organizações na formação e na consolidação da aparelhagem estatal contemporânea, bem como seu significado mais geral para a capacidade de *enforcement* de um equilíbrio democrático entre regras institucionais e jogos de interesse. Uma segunda linha de investigação, menos abrangente porém mais adequada aos estágios iniciais da pesquisa de objetos até aqui inexplorados, poderia mobilizar o esquema conceitual derivado da abordagem da institucionalização para propor uma interpretação preliminar sobre o surgimento desse tipo de organização, as funções desempenhadas por esses serviços de inteligência e as principais dificuldades enfrentadas para se tornarem estáveis (o que depende hoje em dia do que chamei aqui de agilidade) e dotados de valor (o que depende, em se tratando de regimes democráticos, da compatibilização de sua lógica operacional com o princípio da transparência). Essa será a abordagem predominante ao longo do trabalho. Nos capítulos 2 e 3, a literatura recente do novo institucionalismo será mobilizada eventualmente para se tentar extrair dessa análise preliminar do processo de institucionalização dos serviços de inteligência algumas consequências mais gerais para uma taxonomia das agências governamentais nos sistemas políticos democráticos. De modo geral, porém, a enorme dificuldade de obtenção de dados empíricos comparáveis sobre serviços de inteligência impede que se possa ir além de uma primeira tentativa de testar heuristicamente a noção de institucionalização em relação ao caso dos serviços de inteligência.

A definição de instituições como “padrões de comportamento estáveis e valorizados”, em termos que derivam diretamente da formulação original de Huntington (1975), é utilizada para produzir uma síntese entre as diferentes abordagens neo-institucionalistas no trabalho já citado de Goodin (1999:21). Para uma crítica dos aspectos etnocêntricos das teorias sobre desenvolvimento político, ver Tilly (1975:601-638). Para uma avaliação sobre o estágio atual e as potencialidades do programa de pesquisas sobre institucionalização política no Brasil, ver Fábio W. Reis (1999:157-190). Por motivos que ficam evidentes a partir da leitura do texto de Fábio Wanderley Reis, a eventual leitura do texto de Fernando Llinongi sobre o mesmo tema – e que vai publicado no mesmo volume – deve ser feita com bastante cuidado em função da quantidade de equívocos ali contidos. Para um tratamento exaustivo e competente dos problemas associados à modernização e ao desenvolvimento político, de um ponto de vista sensível aos dilemas da ação coletiva em múltiplas arenas, ver Reis (1997).

5. No caso norte-americano, essa busca de novas missões como forma de justificação da existência dos serviços de inteligência recebeu uma síntese emblemática – e nada sutil – na declaração feita ao Senado pelo então diretor de inteligência central James Woolsey: “(...) *We have slain a large dragon. But we live now in a jungle filled with a bewildering variety of poisonous snakes*”. Cf. US Congress (1993a). A mesma declaração sobre a “selva de cobras venenosas no lugar do grande dragão soviético” foi repetida inúmeras vezes por Woolsey. Ver, por exemplo, o discurso: *Future of intelligence: critical issues* (DCI James Woolsey at Chicago Executives’ Club. Sept. 19, 1993. 54min. By Purdue University Public Affairs Video Archives). Dois anos mais tarde, já na segunda metade do primeiro mandato de Bill Clinton, a Casa Branca definiu em seu documento básico de segurança nacional para a década de 1990 quais seriam as missões prioritárias dos serviços de inteligência:

*“Because national security has taken on a much broader definition in this post-Cold War era, intelligence must address a much wider range of threats and dangers. We will continue to monitor military and technical threats, to guide long-term force development and weapons acquisitions, and to directly support military operations. Intelligence will also be critical for directing new efforts against regional conflicts, proliferation of WMD (weapons of mass destruction), counterintelligence, terrorism and narcotic trafficking. In order to adequately forecast dangers to democracy and to US economic well-being, the intelligence community must track political, economic, social and military developments in those parts of the world where US interests are most heavily engaged and where overt collection of information from open sources is inadequate. Finally, to enhance the study and support of worldwide environmental, humanitarian and disaster relief activities, technical intelligence assets (principal imagery) must be directed to a greater degree towards collection of data on these subjects”.* US Government (1995:17).

6. Ver Balachadran (2000), a título de exemplo, sobre o questionamento sobre as falhas analíticas e técnicas das principais agências de inteligência da Índia (RAW e IB) durante o último confronto com o Paquistão em torno da questão da Caxemira e dos testes nucleares. Para um balanço sobre as transformações recentes na estrutura e nas prioridades dos serviços de inteligência e segurança da Rússia, ver Galeotti (1995) e Knight (1996).

7. Três dos documentos citados por Martin (1999) me parecem ser os mais importantes para a compreensão das linhas gerais da nova arquitetura integrada de disseminação de inteligência no governo dos Estados Unidos. US Government (1997b, 1999c e 1999d).

8. Seria injusto não observear que o foco principal do livro de Frederick Martin é posto sobre o processo gerencial e tecnológico de construção do Intelink, a intranet da comunidade de inteligência dos Estados Unidos. Por isso mesmo, os capítulos mais interessantes do livro são aqueles em que se discutem as camadas do Intelink (2), sua arquitetura geral e padrões (3), os capítulos sobre segurança (4 e 5) e os capítulos sobre ferramentas e serviços para usuários (6). Cf. Martin (1999:39-198).

9. Para Huntington (1968:24-25), o nível de institucionalização de um sistema político poderia ser medido a partir dos seguintes pares de variáveis: adaptabilidade/rigidez, complexidade/simplicidade, autonomia/subordinação e coerência/desunião. Caso essas variáveis pudesssem ser desdobradas em indicadores mensuráveis, os sistemas políticos po-

deriam ser comparados em termos de seus níveis de institucionalização. Seria possível também medir o grau de institucionalização de organizações e procedimentos particulares dentro de um sistema político. Numa perspectiva mais explicitamente normativa, Goodin (1999:39-43) oferece alguns princípios desejáveis de desenho institucional que poderiam funcionar também como parâmetros para a avaliação de organizações, regras ou procedimentos. São discutidos por aquele autor cinco princípios que deveriam guiar o esforço de construção institucional: revisibilidade, robustez, sensibilidade à complexidade motivacional, publicidade e variabilidade. Para poder viabilizar algum diálogo entre a escassa evidência empírica disponível sobre serviços de inteligência e características desejáveis de sistemas institucionalizados, decidi considerar de forma muito agregada as “variáveis” independentes “características operacionais” e “perfil organizacional”, além de tomar os valores da “agilidade” e da “transparência” como variáveis dependentes. O jogo de idéias possibilitado por essas quatro variáveis permite testar uma interpretação preliminar (posto que não há condições de se tentar ainda qualquer tipo de explicação propriamente dita) sobre a trajetória moderna dos serviços de inteligência em geral, e do caso norte-americano em particular, em relação a diferentes soluções possíveis (*outcomes*) para o desafio de institucionalização desse tipo particular de organização no contexto do Estado contemporâneo.

10. Uma exceção importante é o recente trabalho de Zegart (1999).

11. Outras tantas siglas poderiam ser mencionadas, muito menos conhecidas mas não menos importantes. São tantas as agências governamentais ligadas à área de inteligência nos diversos países, com funções tão diferentes, que uma definição pragmática poderia assumir que inteligência é tudo aquilo que organizações de inteligência fazem... Mas esse seria claramente um tratamento insatisfatório, e o livro que o leitor tem em mãos é justamente uma tentativa de ir além dessa fórmula pragmática e lacônica. Ver, como um exemplo de comentário-padrão em ciências sociais sobre serviços de inteligência, McLean (1996:242).

12. A dicotomia opacidade/transparência é central, por exemplo, na análise realizada por José Maria Jardim em sua tese de doutoramento sobre os acervos informacionais do Estado brasileiro. Cf. Jardim (1999).

13. Esse uso peculiar da noção de transparência como parte do jargão dos engenheiros de software sempre me causou certa estranheza. Agradeço a Gustavo Torres e Juliana Bemfica a explicação bem-humorada. Para a distinção, por exemplo, entre ferramentas de segurança “transparentes” para os usuários e os aplicativos que utilizam tais ferramentas, ver Martin (1999:123-198).

14. Em texto ensaístico recente sobre a relação entre segredo e democracia, Norberto Bobbio (2000:399-415) já admite, em função da natureza do sistema internacional e apenas como medida defensiva de um Estado democrático num mundo em que nem todos os Estados são democráticos, que, excepcionalmente, os governos de países democráticos se utilizem do segredo e de serviços de inteligência.

15. Caso perguntado sobre quais são os melhores textos disponíveis internacionalmente sobre inteligência para quem quiser iniciar o estudo desse tema, eu recomendaria sete livros: Maurer, Tunstall & Keagle (1985), Shulsky (1992), Gill (1994), Godson (1995), Herman (1996), Swenson (1997), e Lowenthal (2000). A mais completa base de dados

bibliográficos sobre inteligência disponível *online* na internet é a do Muskingum College, Ohio <<http://intellit.muskingum.edu>>. Outros endereços eletrônicos úteis estão listados na seção sobre Fontes. As bibliografias comentadas de Lowenthal (1994) e Constantinides (1983) continuam sendo úteis, principalmente em relação ao caso norte-americano.

16. Os acrônimos utilizados ao longo do texto serão grafados com caracteres minúsculos. Siglas e nomes de organizações, quando não forem acrônimos, serão grafados em maiúsculas (HVA, CIA, UN, KGB etc.); quando forem e tiverem quatro letras ou mais, terão a inicial em maiúscula (Otan, Ukusa etc.)

17. A estimativa é de Jeffrey Richelson (1995:v): “*Today, major intelligence establishments are supported by governments from Washington to Moscow and London to Canberra. In addition, intelligence is no longer a world of spies, counterspies, political operatives, defectors, and dark alleys. It is that and much more – a world of thirty thousand-pound spy satellites, aircraft packed with cameras and electronic equipment, bristling antenna farms, ultra-high-speed computers, and analysts with advanced degrees in mathematics, physics, foreign languages, economics, engineering, and political science. It is a world with over a million inhabitants that costs more than a hundred billions dollars a year. And despite the end of the Cold War, it is a world that will continue to flourish for a long time to come*”.

18. Conheço três dissertações de mestrado que, embora focando o caso brasileiro, utilizam elementos de análise e revelam conhecer a literatura internacional sobre *intelligence*: Emilio (1992), Diniz (1994) e Antunes (2000).

19. Para uma contextualização do surgimento dos estudos de inteligência como campo de pesquisa, ver a introdução de Godson & Robertson (1987) e também a introdução de Godson (1988). Para um comentário sobre o relativo isolamento entre o campo dos estudos de inteligência (*intelligence studies*) e a área mais ampla de relações internacionais, ver Fry & Hochstein (1993). Para uma síntese da agenda de pesquisa comparada em inteligência no começo da década de 1990, ver Hasted (1991). Para uma listagem de 54 teses tratando de temas de inteligência defendidas em seis países entre 1996 e 1997, ver Hindley (1998). Para um *survey* recente sobre os cursos acadêmicos disponíveis internacionalmente, ver Hindley (2000). Finalmente, vale conferir também os *papers* reunidos em Swenson (1999). Os dois periódicos internacionais especializados mais importantes são o *Intelligence and National Security*, publicado na Inglaterra pela FranckCass, e o *International Journal of Intelligence and Counterintelligence*, publicado nos Estados Unidos.

20. Essa delimitação analítica do objeto de pesquisa dos estudos estratégicos aparece formulada em Proença Jr. & Diniz (2001). Sobre a agenda de pesquisa e ensino na área de estudos estratégicos, ver Godson, Shultz & Quester (1997).

21. Dois artigos recentes sobre a situação da área de relações internacionais no Brasil destacam a falta de pesquisas sobre temas relacionados à segurança internacional. Cf. Almeida (1999) e Miyamoto (1999).

22. Como o núcleo de Campinas dedica-se prioritariamente ao estudo das relações civis-militares em contextos de transição e consolidação da democracia, foram os pesquisadores ligados ao GEE que priorizaram no Brasil o estudo das relações entre sistema político (relações internacionais e ordem pública) e as organizações de força do

Estado, com uma abordagem centrada no “estudo do uso da força para dobrar a vontade de outrem”. Para uma visão geral sobre a abordagem teórica do GEE/UFRJ, ver, por exemplo, Proença Jr., Diniz & Raza (1999), e também Proença Jr. & Diniz (1998). Para uma visão geral da produção acadêmica do NEE/Unicamp, ver, por exemplo, Cavagnari (1994) e também Saint-Pierre (1993).

23. Para quem se interessa por situar as diversas abordagens sobre segurança internacional ao longo do *continuum* objetivismo-subjetivismo, ver a introdução e a conclusão do livro de Buzan, Wæver & Wilde (1998:1-20 e 195-213), bem como a revisão crítica da literatura feita por Walt (1991:211-239). Em se tratando de aceitar um rótulo, pode-se dizer que eu me considero mais próximo dos chamados *traditional security studies* (TSS) do que dos *critical security studies* (CSS), embora realmente isso não queira dizer muita coisa.

## 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 involves 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).

Neste primeiro capítulo analiso as principais dinâmicas operacionais que caracterizam as atividades de inteligência. Sem isso, qualquer discussão sobre os requisitos de agilidade e transparência no processo de institucionalização dos serviços de inteligência ficaria prejudicada.<sup>1</sup>

Como avaliar, por exemplo, se as comissões de supervisão congressual atualmente existentes são adequadas sem que se tenha uma noção razoável sobre o que, afinal, tais comissões deveriam estar supervisionando? Como saber se os governantes poderão receber as informações solicitadas e consideradas vitais sem se ter uma noção conceitual mínima sobre os diversos métodos, procedimentos, fontes, tecnologias e técnicas através dos quais os serviços de inteligência coletam, analisam e distribuem informações?

Além de estabelecer pontos de partida para os demais capítulos, o texto que segue examina um problema específico: se a dinâmica operacional das atividades de inteligência é caracterizada por interações conflitivas entre atores que buscam suplantar os procedimentos de segurança do adversário e obter informações sem o seu consentimento ou conhecimento, como então essa dinâmica delimita as expectativas sobre a agilidade das atividades de inteligência no mundo contemporâneo?

### O que é inteligência?

Há dois usos principais do termo inteligência fora do âmbito das ciências cognitivas. Uma definição ampla diz que inteligência é toda informação coletada, organizada ou analisada para atender as demandas de um tomador de decisões qualquer. Para a ciência da informação, inteligência é uma cama-

da específica de agregação e tratamento analítico em uma pirâmide informacional, formada, na base, por dados brutos e, no vértice, por conhecimentos reflexivos. A sofisticação tecnológica crescente dos sistemas de informação que apóiam a tomada de decisões tornou corrente o uso do termo inteligência para designar essa função de suporte, seja na rotina dos governos, no meio empresarial ou mesmo em organizações sociais.<sup>2</sup> Nessa acepção ampla, inteligência é o mesmo que conhecimento ou informação analisada.<sup>3</sup>

Certamente é possível teorizar sobre a natureza da informação e sobre o impacto dos fluxos totais de informação na economia, no Estado e na vida social de modo geral.<sup>4</sup> Porém, a inteligência de que trata este livro refere-se a conjuntos mais delimitados de fluxos informacionais estruturados. Nesse caso, uma definição mais restrita diz que inteligência é a coleta de informações sem o consentimento, a cooperação ou mesmo o conhecimento por parte dos alvos da ação. Nessa acepção restrita, inteligência é o mesmo que segredo ou informação secreta.<sup>5</sup>

Mantive ao longo da pesquisa uma forte ancoragem na definição restrita de inteligência, aplicando-a ao estudo dos serviços governamentais que atuam nessa área. Ignorar a definição restrita implicaria perder de vista o que torna afinal essa atividade problemática. No mundo real, porém, as atividades dos serviços de inteligência são mais amplas do que a espionagem, e também são mais restritas do que o provimento de informações em geral sobre quaisquer temas relevantes para a decisão governamental. Isso coloca uma dificuldade muito concreta, não meramente semântica, para uma conceituação precisa da atividade de inteligência que permita diferenciá-la, simultaneamente, da noção excessivamente ampla de informação e da noção excessivamente restrita de espionagem.

Para superar essa discrepância entre a definição restrita e o leque de atividades concretamente desenvolvidas pelos serviços de inteligência, é preciso levar em conta uma segunda dimensão do conceito restrito de inteligência que tomarei como ponto de partida para este livro. Enquanto a primeira dimensão destaca os meios especiais utilizados para coletar informações sem a cooperação e/ou o conhecimento de um adversário, essa segunda dimensão é analítica e diz basicamente que a inteligência se diferencia da mera informação por sua capacidade explicativa e/ou preditiva. A combinação dessas duas faces ou dimensões fundamentais do conceito de inteligência traduz-se numa organização característica do processo de trabalho aí envolvido. Essa organização foi descrita de forma mais precisa por Michael Herman (1996) como um processo de trabalho seqüencial, separado entre um estágio de coleta, que é especializado segundo as fontes e meios utiliza-

dos para a obtenção das informações (*single-sources collection*), e um estágio de análise das informações obtidas a partir das diversas fontes singulares e de outros fluxos não-estruturados (*all-sources analysis*).<sup>6</sup>

Apesar da tensão potencial entre as duas dimensões do conceito (operacional e analítica), não me parece que as associações históricas entre inteligência e os aspectos mais ásperos da política sejam meramente idiosíncráticas, acidentais ou espúrias. A associação persistente entre inteligência e conflito é forte justamente porque as duas dimensões do conceito são indissociáveis na práxis das organizações encarregadas do provimento desse tipo de informação e conhecimento. Tanto as dificuldades práticas quanto os critérios para uma diferenciação da atividade que justifique essa associação entre inteligência e conflito podem ser demonstrados através de duas delimitações epistêmicas, cada uma delas baseada em uma das faces do conceito.

Em relação à dimensão analítica do conceito, a diferença entre as análises e estimativas elaboradas no âmbito das atividades de inteligência e quaisquer outras análises de órgãos de assessoramento técnico governamental está nos fins a que se destinam as análises de inteligência: aumentar o grau de conhecimento sobre os adversários e os problemas que afetam a segurança estatal e nacional (*situational awareness*). Diferentemente de institutos de geografia e estatística ou de centros de pesquisa econômica aplicada, serviços de inteligência estão voltados para a compreensão de relações adversariais, e por isso a maioria de seus alvos e/ou problemas é principalmente internacional e “difícil”. Inteligência lida 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. Os chamados serviços de inteligência de segurança (*security intelligence*) têm muitos alvos puramente domésticos, mas mesmo estes compartilham a condição de “outro” aos olhos do arcabouço constitucional e da ordem política constituída.<sup>7</sup>

O argumento aplica-se mesmo ao estudo de tendências, fatos e problemas não diretamente relacionados a um ator específico. Nem todos os problemas nacionais e internacionais possivelmente relevantes para um governo são adequadamente tratados por serviços de inteligência. Mesmo que a lista de temas sobre os quais as agências precisam informar seus usuários seja crescente, indo desde aspectos culturais de outras sociedades até detalhes sobre tecnologias de uso dual, novos itens deveriam ser incorporados à agenda de trabalho das agências de inteligência somente quando estas tivessem condições de “agregar valor” em áreas que não são de sua especialidade, mas nas quais suas fontes e métodos fossem julgados necessários pelos usuários civis e militares. Enfim, quanto mais ostensivas (públicas) as fontes de informação, quanto menos conflitivos os temas e situações, menos as análi-

ses de inteligência têm a contribuir para o processo de tomada de decisão governamental.<sup>8</sup>

Esse é um critério que realça o valor de uma definição restrita de inteligência. A fronteira do trabalho analítico em inteligência precisa ser traçada em relação a alguma conexão com a relevância dos conteúdos analisados para os processos de decisão governamental em política internacional, defesa nacional e provimento de ordem pública.<sup>9</sup>

Em relação à dimensão operacional do conceito, a diferença entre a coleta de informações para fins de produção de inteligência e outras operações governamentais que envolvem a aquisição sistemática de informações sobre atores e problemas relevantes para a segurança nacional é mais nebulosa, embora não impossível de ser traçada. Duas situações típicas em que se pode visualizar essa diferença são as próprias relações diplomáticas entre Estados e as operações militares.

Normalmente, os países mantêm relações diplomáticas, e cada Estado soberano permite que as representações formais dos demais Estados em seus territórios enviem relatórios para seus governos e países de origem. É certo que oficiais de inteligência usam cobertura diplomática, assim como é possível que certas fontes mais confidenciais dos embaixadores superponham-se às fontes dos espiões. Entretanto, as diferenças entre uma atividade e outra são relativamente claras, especialmente no que diz respeito ao grau de fragilidade das fontes diplomáticas ou secretas de informação em relação às contramedidas de segurança dos alvos. A maioria das fontes de um diplomata é ostensiva e não cessa o fluxo informacional quando o governo do país anfitrião aumenta seus procedimentos de segurança, o que tende a ocorrer com as fontes dos oficiais de inteligência. Basta dizer que diplomatas, adidos militares ou inspetores internacionais suspeitos de espionagem são declarados *personae non grata*, expulsos do país de hospedagem e devolvidos aos seus países de origem com base na Convenção de Viena sobre Relações Diplomáticas (1961). Os esforços de obtenção de informações conduzidos através de canais diplomáticos e de operações de inteligência são reconhecidos como diferentes pelos atores envolvidos, principalmente com base nos distintos meios utilizados.<sup>10</sup>

No caso das operações militares, talvez seja mais adequado falar de um *continuum* entre informações de combate e inteligência. Ainda assim, mesmo em situações de combate algumas especificidades marcam a atividade de inteligência. A mais óbvia é o grau de controle que as organizações de inteligência têm sobre cada tipo de fluxo informacional. No caso das informações de combate, trata-se normalmente daqueles dados obtidos em função do contato direto das tropas com o inimigo – e que são utilizados imediatamente para alerta operacional ou para a tomada de decisão sobre ações im-

diatas. Tais dados são controlados pelos *staffs* de operações (e não de inteligência) das estruturas de comando das forças. Ainda que alguns desses dados possam mais tarde ser integrados aos fluxos informacionais que alimentam a etapa de produção e disseminação de relatórios de inteligência, as chamadas informações de combate (*combat informations*) permanecem uma atividade distinta das atividades de inteligência.

Apesar de pragmático, nem sempre é fácil aplicar esse critério sobre quem controla os meios de coleta e os fluxos informacionais resultantes. Na Guerra do Golfo Pérsico de 1991, a coalizão sob mandato das Nações Unidas era apoiada por satélites e analistas norte-americanos controlados pela CIA e pelas agências de inteligência do Pentágono, além de contar com recursos comandados pelos *staffs* de inteligência no teatro de operações. Tanto o trabalho de inteligência quanto a gerência de informações de batalha dependiam fortemente dos sistemas de controle e comando aero-transportados, como os Awacs (Airborne Warning and Control Systems) e os Jstars (Joint Surveillance Target Attack Radar Systems), subordinados ao comando aliado no teatro de operações. Ou seja, com uma maior integração das operações militares conjuntas, o controle operacional de recursos específicos de inteligência e de informações de combate pode mudar de esfera de comando dependendo das necessidades, como no caso das unidades militares de coleta de inteligência tática empregadas eventualmente pela artilharia ou dos satélites que transmitem imagens e/ou decodificações processadas diretamente sob demanda dos comandantes de unidades no teatro de operações. Comunicações em tempo quase real e a crescente sofisticação dos recursos disponíveis para a obtenção de informações de combate (aquisição de alvos, alerta avançado e operações de guerra eletrônica) também contribuem para a criação de novas áreas de sombra entre inteligência e informações operacionais de combate, especialmente entre as áreas de inteligência de sinais e de operações de suporte de guerra eletrônica. Em particular, quando se trata de localização, identificação e produção de contramedidas às emissões eletromagnéticas dos radares e sistemas adversários, é muito difícil saber onde começa uma coisa e termina outra.

Mesmo assim, pode-se tentar diferenciá-las. Durante a II Guerra Mundial, por exemplo, a superioridade informacional foi um fator importante para o resultado das batalhas da Inglaterra e do Atlântico. Porém, na batalha da Inglaterra foram decisivas as informações de combate imediatamente produzidas pelos radares britânicos, enquanto na batalha do Atlântico o fator decisivo foi o esforço anglo-americano de longo prazo na decodificação de cifras e códigos secretos alemães na área de inteligência de sinais.<sup>11</sup> Recentemente, o conceito de guerra informacional (IW) passou a ser empregado para abranger tanto a obtenção e a negação de informações de combate

quanto a inteligência propriamente dita, mas trata-se ainda de uma mudança em curso.<sup>12</sup>

Do ponto de vista operacional, portanto, os critérios mais importantes para a distinção entre inteligência e outros tipos de aquisição de informações são o grau de intervenção humana requerido para a análise e a disseminação dos dados obtidos, associados ao grau de vulnerabilidade das fontes de informação às contramedidas de segurança e à consequente necessidade de segredo para a proteção das atividades de inteligência.<sup>13</sup>

Essas características analíticas e operacionais da atividade governamental de inteligência oferecem um ponto de partida para o estudo dos processos de institucionalização desses serviços no Estado contemporâneo. Mas é necessário avançar mais, e na próxima seção serão consideradas as etapas fundamentais do chamado ciclo da inteligência.

## O ciclo da inteligência

As descrições convencionais do ciclo da inteligência chegam a destacar até 10 passos ou etapas principais que caracterizariam a atividade, a saber:

1. Requerimentos informacionais.
2. Planejamento.
3. Gerenciamento dos meios técnicos de coleta.
4. Coleta a partir de fontes singulares.
5. Processamento.
6. Análise das informações obtidas de fontes diversas.
7. Produção de relatórios, informes e estudos.
8. Disseminação dos produtos.
9. Consumo pelos usuários.
10. Avaliação (*feedback*).

Entretanto, na maior parte desta seção serão destacadas basicamente as duas etapas fundamentais de coleta (*single sources*) e de análise (*all-sources*).<sup>14</sup>

A própria idéia de ciclo de inteligência deve ser vista como uma metáfora, um modelo simplificado que não corresponde exatamente a nenhum sistema de inteligência realmente existente. Por outro lado, essa falta de acuidade descritiva não é o que mais importa, pois a caracterização das atividades de inteligência enquanto um processo de trabalho complexo e dinâmico é importante para que se possa distinguir as mudanças qualitativas que a informação sofre ao longo de um ciclo ininterrupto e inter-relacionando de trabalho. A principal contribuição da idéia de ciclo de inteligência é justamente ajudar a compreender essa transformação da informação e explicitar a existência desses fluxos informacionais entre diferentes atores (usuários, gerentes, coletores, analistas etc.).

Como a atividade de inteligência é ela mesma uma função subsidiária dos processos de formulação, decisão e implementação de política externa, de defesa e segurança pública, pode-se pensar também o ciclo da inteligência como um subconjunto de atividades do chamado “ciclo das políticas públicas”: um ciclo formado pelo surgimento de problemas (*issues*), o esta-

belecimento de uma agenda, a formulação de políticas e linhas de ação alternativas, os processos de tomada de decisão, a implementação e a avaliação.<sup>15</sup> Nesse sentido, as informações que os serviços de inteligência coletam e analisam para os usuários deveriam ser determinadas pelas necessidades e prioridades daqueles mesmos usuários.

Idealmente, os responsáveis pela tomada de decisões, sejam eles políticos eleitos, ministros, altos burocratas civis, comandantes militares ou chefes de polícia, identificam lacunas e necessidades informacionais, estabelecem prioridades e as transmitem para os dirigentes da área de inteligência. Estes, por sua vez, transformam aquelas necessidades percebidas pelos usuários em requerimentos informacionais para os setores responsáveis pela coleta e análise.

Dado que mesmo os recursos dos países mais ricos são escassos, os responsáveis pelas diversas disciplinas de coleta precisam planejar a utilização dos meios técnicos e fontes humanas disponíveis para produzir a máxima sinergia possível e atender às demandas dos *policymakers*. O gerenciamento dos meios técnicos de coleta, dependendo das plataformas utilizadas (aviões, estações fixas de interceptação, satélites etc.), é uma atividade especializada e altamente complexa. É importante destacar essa diferença entre o planejamento geral da coleta de informações e o gerenciamento dos meios técnicos, principalmente porque a atividade de inteligência tende a ser cada vez mais um tipo de produção maciça, com algumas linhas de produção operando 24 horas e certos produtos sendo gerados praticamente sem interferência humana (nas áreas de *elint* e *masint*, por exemplo). As funções de direção, planejamento e gerenciamento constituem etapas preliminares e relativamente invisíveis (a despeito de sua importância) para o que costuma ser considerado tradicionalmente como inteligência: a coleta de informações (inclusive através de espionagem) e a produção de análises sobre temas e alvos.

Antes de passar para essas etapas mais visíveis do processo de trabalho em inteligência, é preciso acrescentar ainda um comentário. Um dos problemas com a metáfora de ciclo de inteligência é que muitos autores assumem acriticamente que o ciclo é completamente dirigido pelos requerimentos informacionais dos usuários finais. Isso é problemático justamente porque induz expectativas exageradas sobre o tipo de racionalidade que orienta os processos decisórios governamentais e sobre o próprio papel da inteligência.

Como lembram Michael Herman (1996:283-304) e Mark Lowenthal (2000:40-52), 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. Nesses casos, as listas de demandas tendem a ser genéricas (por exemplo, uma solicitação de informes sobre a “situação” na Colômbia), ou são formuladas

sem que os oficiais de inteligência tenham uma idéia precisa sobre a finalidade da informação no âmbito mais geral dos desafios enfrentados pelo governo (por exemplo, um requerimento sobre o desempenho dos helicópteros de transporte de tropas de um determinado fabricante russo, sem que se comunique à área de inteligência que aquele relatório é necessário para a tomada de decisão referente às alternativas de ação em relação ao conflito na Colômbia). Ou seja, a natureza incerta da política e a pressão de padrões de pensamento derivados das experiências passadas mais ou menos recentes tendem a tornar os “requerimentos” dos usuários algo muito menos estruturado do que a suposição inicial do modelo. Esses requerimentos formais legitimam e fornecem uma autorização para que as agências mobilizem seus meios para a produção de inteligência sobre determinado problema ou alvo, mas estão longe de ser o único fator a determinar o ciclo da atividade de inteligência.<sup>16</sup>

Caberia, portanto, aos responsáveis pela área de inteligência utilizar um conjunto de ferramentas organizacionais e analíticas para completar, detalhar e priorizar aquelas demandas, transformando-as em requerimentos informacionais mais efetivos. Embora seja imprescindível que as agências de inteligência atuem nessa especificação para evitar uma “falha de requerimentos” que comprometeria todo o ciclo, há aqui um risco evidente de “intromissão” e autonomização das agências em áreas que seriam prerrogativas dos usuários (*principals*). Mesmo levando em conta tais riscos, Michael Herman (1996:288) sustenta que um papel proativo das agências é preferível e compatível com a manutenção de um nível alto de responsividade, desde que acompanhado de procedimentos de avaliação sistemática da satisfação dos usuários com os produtos de inteligência recebidos e de mecanismos de controle externo.

Uma analogia freqüentemente utilizada na literatura é com as grandes empresas de notícias, tais como Reuters, Associated Press ou CNN. Assim como essas empresas, mas levando em conta as especificidades técnicas e políticas, as agências de inteligência seriam estruturadas a partir de um ciclo informacional governado simultaneamente por iniciativa (coleta e análise de informações que o órgão avalia que seriam úteis para o usuário – *pushes*) e responsividade (coleta e análise de informações solicitadas diretamente pelos usuários – *pulls*).<sup>17</sup>

Segundo Lisa Krizan (1999:13-20), mesmo com uma correta utilização de ferramentas voltadas para a identificação das necessidades dos usuários (ex.: taxonomia de problemas, listas de questões-chave e matriz de tempestividade e escopo), é preciso ter em mente que os fluxos informacionais associados aos requerimentos apresentam uma grande complexidade. Além de requerimentos estruturados a partir das necessidades dos diversos tipos de usuários finais e que são comunicados às agências de coleta pelos respon-

sáveis nacionais da área de inteligência, é preciso considerar ainda que muitos desses usuários comunicam suas necessidades diretamente às agências de coleta. E que os próprios analistas de inteligência solicitam não apenas informações sobre os requerimentos atuais dos usuários, mas também um leque mais amplo de informações necessárias para a atualização de bases de dados e/ou a compreensão mais ampla de alvos e problemas sobre os quais os analistas estão trabalhando. Finalmente, é preciso observar que as agências de coleta também trabalham a partir de oportunidades criadas por eventuais falhas de segurança dos adversários.<sup>18</sup>

Portanto, as limitações procedimentais, cognitivas e mesmo a escassez de recursos mostram que o chamado ciclo da atividade de inteligência depende muito mais da iniciativa das próprias agências de inteligência do que a metáfora de um ciclo iniciado e dirigido por requerimentos formais dos usuários indicaria à primeira vista. Afinal, como também destaca Mark Lowenthal (2000:42), as “falhas de requerimento” ocorrem não apenas quando os usuários são incapazes de transmitir suas necessidades com clareza, mas principalmente quando as agências falham em perceber as necessidades cambiantes dos usuários e não respondem de forma ágil, seja por inércia burocrática ou por incapacidade de interagir adequadamente com os *policymakers* e comandantes.

Seja como for, para além da questão dos requerimentos ainda estão os problemas relacionados aos recursos e meios de coleta, que afinal definem que informações podem ou não ser obtidas.

### *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. A maioria desses recursos é dedicada às plataformas, aos sensores e sistemas tecnológicos de coleta e processamento de informações, especialmente os satélites, no caso dos Estados Unidos, Rússia, China, França e outros poucos países que operam frotas desse tipo. O volume de dados brutos e informações primárias coletadas é muito maior do que os relatórios efetivamente recebidos pelos usuários finais. Segundo uma estimativa dos anos 1980, somente 10% das informações coletadas chegariam a sair dos muros dos sistemas de inteligência. Ocorre algo semelhante na indústria petrolífera, onde a estrutura de custos também reflete o risco e os investimentos mais pesados em prospecção e extração, enquanto o valor vai sendo agregado ao produto nas diversas etapas de refino.<sup>19</sup>

Os meios de coleta e as fontes típicas de informação definem disciplinas bastante especializadas em inteligência, que a literatura internacional designa

através de acrônimos derivados do uso norte-americano: *humint* (*human intelligence*) para as informações obtidas a partir de fontes humanas, *sigint* (*signals intelligence*) para as informações obtidas a partir da interceptação e decodificação de comunicações e sinais eletromagnéticos, *imint* (*imagery intelligence*) para as informações obtidas a partir da produção e da interpretação de imagens fotográficas e multiespectrais, *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. Além dessas disciplinas, que envolvem tanto fontes clandestinas quanto ostensivas, quando a obtenção de informações ocorre exclusivamente a partir de fontes públicas, impressas ou eletrônicas, essa atividade de coleta é então chamada de *osint* (*open sources intelligence*). Vejamos brevemente cada uma dessas disciplinas.<sup>20</sup>

### Humint

A fonte de informação mais antiga e barata consiste nas próprias pessoas que têm acesso aos temas sobre os quais é necessário conhecer. O acrônimo em inglês que designa essa disciplina (*humint*) é um eufemismo tipicamente norte-americano, incorporado ao jargão internacional porque evita o uso do termo *espionagem*, muito mais pesado do ponto de vista legal e político. O acrônimo também é utilizado para indicar que a inteligência obtida a partir de fontes humanas está longe de resumir-se aos arquétipos da espionagem.<sup>21</sup>

É preciso diferenciar basicamente dois tipos de atores nessa área: os oficiais de inteligência, ou seja, aqueles funcionários de carreira que trabalham para um serviço de inteligência e são responsáveis pelas operações de coleta de informações, e suas fontes, algumas das quais são agentes. Uma confusão bastante comum acontece porque tende-se a chamar ambos os atores relevantes de espiões. Embora a espionagem seja considerada crime grave em qualquer ordenamento jurídico contemporâneo, as penalidades para um oficial de inteligência estrangeiro dirigindo operações em território nacional são muito diferentes do que a pena por traição, aplicada a um cidadão ou residente permanente que esteja passando informações classificadas (*secretas*) para uma potência estrangeira.

Do ponto de vista das fontes, pode-se utilizar aqui a noção de “pirâmide” de sensitividade, quantidade e valor informacional na área de humint, desenvolvida há alguns anos por Michael Herman (1996:61-66). Segundo Herman, a profissionalização e o desenvolvimento de técnicas e habilidades específicas para obter sistematicamente informações de pessoas desenvolveram-se sistematicamente ao longo dos últimos 150 anos (nesse caso, o

*tradecraft* ou os “segredos do ofício” são algo literais). As atuais organizações civis e militares de humint são responsáveis pela espionagem propriamente dita, mas também por uma variedade de fontes não-clandestinas.

Na base da pirâmide de humint encontram-se as fontes menos glamourosas, com acesso às informações de menor sensitividade e valor isolado. Tais informações, no entanto, por sua abundância e informalidade, ajudam a montar o quebra-cabeça representado por um alvo ou problema. Serviços de inteligência e de segurança mantêm programas sistemáticos de entrevistas (*debriefings*) com pessoas que têm acesso a países ou áreas “negadas” ou difíceis, em relação às quais podem ser úteis as informações de turistas e viajantes ocasionais, especialistas acadêmicos, contatos de negócios ou mesmo refugiados e indivíduos oriundos de minorias oprimidas. Em situações de guerra, uma fonte importante de informações são as próprias populações de áreas ocupadas e os prisioneiros de guerra (POWs) interrogados pelas unidades de inteligência das Forças Armadas.<sup>22</sup> Em nenhum desses casos as fontes são agentes formais do serviço de inteligência, e tais programas tendem a ser conduzidos por outros oficiais da organização, não pelos responsáveis pelas operações de espionagem propriamente ditas. Porém, na medida em que se passa da exploração relativamente passiva do que as fontes já sabem para uma tentativa mais ativa de solicitar certos tipos de informações (*tasking*), isso significa certa progressão para cima na pirâmide. Nessa camada intermediária de fontes encontram-se os informantes *ad hoc*, exilados políticos, partidos de oposição etc. O grau de clandestinidade nos contatos com esse tipo de fonte pode variar, indo desde a abordagem formal para o provimento de uma informação específica até a manipulação das fontes e a obtenção de informações sem que o alvo tenha sequer consciência do relacionamento com um órgão de inteligência, muitas vezes disfarçado de contato jornalístico ou comercial.

No topo da pirâmide encontram-se as fontes secretas que transmitem regularmente informações que podem não ser muito numerosas, mas tendem a ser de maior valor agregado e de alta sensitividade. Esses agentes regulares, conscientes de que espionam seu próprio governo ou organização e fornecem informações mais ou menos vitais para a segurança nacional para serviços de inteligência estrangeiros, podem ser tanto agentes recrutados pelos oficiais de inteligência quanto pessoas que se voluntariaram para desempenhar tal papel (*walk-ins*). De modo geral, agentes voluntários são vistos com muita desconfiança por parte dos serviços de inteligência exterior, pois podem ser parte de operações dos serviços de contra-inteligência do país-alvo e ter como missão desinformar ou infiltrar o serviço de inteligência que o aceita. Por outro lado, uma desconfiança excessiva pode impedir o acesso a uma fonte bem situada.<sup>23</sup> Na verdade, os motivos pelos quais alguém começa a espionar para um adversário são bastante variados e mudam

ao longo do tempo. Concordância ideológica era um fator importante no recrutamento soviético de agentes em países da Otan até depois da II Guerra Mundial, mas a maioria dos agentes mais importantes para a União Soviética nas últimas décadas da Guerra Fria espionava por dinheiro. Um declínio relativo de rationalizações altruísticas e um peso crescente para compensações materiais tendeu a marcar os dois lados na medida em que a Guerra Fria avançou. Ambos os lados também utilizaram recorrentemente chantagem e pressão psicológica para recrutar agentes mais ou menos cínicos ou mais ou menos vulneráveis moralmente.<sup>24</sup> Finalmente, um dos tipos mais importantes de agentes é o chamado *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 até que seja apanhado ou possa evadir-se.<sup>25</sup> Embora os serviços especializados de humint tendam a focar sua atenção em fontes situadas no vértice dos processos decisórios e organizações mais importantes do adversário, a evidência histórica mostra que outras fontes situadas em posições menos centrais podem ser tão eficientes quanto e ainda garantir um fluxo de informações mais estável. Um exemplo eloquente do uso combinado dos dois tipos de agentes foi a infiltração realizada no governo da Alemanha ocidental por parte do serviço de inteligência exterior da Alemanha Oriental (HVA) até a década de 1970.<sup>26</sup>

Do ponto de vista dos serviços de inteligência responsáveis por dirigir os programas e agentes recrutados, é preciso diferenciar duas categorias básicas de oficiais de inteligência no exterior: aqueles que operam com “cobertura oficial” e os demais.

Cobertura oficial refere-se à integração dos oficiais de inteligência ao corpo diplomático da embaixada ou consulado, disfarçados de adido cultural, conselheiro político, técnico, assistente do adido militar, representante do Ministério da Agricultura, secretário ou qualquer outro cargo governamental que dê ao oficial uma desculpa para estar naquele país e também garanta imunidade diplomática em caso de detecção de suas verdadeiras atividades, pois a lei internacional obriga que esses oficiais sejam declarados *personae non gratum* e expulsos do país. Outras vantagens da cobertura oficial são o maior acesso às autoridades do país que está sendo espionado e a segurança fornecida pela embaixada e por consulados para que os oficiais de inteligência possam manter seus arquivos e se comunicar com o quartel-general de seu serviço no país de origem. O oficial mais graduado dirigindo as operações de inteligência num país estrangeiro chefia a “estação” (no jargão norte-americano, ou a *rezidentura*, no jargão russo) local de seu serviço de inteligência.<sup>27</sup> Pelo ângulo inverso, o uso excessivo de cobertura oficial facilita o trabalho das equipes de vigilância da contra-espionagem do país-alvo, limita os tipos de pessoas

com as quais os oficiais de inteligência podem ter contato sem levantar suspeitas e, em casos extremos nos quais as relações diplomáticas são interrompidas, isso desestrutura o trabalho de coleta de informações.

As vantagens do uso de oficiais “sem cobertura oficial” (NOCs, no jargão americano, ou “ilegais”, no jargão russo) estão localizadas na maior flexibilidade e eficiência das operações. Montando estórias de cobertura que podem relacionar-se a uma variedade de estratos sociais e profissionais (jornalistas, representantes comerciais, financistas, residentes estrangeiros de uma terceira nacionalidade, entomologistas, membros do clero, industriais, médicos etc.), os serviços de inteligência ampliam o leque de alvos possíveis para recrutamento de agentes e informantes e dificultam o trabalho de vigilância da contra-espionagem. Por outro lado, isso pode limitar o contato com o mundo oficial, expor os quadros do serviço a um risco muito mais elevado, sem contar que a cobertura não-governamental exige um tempo de maturação e treinamento muito maior, assim como requisitos logísticos e comunicacionais muito mais complexos.<sup>28</sup>

De modo geral, inteligência obtida a partir de fontes humanas (humint) não é apenas a forma mais antiga e barata de se obter informações secretas, mas também a mais problemática. Os problemas de gerenciamento vão desde a enorme pressão sofrida por agentes recrutados, não importa o tipo de motivação que os tenha levado a espionar, até as dificuldades associadas ao controle da credibilidade da fonte e da confiabilidade/acurácia das informações. Além dos riscos representados pelas operações de contra-espionagem dos adversários, que tentam neutralizar os agentes ou então controlá-los como agentes duplos, há um risco sempre presente nas próprias fontes, tentadas a preencher certos vácuos informacionais com informações fabricadas (*paper mills*). Além de riscos de segurança e dificuldades para controlar a qualidade das informações obtidas, outras características operacionais da área de humint são derivadas dos longos processos de identificação e recrutamento de agentes, das comunicações restritas entre agentes e seus controladores e de todas as limitações cognitivas e mnemotécnicas inerentes à observação humana direta.

Apesar dessas limitações, humint é insubstituível como fonte de informação. Especialmente quando se trata de descobrir as reais intenções de um ator, mensagens interceptadas (sigint) ou fotografias (imint) são evidências insuficientes. Documentos e explicações orais apresentam, ao menos potencialmente, um grau de comprehensividade que as outras disciplinas de coleta não conseguiram até hoje obter.<sup>29</sup> A espionagem é muitas vezes imprescindível para uma exploração eficaz de outras fontes de informações, como nos lembra o fato de que a obtenção de cópias dos livros de códigos e de materiais cifrados sempre ajudou a área de criptologia das organizações de sigint. Com base nesse traço organizacional flexível e especializado (*can do*), Michael

Herman (1996:65-66) destaca a tendência de as organizações especializadas em humint funcionarem como organizações multifinalitárias, indo desde a espionagem propriamente dita até o desenvolvimento pioneiro de novas formas de coleta de informações através de meios técnicos.<sup>30</sup>

## Sigint

A segunda disciplina mais antiga de coleta de informações é conhecida como inteligência de sinais ou sigint (*signals intelligence*). Historicamente, sigint originou-se de interceptação, decodificação, tradução e análise de mensagens por uma terceira parte além do emissor e do destinatário pretendido. Com o uso cada vez mais intenso de comunicações escritas para fins militares ou diplomáticos no mundo moderno, desenvolveram-se igualmente as disciplinas de criptografia (uso de códigos e cifras para garantir a inviolabilidade do conteúdo das mensagens) e de criptologia (decifração e/ou decodificação de mensagens interceptadas).<sup>31</sup>

Atualmente, a disciplina de inteligência de sinais divide-se em dois campos complementares, chamados de *comint* (*communications intelligence*) e de *elint* (*electronics intelligence*).

Inteligência de comunicações, ou comint, é 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 (a seguir). Além do acesso ao conteúdo das mensagens transmitidas, pode-se obter inteligência também monitorando os padrões de tráfego de mensagens entre diversos pontos (*traffic analysis*) e ainda através de técnicas de localização dos transmissores (*direction finding – DF*). Análise de tráfego e localização de transmissões são parte integrante da disciplina de comint.

Por sua vez, inteligência eletrônica, ou elint, é obtida através de interceptação, processamento e pré-análise de sinais eletromagnéticos não-comunicacionais, emitidos por equipamentos militares e civis, com exceção das emissões decorrentes de explosões nucleares, as quais caem na área de especialização de masint (ver a seguir). Os primeiros alvos das operações de elint foram os radares dos sistemas de defesa antiaérea na II Guerra Mundial. Com o desenvolvimento dos mísseis e a proliferação do uso de equipamentos eletrônicos ao longo da Guerra Fria, surgiram outros alvos prioritários para além dos vários tipos de radar, principalmente sistemas operacionais (aquisição de alvos, navegadores, detecção submarina, teleguiagem de armas etc.) e sistemas de comando, controle, comunicações e inteligência (C<sup>3</sup>I).

De acordo com Jeffrey Richelson (1999:182-185), a facilidade com que as comunicações e/ou os sinais eletrônicos podem ser interceptados e interpretados

depende de três fatores: o método de transmissão, as freqüências empregadas e o uso (ou não) de medidas defensivas de segurança, especialmente criptografia.

A forma mais segura de transmitir informações importantes é não transmiti-las, mas políticas de “silêncio de rádio” e programas de redução das emissões esbarram nas necessidades de comunicação de organizações complexas e em falhas humanas mais ou menos inevitáveis. Num nível menos exigente, comunicações através de cabos terrestres e marítimos, especialmente cabos de fibra óptica, também são mais seguras. A interceptação desse tipo de tráfego depende do acesso físico aos cabos (*tapping*), uma operação de baixa produtividade e custos muito altos, dificultada ao extremo no caso de cabos de fibra óptica. Por outro lado, 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 das medidas de segurança (*comsec*) e a necessidade de contramedidas eletrônicas (ECM) no caso dos sistemas militares. Em função dessas medidas, as organizações de sigint enfrentam agora não apenas recursos de criptografia e de *scrambling* mais sofisticados, disponíveis comercialmente, mas também uma variedade de tecnologias, técnicas e sistemas comunicacionais de uso militar e comercial que desafiam a interceptação e a decodificação.<sup>32</sup>

Apesar do uso crescente de comunicações corporativas através de redes locais (LANs) e regionais (WANs) de acesso relativamente mais difícil para os interceptadores, o volume de informações transmitido diariamente pelo ar através de bandas de freqüência diversas (ELF, VLF, LF, HF, VHF, UHF, SHF e EHF) e de meios (satélites, antenas de rádio etc.) que são passíveis de interceptação por sensores diversos simplesmente não tem termo de comparação e, além de gigantesco, também é igualmente crescente.<sup>33</sup>

Somente através da rede comercial de satélites Intelsat (International Telecommunications Satellite Organization) passam mais de dois terços de todo o tráfego telefônico internacional, praticamente todas as transmissões internacionais de sinais de televisão, bem como a maioria das transmissões de telex, dados digitalizados, fax, *e-mail*, vídeo e teleconferências. Dada a disparidade de meios na área de coleta de inteligência de sinais, a capacidade de países como os Estados Unidos e, em menor escala, os demais países europeus ocidentais da Otan, Rússia e China tende a ser muito superior do que a capacidade de os demais governos ou empresas garantirem a segurança de suas comunicações (*comsec*), mesmo com o barateamento das novas tecnologias de informação e comunicação (TICs).

Como foi amplamente divulgado durante as investigações do Parlamento europeu em 1999 sobre o chamado *Echelon*, somente a rede norte-ameri-

cana de 10 estações fixas de vigilância das comunicações globais via satélite interceptava um volume mensal de cerca de 100 milhões de mensagens, incluindo internet, telefonia fixa, telefonia celular, transferências bancárias, transmissões de fax e outros sinais.<sup>34</sup> Na verdade, considerando todos os outros sistemas e plataformas combinados, a capacidade de interceptação dos Estados Unidos é muito maior do que isso. Segundo Matthew Aid (2000:17-20), já em 1995 a agência central de sigint norte-americana (NSA) era capaz de interceptar um volume de sinais equivalente a todo o volume de informações da Library of Congress (um quatrilhão de *bits*) a cada três horas de operação de suas inúmeras plataformas e sensores no mundo todo.

Do ponto de vista dos governantes que utilizam tais recursos, portanto, o grande problema da área de sigint seria a falta de agilidade para processar volumes tão gigantescos de interceptações. As estimativas existentes para o caso dos Estados Unidos apontam para uma relação de 1 milhão de *inputs* para cada informação relatável. E as condições de processamento do volume de tráfego interceptado são ainda mais precárias do que a baixa proporção de material útil em relação ao volume total. Ou seja, enquanto a NSA conseguia processar 20% de tudo o que era interceptado na década de 1980, atualmente, a partir da explosão das novas tecnologias (TICs) nos anos 1990, a agência não seria capaz de processar mais do que 1% de todo o material interceptado. Processamento, decodificação, tradução, armazenamento, recuperação e disseminação de informações de sigint são áreas tão ou mais decisivas para investimento em pesquisa e desenvolvimento quanto o são as tecnologias, os sensores e plataformas de coleta.<sup>35</sup>

Especialmente nos casos norte-americano e russo, além de grandes estações terrestres de interceptação de comunicações, também são utilizados postos de escuta nas embaixadas em capitais estrangeiras (para interceptação de comunicações oficiais de curta distância, inclusive telefonia celular), centros regionais de operações subordinados aos principais comandos militares e ainda plataformas móveis, desde aviões e *drones* (UAVs) até navios e submarinos equipados com sensores e pessoal especializado na coleta de sigint.<sup>36</sup> Desde a década de 1960, porém, nenhuma plataforma é tão importante quanto os satélites de vigilância eletrônica e interceptação de comunicações. Essas grandes “orelhas”, ou “aspiradores de sinais”, começaram a ser postas em órbita espacial antes mesmo dos satélites de coleta de imagens, e constituem a maioria das frotas de satélites-espiões.<sup>37</sup> Basicamente, existem atualmente três tipos principais de satélites de sigint.

■ Os satélites para interceptação de sinais eletrônicos não-comunicacionais, lançados em órbitas circulares de baixa altitude, que são conhecidos como *ferrets*.<sup>38</sup> No caso dos Estados Unidos, as sucessivas gerações de constelações desse tipo de satélite deram lugar, na década de 1990, a uma tentativa

de consolidação de sistemas e missões com o que anteriormente era um programa separado de satélites de vigilância oceânica. Aumentando a altitude orbital para cerca de 1.126km e diminuindo o ângulo das órbitas circulares, os novos satélites de vigilância oceânica são capazes de interceptar sinais de radares, telemetria de mísseis de cruzeiro e outras emissões de navios e submarinos a partir de seus *scanners* e sensores passivos de microondas, infravermelho e freqüências de rádio. Segundo Jeffrey Richelson (1999:187), a partir de 1994 os Estados Unidos desenvolveram uma nova geração de satélites em órbitas circulares de baixa altitude para a vigilância eletrônica de alvos, tanto marítimos quanto terrestres.

» Os satélites de interceptação de comunicações utilizam órbitas geossíncronas e ângulos de inclinação do plano orbital em relação ao equador próximos de zero grau. As órbitas geossíncronas são atingidas a uma altitude de 35.875km. Como o período orbital aumenta dependendo da altitude, ao atingir aquela altitude o período orbital do satélite será de 1.436 minutos, próximo ou igual ao da Terra. Isso significa basicamente que um satélite em órbita geossíncrona parece estar estacionário sobre um ponto fixo acima do planeta, tornando-o ideal para a interceptação de sinais comunicacionais. Ao contrário dos satélites de baixa altitude, com períodos orbitais mais curtos, adequados à vigilância eletrônica, mas muito curtos para a interceptação de comunicações, os satélites geoestacionários são especialmente desenvolvidos para comint. Cada satélite em órbita geoestacionária cobre 42% da superfície terrestre, o que implica dizer que três satélites separados entre si por uma distância de 120° ao longo da órbita geoestacionária garantiriam uma cobertura permanente de quase todo o planeta.<sup>39</sup>

» Digo quase todo o planeta porque a cobertura, na prática, está restrita às regiões com latitude de 70° ao sul e ao norte. Acima dessas latitudes as órbitas geossíncronas proporcionam uma “visão” muito oblíqua da superfície terrestre nos círculos polares Ártico e Antártico, e os sinais comunicacionais são distorcidos pelo longo percurso através da atmosfera. Como a União Soviética/Rússia tem considerável massa terrestre e grande tráfego marítimo e aéreo ao norte dessa latitude, foram os soviéticos que primeiro utilizaram um tipo de órbita altamente elíptica (conhecido como *Molniya*) para otimizar seus sistemas de comunicação via satélite. Com uma inclinação de 63°, as órbitas elípticas têm uma altitude de 450km no perigeu e 40 mil km no apogeu, com um tempo orbital de cerca de 12 horas. Isso significa que o satélite passa pelo ponto mais distante da Terra duas vezes ao dia, uma sobre a região polar da Rússia e outra sobre a região polar do Canadá. Enquanto os russos utilizam essas órbitas altamente elípticas primariamente para suas comunicações e secundariamente para coleta de sigint, os Estados Unidos desenvolveram frotas

de satélites que também usam os mesmos parâmetros orbitais *Molniya* primariamente para interceptação de comunicações e sinais eletrônicos soviéticos/russos e, secundariamente, para comunicações e controle de missões de suas forças militares através do Pólo Norte.

Em 1998, o diretor do National Reconnaissance Office (NRO) dos Estados Unidos anunciou que sua agência estava desenvolvendo um novo sistema de satélites de coleta de sigint cujas arquitetura e tecnologias de processamento, combinadas com os novos sistemas de controle terrestre das missões desenvolvidas pela National Security Agency (NSA), permitiriam a substituição e a consolidação num único programa, já a partir de 2002/03, dos três tipos de satélites atualmente em órbita.<sup>40</sup>

Mesmo com uma diversidade relativamente menor de tipos de fontes do que a área de humint, as fontes da área de sigint também podem ser classificadas segundo uma pirâmide de sensitividade, quantidade e valor. Como lembra Michael Herman (1996:69-74), a ruptura dos códigos e cifras mais elevados de um adversário permite um acesso aos conteúdos comunicacionais de tráfegos de mensagens que, embora não muito volumosos, têm importância equivalente ao de agentes do topo da pirâmide em humint. Numa escala intermediária encontram-se as informações decorrentes da análise de tráfego e DF (*direction finding*), enquanto na base da pirâmide estão as comunicações sem codificação (*plain text*) e as mensurações de parâmetros de sinais eletrônicos. As comunicações tendem a ser transmitidas em “claro” quando os riscos de interceptação são considerados baixos, ou quando o valor para o adversário é potencialmente baixo, ou ainda quando os custos da utilização de criptografia são elevados. Embora sigint seja uma área em que há um confronto muito claro entre medidas ativas de obtenção de inteligência e medidas defensivas de segurança informacional, a mesma dinâmica marca, de um modo ou de outro, as demais disciplinas de coleta, especialmente a inteligência de imagens.

### Imint

Das três fontes de informações mais utilizadas na área de inteligência, a chamada área de inteligência de imagens, ou imint (*imagery intelligence*), é a mais recente. Embora evidências visuais tenham sido importantes para as operações militares desde muito antes da invenção da fotografia, o surgimento da área de imint como uma disciplina especializada de coleta de informações é posterior ao uso da aviação militar para reconhecimento e vigilância, durante e após as duas guerras mundiais do século XX. Imagens fotográficas, imagens televisionadas e outros tipos de evidências visuais também são obtidos por oficiais de inteligência, patrulhas de reconhecimento e

equipes de vigilância em terra e no mar. Porém, o desenvolvimento de imint como uma disciplina especializada de coleta de informações deu-se fundamentalmente a partir da associação entre o uso de câmeras fotográficas e plataformas aeroespaciais.<sup>41</sup>

Segundo William Odom (1997:79) e Jeffrey Richelson (1999:150), as raízes históricas da coleta e do uso de evidências visuais para a produção de inteligência remontam aos desenhos feitos por oficiais militares em missões de reconhecimento. Tanto o mapeamento cartográfico quanto o desenho (do terreno, panoramas, fortificações, portos etc.) historicamente fizeram parte das habilidades necessárias para o planejamento e a execução de operações militares. Entretanto, as atuais plataformas aeroespaciais para a coleta de evidências visuais têm antecessores mais recentes na companhia de *aerostiers* (balonistas) organizada pelos franceses depois da Revolução de 1789, ou nas tentativas semelhantes de utilização de balões para missões de reconhecimento feitas pelas tropas da União durante a guerra civil norte-americana de 1861/65 e, mais ao final do século XIX, pelos exércitos britânico e alemão. A partir da I Guerra Mundial, câmaras fotográficas passaram a ser instaladas em aviões enviados em missões de reconhecimento. O maior alcance das aeronaves na época da II Guerra Mundial permitiu uma utilização mais arrojada dos vôos de reconhecimento aero-fotográfico, com cobertura do próprio território inimigo. Utilizando câmaras, filmes e lentes cada vez mais aperfeiçoados para fotos verticais e oblíquas, montadas em aeronaves de caça e bombardeiros adaptados, foi possível uma exploração mais intensa e sistemática de evidências visuais na produção de inteligência.<sup>42</sup> Com o aprofundamento da Guerra Fria depois de 1945, a natureza do território da União Soviética e a falta de acesso a outras fontes de informação (ex.: humana e ostensiva) levaram os Estados Unidos a intensificar as missões aero-fotográficas de grande altitude sobre o território soviético e na sua periferia mais imediata. O desenvolvimento de sistemas e plataformas especializados na coleta de inteligência de imagens acrescentou desde então uma camada específica à dinâmica competitiva e conflitiva que marcaria a Guerra Fria entre Estados Unidos e União Soviética.<sup>43</sup>

Os riscos diplomático-militares derivados da violação do espaço aéreo de nações soberanas em tempo 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. Até 1960, porém, os Estados Unidos utilizaram vários tipos de aeronaves para missões clandestinas de reconhecimento sobre o território soviético, especialmente porque durante algum tempo os aviões especializados U-2s, de alta velocidade, alcance e altitude, eram inalcançáveis pelos interceptadores soviéticos. Embora esses aviões tenham sido e ainda

sejam utilizados em uma variedades de lugares e missões, o episódio da derubada de um deles por caças soviéticos em 1960 foi o marco de uma nova etapa no desenvolvimento da área de imint.<sup>44</sup> No começo daquela década os Estados Unidos e, logo depois, a União Soviética conseguiram pela primeira vez orbitar satélites-espiões capazes de sobrevoar os territórios adversários e fotografar alvos numa escala impensável com os sistemas até então disponíveis.<sup>45</sup>

A despeito do alto grau de segredo que cerca os programas militares de satélites de imagens, entre 1967 (quando foi assinado o Outer Space Treaty) e 1992 (quando foi assinado o Open Skies Treaty), o restrito clube das potências que dispõem de capacidade de coleta de imint a partir de plataformas espaciais aceitou mais ou menos tacitamente a inevitabilidade desses sobrevôos. Com recursos muito mais limitados do que aqueles de que dispõem os Estados Unidos e a Rússia, esses países incluem (ou passarão a incluir nos próximos anos) França, Japão, Índia, China, Israel, África do Sul, Canadá, Coréia do Norte e Taiwan. Ao longo das três últimas décadas, algumas das vantagens técnicas e políticas dos satélites alcançaram mesmo os países que não têm frotas próprias, na medida em que se tornaram disponíveis imagens vendidas comercialmente com melhor resolução.<sup>46</sup> De modo geral, dois desenvolvimentos contribuíram para tornar a disciplina de imint cada vez mais central para a dinâmica operacional das atividades de coleta de inteligência.

Em primeiro lugar, os satélites de imagens podem sobrevoar o território de um país sem que isso seja considerado pela lei internacional uma violação do espaço aéreo nacional. Basicamente, satélites de imagens movimentam-se em órbitas circulares de altitude relativamente mais baixa do que os satélites de sigint (ex.: os satélites de imint norte-americanos conhecidos como KH-11 Advanced operavam com 241km de perigeu e 965km de apogeu). Em órbitas circulares, a altitude orbital é definida segundo as necessidades de maior precisão das imagens coletadas ou de maior amplitude de área a ser coberta em cada passagem periódica sobre as mesmas áreas de interesse. Lançando os satélites com uma inclinação de cerca de 98º em relação ao plano orbital da Terra, pode-se rotar a órbita gradualmente ao longo do ano para compensar o efeito da passagem da Terra em torno do Sol. Isso garante que as imagens fotográficas sobre uma região serão obtidas sempre com as mesmas condições de luz solar, auxiliando o trabalho de fotogrametria e interpretação. As sucessivas gerações de satélites de imint foram aperfeiçoadas em relação ao tempo de permanência em órbita, à flexibilidade para o ajuste de parâmetros orbitais, aos sistemas de transmissão de dados e em relação à carga útil (*payload*).<sup>47</sup>

Enquanto os primeiros satélites registravam suas imagens em filmes que, uma vez expostos, eram ejetados e precisavam ser recolhidos depois de

sua reentrada na atmosfera, com a utilização de sistemas ópticos digitais a partir da década de 1980 as fotografias e outras imagens digitais passaram a ser transmitidas automaticamente para estações de controle em terra, diretamente ou através de satélites de comunicação em órbitas intermediárias. Isso permitiu o aumento da vida útil dos satélites e maior agilidade no ciclo de coleta e processamento. Depois da Guerra do Golfo de 1990/91, houve intensa discussão no Congresso norte-americano sobre a viabilidade de se transmitir diretamente e em tempo real as imagens de satélites para os comandantes de unidades terrestres, para aviões de combate e navios de guerra atuando no teatro de operações. Finalmente, é importante destacar uma vez mais que a amplitude da área coberta pela passagem de um único satélite de imagens corresponde a várias missões de esquadrões inteiros de aviões especializados operando em condições ideais.<sup>48</sup>

Em segundo lugar, vale esclarecer que a importância crescente da coleta de imagens para a produção de inteligência é determinada também pelo aperfeiçoamento tecnológico das câmaras, lentes, sensores e sistemas utilizados numa variedade de plataformas, especialmente os satélites. Aperfeiçoamentos ópticos nas lentes e câmaras fotográficas aumentaram enormemente a precisão e a amplitude das fotografias analógicas e digitais, que hoje abarcam centenas de quilômetros quadrados de área e têm resolução definida na escala de centímetros.<sup>49</sup> Além de explorar os limites da luz visível ao olho humano no espectro eletromagnético, a área de coleta de imagens também passou a utilizar sensores para a produção de imagens a partir de outras porções do espectro.

Como as imagens baseadas na luz visível ou nas porções próximas ao infravermelho dependem do reflexo da radiação solar nos objetos e não do registro das radiações emitidas pelos próprios objetos, as imagens resultantes de sensores ópticos só podem ser produzidas sob a luz do dia e, no caso das plataformas aeroespaciais, em condições meteorológicas favoráveis, com poucas nuvens. A partir do final da década de 1980, classes adicionais de satélites de imint norte-americanos e soviéticos/russos passaram a contar com novos sensores que registram imagens a partir do calor emitido pelos objetos (infravermelho), tornando-os operacionais também durante a noite, e ainda com sensores que formam imagens a partir do uso de radares de abertura sintética (SAR). Embora com uma resolução pior do que aquela possibilitada por sensores eletroópticos e termais, o uso de radares para a formação de imagens a partir de satélites tem como grande vantagem o fato de que as ondas de rádio não são atenuadas pelo vapor d'água presente na atmosfera, o que permite que tais sensores sejam empregados mesmo sobre alvos e regiões encobertos por nuvens.<sup>50</sup>

Como informa Jeffrey Richelson (1999:152), a coleta simultânea de imagens de um mesmo alvo por sensores operando em múltiplas bandas

discretas do espectro eletromagnético (MSI, ou *multispectral imagery*) permite uma exploração sinérgica dessas evidências visuais. Além disso, também é possível empregar sensores que operam em bandas espectrais contíguas incluindo luz visível, infravermelho, termoinfravermelho, ultravioleta e ondas de rádio (HSI, ou *hyperspectral imagery*). Os dados produzidos por esses sistemas de coleta permitiriam a identificação de forma, densidade, temperatura, movimento e composição química dos objetos.<sup>51</sup> Supõe-se que a complexidade técnica seja ainda proibitiva e que os recursos disponíveis para a exploração desse tipo de imagens sejam restritos mesmo no caso das potências centrais, o que talvez explique por que a literatura tende a incluir MSI e HSI como parte da disciplina de masint, não de imint.

A despeito da crescente importância do reconhecimento e da vigilância a partir de plataformas aeroespaciais para a produção de evidências visuais (mapas, fotografias e outros tipos de imagens), existem algumas limitações extrínsecas e intrínsecas à utilização de imint como fonte de informações para a produção de inteligência.

A principal limitação externa são os custos de obtenção. Com observou William Burrows (1999:17), com um custo de alguns bilhões de dólares para desenvolver e lançar satélites de coleta de imagens com resolução aproximada de 10cm, esse é um tipo de investimento que poucos países podem fazer. Mesmo aqueles que podem necessitam avaliar cuidadosamente suas percepções de ameaça e prioridades na área de defesa nacional e política externa. Mesmo que o acesso a fotos comerciais com resolução igual ou inferior a um metro tenha sido facilitado pelo final da Guerra Fria e pela “guerra de preços” entre Rússia, Europa e Estados Unidos (afinal, sensoriamento remoto é um mercado estimado em US\$17 bilhões para a década de 2000), os controles de segurança nacional ainda existem, e o acesso às imagens é regulado pelos interesses dos governantes dos países que têm frotas de satélites.

Do ponto de vista das limitações intrínsecas à área de imint, Michael Herman (1996:76-77) destaca três aspectos importantes. Em primeiro lugar, mesmo com a utilização cada vez mais intensa de software para processamento de imagens, fotogrametria e identificação automatizada de alvos, a interpretação das imagens obtidas por satélites, aviões e drones é uma atividade essencialmente humana, que demanda pessoas com habilidades especiais, cuja formação é demorada e artesanal.<sup>52</sup> Em segundo lugar, por mais precisas que sejam as imagens e por mais ampla que seja a cobertura dos sistemas de reconhecimento, trata-se principalmente de fotografias e outros tipos de imagens fixas, uma vez que as plataformas atuais estão sujeitas a um *trade-off* entre a quantidade de passagens sobre uma mesma coordenada e a amplitude da cobertura. Mesmo que drones e sistemas espaciais integrados com um número maior de satélites mais simples possam prover

vigilância permanente sobre determinados alvos em movimento (imagens televisivas), este ainda é um recurso limitado mesmo para os Estados Unidos e a Rússia. O terceiro e mais importante aspecto limitador do alcance da disciplina de imint decorre do fato trivial de que, independentemente da sofisticação de sistemas, lentes, antenas, plataformas e mesmo da habilidade dos fotogrametristas e intérpretes, não se pode ver o que está escondido ou ainda não foi construído. Grandes alvos fixos ainda são os mais vulneráveis e suscetíveis à vigilância dos sistemas de imint.<sup>53</sup>

Embora esse tipo de limitação resultante das contramedidas de segurança tomadas por um adversário seja comum a todas as disciplinas de coleta (no caso de imint, trata-se principalmente da camuflagem ou, como é corrente chamá-la a partir da grande *expertise* acumulada pelos russos, da arte da *maskirovka*), na área de imint isso é mais dramático justamente em função da expectativa de que a “revolução da imagem” desencadeada a partir da década de 1970 poderia tornar os adversários “transparentes” para os serviços de inteligência das superpotências. Na verdade, até aqui as novas capacidades de coleta e de contramedidas acrescentaram apenas vários níveis de complexidade à dinâmica operacional que opõe inteligência e segurança, tema sobre o qual se deverá discutir um pouco mais adiante. Antes, porém, será necessário fazer um brevíssimo comentário sobre as áreas de masint e osint, bem como sobre a etapa de análise e disseminação dos produtos no ciclo da atividade de inteligência.

## Masint

Na verdade, a área conhecida como inteligência derivada de mensuração e “assinaturas” (masint, ou *measurement and signature intelligence*) está longe de ter a mesma coerência que têm as três disciplinas de coleta mais tradicionais. O uso do termo vem se generalizando nos Estados Unidos desde 1986, como uma tentativa de classificar e agrupar uma série de atividades, programas e sensores especializados que não eram facilmente acomodados nas práticas mais estabelecidas de coleta de evidências visuais ou comunicacionais a partir do uso de meios técnicos. A unificação desse conjunto de atividades sob uma mesma rubrica deveu-se muito mais a uma necessidade organizacional do que a algum traço em comum entre os fenômenos observados, ou mesmo entre os meios técnicos utilizados para monitorá-los.<sup>54</sup>

No contexto norte-americano, fazem parte da área de masint desde 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 su-

perfície terrestre e no espaço, pelo registro e análise de radiações não-intencionais emitidas por equipamentos eletrônicos e radares e, para ficar por aqui, pela coleta e análise físico-química de materiais (efluentes, partículas, resíduos, partes de equipamentos estrangeiros etc.).

Segundo Jeffrey Richelson (1999:214-240), pelo menos três tipos de satélites norte-americanos carregam sensores dedicados à coleta de masint:

- os satélites do Defense Support Program (DSP) são equipados com sensores infravermelhos (diferentes dos sensores utilizados para a produção de imagens) capazes de detectar o lançamento e monitorar a trajetória de mísseis balísticos; os dados derivados desses sensores permitem a identificação dos tipos de combustíveis utilizados e das assinaturas espectrais associadas a diferentes sistemas de mísseis; em tese, quaisquer eventos terrestres que gerem suficiente radiação infravermelha para ser detectada do espaço podem ser mensurados e identificados pelos sensores dos satélites DSP;
- os satélites Navstar Global Positioning System (GPS) são equipados com sistemas de detecção de explosões nucleares (Nudet); embora a missão primária dos satélites Navstar seja prover dados precisos sobre localização para fins de aquisição de alvos e navegação, a órbita quase circular de 17,7 mil km de altitude da constelação de 21 satélites Navstar fez com que o Pentágono a utilizasse também para o monitoramento global de detonações nucleares, que podem ser detectadas por sensores de raios X, raios gama e pulso eletromagnético;
- também os satélites meteorológicos de uso militar (DMSP) são equipados com sensores para radiação eletromagnética e *tracking* de fragmentos de explosões nucleares na atmosfera.<sup>55</sup>

Além de sensores instalados em espaçonaves, outros meios técnicos utilizados pelos Estados Unidos para a coleta de masint envolvem plataformas aerotransportadas para a detecção e o recolhimento de amostras de agentes químicos e bacteriológicos na atmosfera, estações fixas para vigilância de mísseis (tais como a estação de radar *phased array* Cobra Dane, localizada na ilha Shemya, no Alasca), laboratórios sismológicos do centro de inteligência técnica da Força Aérea, radares passivos embarcados em navios de guerra, para monitoramento de veículos espaciais de reentrada, redes submarinas de hidrofones para monitoramento acústico de submarinos e de espaçonaves sobrevoando o oceano etc.<sup>56</sup> Infelizmente, as poucas informações disponíveis sobre a natureza das atividades de masint dizem respeito a esse país. Tal diversidade de meios de coleta e tipos de dados coletados decorre não apenas da complexidade técnico-científica dos fenômenos observados, mas também da própria escala das operações e das forças militares dos Estados Unidos.

Uma das principais funções da área de masint é a coleta de informações sobre características singulares – as assinaturas – de sistemas de armas,

veículos de combate, aeronaves, embarcações e radares para a montagem de bancos de dados e posterior emprego em sistemas de aquisição de alvo, ou para a produção de inteligência militar e o monitoramento de tratados internacionais, especialmente na área nuclear.

## Osint

A disseminação de bases eletrônicas de dados públicas e privadas, acessíveis via internet, aumentou imensamente o papel da coleta de inteligência a partir de fontes ostensivas mais ou menos especializadas. A chamada inteligência de fontes ostensivas, ou osint (*open sources intelligence*), sempre foi importante para qualquer sistema governamental de inteligência, mas há um razoável consenso na literatura de que sua importância cresceu recentemente no contexto da chamada “explosão informacional” da última década.<sup>57</sup>

De modo geral, osint 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 (jornais, rádio e televisão), 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. Quanto mais abertos os regimes políticos e menos estritas as medidas de segurança de um alvo para a circulação de informações, maior a quantidade de inteligência potencialmente obtida a partir de programas de osint.

Mesmo sob condições mais restritivas de segurança, o volume de informações ostensivas disponíveis tende a ser muito alto. Por exemplo, sabe-se atualmente que durante a Guerra Fria um programa conjunto da CIA e da US Air Force resumia e/ou traduzia inteiramente a maioria das publicações tecnocientíficas da União Soviética. Já em 1956, isso significava o resumo/tradução do conteúdo de 328 periódicos científicos e cerca de 3 mil livros e monografias por ano. Com o final da Guerra Fria, a aceleração da globalização e o advento das novas tecnologias de informação e comunicação (TICs), a disponibilidade de fontes ostensivas aumentou enormemente. De acordo com declarações do então *deputy director of central intelligence*, em 1992 o serviço de vigilância de mídia estrangeira da CIA (o Foreign Broadcast Information Service – FBIS) monitorava 790 horas semanais de programação de TV em 50 países e 29 línguas diferentes. As estações de monitoramento do FBIS eram então localizadas em lugares tão diferentes quanto Abidjá, Amã, Assunção, Bangcoc, Cidade do Panamá, Hong Kong, Islamabad, Key West, Londres, Mbabane, Nicósia, Okinawa, Seul, Tel Aviv e Viena. Além de publicações tecnocientíficas e mídias convencionais, em 1997 os programas de osint da CIA e da DIA já dispunham de acesso co-

mercial a cerca de 8 mil bases de dados eletrônicas via internet, além da assinatura de 2 mil periódicos eletrônicos.<sup>58</sup> No caso dos Estados Unidos, os principais programas e escritórios responsáveis pela coleta de informações ostensivas são as próprias agências e os departamentos encarregados da etapa de análise no ciclo de inteligência.

Aliás, uma característica comum a todas as disciplinas de coleta de inteligência discutidas nesta seção é a quantidade significativa de trabalho envolvida no processamento e pré-análise de volumes crescentes de informação. As agências de coleta são obrigadas a processar volumes crescentes de informações, tais como dados de telemetria e sinais eletrônicos, processamento digital de fotos e imagens, decodificação de mensagens, tradução de materiais em língua estrangeira etc. Mesmo o teste sistemático da confiabilidade e da acuidade das fontes humanas precisa ser feito antes que os relatórios de humint sejam encaminhados para os setores responsáveis pela análise e disseminação. Além da desproporção entre a quantidade de dados brutos coletados e a capacidade de as organizações processarem de forma ágil as informações, uma consequência adicional desse fenômeno é que alguns tipos de informações efetivamente produzidos ainda na etapa de coleta, especialmente as mais efêmeras e de uso diplomático ou militar imediato, precisam ir direto para os usuários finais sem passar pela etapa de análise e produção final (*all-sources analysis*).

Mesmo considerando essa etapa de processamento e pré-análise, pode-se concordar com a afirmativa de Michael Herman (1996), segundo a qual os coletores são especialistas em “disciplinas”, com suas fontes, tecnologias e técnicas peculiares e únicas, enquanto analistas são especialistas em temas, áreas e problemas. Os analistas têm a responsabilidade de avaliar as evidências obtidas sobre esses temas e problemas, produzir relatórios e informes, e disseminá-los para os comandantes militares e os governantes. Essa é parte do ciclo da inteligência que será comentada a seguir.

### *Análise e disseminação*

A atividade de análise e produção de inteligência assemelha-se ao que fazem outros sistemas de informação que apóiam decisões governamentais em pelo menos um aspecto: na necessária separação entre a produção de conhecimento relevante para a decisão e a defesa de uma alternativa específica de curso de ação (*policy advocacy*). Obviamente, isso é muito mais uma prescrição normativa do que uma realidade nos processos de tomada de decisão governamental.<sup>59</sup> Ainda assim, essa e outras instituições especializadas no provimento de informações e na produção de conhecimento não justificariam sua existência se isso fosse a mesma coisa que o aconselhamento, o planejamento ou a formulação e a execução de políticas.<sup>60</sup>

Nesse sentido, o *ethos* profissional da atividade de análise em inteligência e suas regras de produção de conhecimento são os mesmos que governam qualquer outra atividade de pesquisa. Também como em qualquer outra atividade desse tipo, os serviços de inteligência podem cair bem abaixo dos padrões esperados de isenção, relevância e qualidade das análises produzidas.<sup>61</sup>

Por outro lado, os problemas sobre os quais são elaboradas as análises variam conforme as necessidades dos usuários. Há várias formas de classificar tais necessidades e os tipos de inteligência resultantes. Tais classificações variam um pouco conforme o país e mesmo conforme o foco na área de análise, produção ou disseminação.<sup>62</sup>

Um dos mais influentes autores norte-americanos nessa área, o ex-professor da Universidade de Yale e ex-diretor do Office of National Estimates da CIA, Sherman Kent (1949), por exemplo, dividia os produtos analíticos segundo a função esperada e o foco temporal (presente/passado/futuro). Resultava desse critério uma separação entre inteligência sobre fatos correntes (chamada de relatorial), inteligência sobre características básicas e estáveis dos alvos (chamada de 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 chamado de alerta (*warning intelligence*). A tipologia de Kent ainda é empregada em muitos livros e documentos governamentais.<sup>63</sup>

No entanto, as categorias de trabalho mais utilizadas convencionalmente na área de análise e produção de inteligência ainda são organizadas segundo disciplinas acadêmicas, dividindo os produtos finais em, por exemplo, inteligência política (ex.: como os militares russos reagirão à expansão da Otan para o Leste europeu?), militar (ex.: como funcionam os sistemas de aquisição de alvo das novas armas antibalísticas norte-americanas em desenvolvimento?), científica e tecnológica (ex.: quais as prioridades atuais de pesquisa em sistemas ópticos e lasers direcionais nos 10 principais laboratórios europeus?), econômica (ex.: quais as consequências da reestruturação do sistema bancário japonês para as decisões de investimento dos países do Leste asiático?) e mesmo sociológica (ex.: como a composição demográfica e religiosa do norte do Cáucaso condiciona as chances de o fundamentalismo wahabita expandir-se no flanco sul da Rússia?).

Do ponto de vista dos alvos das operações de inteligência, eles costumam ainda ser divididos em transnacionais (terrorismo, crime organizado etc.), regionais (África Austral, União Européia etc.), nacionais (Estados Unidos, China etc.) e subnacionais (grupos militantes armados etc.).

Segundo autores como David Kahn (1995) e Michael Herman (1996), a diferença crucial dar-se-ia justamente entre as análises produzidas sobre as “coisas” e as “capacidades” e a inteligência sobre os “significados” e as “in-

tenções". Os diferentes meios de coleta e os distintos métodos de análise seriam mais ou menos adequados a cada um desses tipos de inteligência. Por exemplo, uma foto de satélite pode fornecer uma evidência forte e irrefutável sobre a localização precisa de um porta-aviões, mas somente a interceptação e a decodificação de suas comunicações podem fornecer uma forte indicação *ex ante* sobre qual é sua missão.

Na prática, porém, a maioria dos meios de obtenção e procedimentos de análise de informações lida com os dois tipos de inteligência ao mesmo tempo. Na área de inteligência de sinais, por exemplo, quando o sistema de C<sup>3</sup>I (comando, controle, comunicações e inteligência) de uma força armada é penetrado, isso garante acesso ao conteúdo das mensagens, mas também permite localizar materialmente a ordem de batalha do inimigo através da identificação dos emissores (*direction finding*) e do mapeamento dos parâmetros dos sinais. Aliás, de modo geral, mensagens interceptadas fornecem informações sobre intenções e significados (ordens transmitidas, planos, requisições, relatórios etc.), mas também sobre capacidades e coisas (equipamentos, logística, desempenho operacional etc.). Mas isso não quer dizer de modo algum que inteligência de sinais (sigint) seja intrinsecamente superior à inteligência de imagens (imint).

O que existe são diferentes tipos de adaptabilidade a inferências analíticas e, consequentemente, uma maior afinidade entre certas disciplinas de coleta e certas áreas de análise. Por exemplo, quando a questão analítica relevante é saber se um determinado governo possui ou não ogivas químicas, amostras ou pelo menos fotos das mesmas são evidências mais fortes do que mensagens interceptadas do Estado-maior mencionando sua existência. Por outro lado, a vulnerabilidade da inteligência de sinais às contramedidas defensivas de um alvo é maior do que a da inteligência de imagens. Uma força-tarefa naval atravessando um oceano para fazer um ataque de surpresa pode observar silêncio de rádio ou aumentar o nível de segurança de sua criptografia, mas não pode esconder-se facilmente de operações de reconhecimento aéreo, especialmente de um inimigo que disponha de cobertura de satélites para vigilância oceânica. Por isso é que se diz que a adaptabilidade das diferentes fontes de inteligência a inferências depende dos problemas analíticos a serem resolvidos.

Enfim, o próprio esforço de categorizar a atividade de inteligência deve ser visto ao mesmo tempo como uma necessidade administrativa e um imperativo epistemológico. Para dar uma idéia de como os países da Otan alocaram recursos em inteligência na década de 1990, Michael Herman (1996:54) organizou a seguinte hipótese de trabalho por categoria de investimento, e não por volume de produção: inteligência de defesa, para suporte às operações militares (SMO), suporte ao projeto de força, monitoramento das dinâmicas internacionais de armamentos e proliferação nuclear, cerca de 35%. Vigilância de conflitos internacionais e insurgências, cerca de 15%. Inteligência so-

bre a política interna de outros países, bem como suas respectivas políticas externas, inclusive econômicas, cerca de 20%. Suporte tático para negociações diplomáticas bilaterais, fóruns econômicos multilaterais e outras negociações internacionais, cerca de 10%. Inteligência externa e interna sobre terrorismo, cerca de 10%. Contra-inteligência, subversão e narcotráfico, 10%. Supondo-se que essa alocação hipotética reflita – ainda que remotamente – a realidade dos requerimentos e produtos informacionais dos países da Otan, ela indica uma grande continuidade – a despeito da retórica oficial sobre as novas ameaças – da agenda de segurança nacional dos países centrais do sistema internacional no imediato pós-Guerra Fria.<sup>64</sup>

Mas, voltando ao problema das dinâmicas operacionais e fluxos informacionais na atividade de inteligência, de modo geral essa etapa da análise pode ser vista como um “funil” que recebe informações de fontes diversas, não necessariamente e nem principalmente secretas, analisa e produz a inteligência propriamente dita. Os produtos finais vão desde sumários diários/semanais sobre temas correntes até estudos mais aprofundados sobre tendências e problemas delimitados a partir de critérios espaciais ou funcionais. Além de avaliar tendências e tentar descrever a realidade, os produtos de inteligência visam também a antecipar eventos cruciais, tanto fornecendo alerta avançado quanto contribuindo para a formulação de políticas, planos operacionais e projetos de força. As bases de dados e a produção de inteligência para referência (bancos biográficos, de “assinaturas” de sistemas de armas, vetores e plataformas, de dados cartográficos e de elevação de terreno etc.) constituem uma camada intermediária e fundamental, que alimenta tanto os produtos analíticos de consumo mais imediato quanto as estimativas e os estudos mais estruturados e voltados para o médio e o longo prazos. Costuma-se dizer que a qualidade das bases de dados e o grau de preparação dos próprios analistas são os principais indicadores da qualidade de uma organização de inteligência.<sup>65</sup>

Uma vez produzidas as análises, elas são disseminadas para os diversos usuários finais, responsáveis pela tomada de decisões e pelo planejamento e execução de políticas. Feito isso, nada garante que os relatórios de inteligência terão qualquer impacto sobre as decisões tomadas ou não tomadas. Um ponto importante para a compreensão do ciclo da inteligência é ter claro que as análises e os produtos de inteligência são apenas um dos diversos fluxos informacionais (*inputs*) que influenciam o processo de tomada de decisões, e que relatórios específicos podem ser mais ou menos importantes para certas decisões governamentais específicas.<sup>66</sup>

Disseminação tende a ser o elo mais sensível do ciclo da 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 usu-

ário dos coletores. Além disso, como alguns relatórios de inteligência – especialmente nas áreas de sigint e imint – precisam seguir diretamente das unidades de coleta para os usuários finais, todos esses fluxos contribuem para tornar complexo e confuso o que à primeira vista parece ser um ciclo com estágios claros e papéis definidos. Nesse contexto, as etapas de disseminação e avaliação tendem a sobrepor-se uma à outra. Embora difíceis de mensurar, existem indicadores de desempenho objetivos sobre a qualidade e o impacto dos produtos de inteligência nos processos de tomada de decisões, e também formas de monitorar o grau de satisfação dos usuários durante e após a fase de disseminação.<sup>67</sup>

A utilização crescente de arquiteturas virtuais de trabalho nas organizações de inteligência coloca novos desafios e possibilidades para a exploração de ferramentas de processamento, armazenamento, análise, produção, disseminação e avaliação de inteligência de forma mais segura e ágil. Obviamente os aspectos de segurança informacional são decisivos nesse tipo de utilização de redes corporativas interconectadas à internet, mas vale destacar aqui a multiplicidade de ferramentas e serviços possibilitados pela digitalização de informações e sua disponibilização em diferentes formatos e mídias para as diversas organizações e indivíduos ao longo do ciclo. O crescimento do chamado Intelink, a rede que integra as diversas organizações de inteligência do governo norte-americano, pode bem ilustrar a centralidade das novas tecnologias. Em 1994, quando iniciou suas operações, o Intelink já operava com mais de 400 servidores e centenas de milhares de usuários, sendo que apenas a camada de serviços com restrição de acesso para informações classificadas como *secret* já provia acesso para 265 mil usuários interligados através de redes de fibras ópticas ou via satélite.<sup>68</sup>

Em resumo, a complexidade dos requerimentos informacionais, os problemas de relacionamento entre usuários e produtores, os requisitos técnicos das disciplinas de coleta, as limitações decorrentes da necessária separação entre as etapas especializadas do ciclo, os problemas de mensuração e de obtenção de *feedback* sobre a qualidade e a eficiência da inteligência disseminada para os processos decisórios relevantes, tudo isso diz respeito à dinâmica operacional “interna” do ciclo da atividade de inteligência. Na próxima seção será preciso comentar um pouco sobre uma outra dinâmica, relativa ao confronto entre inteligência e segurança.

## Segurança de informações e contra-inteligência

A dinâmica operacional mais elementar da área de inteligência, e também a menos compreendida por observadores externos, é aquela engendrada a partir do seu conflito com as medidas de segurança que são tomadas por um alvo potencial para proteger suas informações. Partindo da definição restrita de inteligência adotada no começo deste capítulo – e correndo de novo o risco da

simplificação exagerada –, enquanto a inteligência procura conhecer o que os comandantes e governantes que a dirigem necessitam saber sobre as ameaças e problemas relativos à segurança do Estado e dos cidadãos, a área de segurança de informações (*infosec*, ou *informations security*) procura proteger as informações que, uma vez obtidas por um adversário ou inimigo – por exemplo, através das operações de inteligência de um governo estrangeiro –, poderiam tornar vulneráveis e inseguros o Estado e os cidadãos. A área de inteligência e a área de segurança exercem funções simétricas e mutuamente dependentes.<sup>69</sup>

A incompreensão dessa dinâmica conflitiva freqüentemente resulta de um senso comum que iguala inteligência e segurança como se fossem uma e a mesma coisa. Não se trata da mesma coisa e, embora existam confusões terminológicas em abundância nessa área, tampouco creio que o problema seja apenas nominal.<sup>70</sup> 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. As duas missões são cumpridas no Estado contemporâneo por organizações distintas, sendo que segurança pode ser considerada uma função gerencial nas organizações civis e uma responsabilidade do comando nas organizações militares. Mas a confusão ocorre porque as duas atividades existem simultaneamente e interagem de forma mais ou menos sinérgica para cada ator envolvido num conflito informacional. Por outro lado, a dialética entre inteligência e segurança é mais complexa do que a mera dicotomia ofensivo/defensivo é capaz de descrever.<sup>71</sup>

Pode-se pensar a segurança informacional como formada por três componentes relativamente autônomos entre si: contramedidas de segurança (SCM), contra-inteligência (CI) e segurança de operações (Opsec).

O primeiro componente é formado pelas medidas de proteção que “espelham” as capacidades adversárias de obtenção de informações. Tais medidas 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, investigações do pessoal empregado antes da concessão de credenciais de acesso às informações classificadas e vigilância sobre seus contatos com pessoal externo e estrangeiros até as várias políticas e camadas de segurança eletrônica nas redes de computadores e o uso de criptografia para a preservação da segurança das comunicações (comsec). Na área militar, esse conjunto de contramedidas de segurança (SCM, ou *security countermeasures*) inclui ainda o uso de camuflagem para evadir-se dos sensores de imint das forças inimigas, reduções de emissões não-intencionais e de “assinaturas” como medidas contra masint, treinamento para resistir a interrogatórios e outras medidas preventivas contra a coleta de humint. Programas de

sensibilização e educação na área de proteção ao conhecimento enquadraram-se nessa primeira “família” de ações na área de infosec.<sup>72</sup>

O segundo conjunto de medidas de infosec depende da 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. Embora o foco tradicional da área de contra-inteligência (CI, ou *counterintelligence*) tenha sido na contra-espionagem, o alcance das medidas de neutralização das operações de coleta de inteligência de um adversário vai muito além da identificação e da repressão de suas redes de coleta de humint. Como escreveu Michael Herman (1996:168), um agente pode ser preso, um oficial de inteligência estrangeiro atuando sob cobertura diplomática pode ser expulso do país depois de declarado *persona non grata*, mas também os microfones e escutas telefônicas podem ser “varridos” eletronicamente e desativados, os aviões de imint e sigint podem ser abatidos ou forçados a pousar, navios de coleta de sigint podem ser capturados em caso de violação de águas territoriais etc. Para todas essas medidas, os conhecimentos acumulados pela área de contra-inteligência são fundamentais.

Em terceiro lugar, por segurança de operações (opsec) entende-se aqui o conjunto de procedimentos que visam a 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. Embora opsec envolva também alguns programas de redução de ruídos e emissões não-intencionais, silêncio de rádio, camuflagem contra imint e outros, que poderiam tornar confusas as fronteiras entre esse componente e as contramedidas passivas de segurança (SCM), essa área de segurança de operações destaca-se fundamentalmente por sua dimensão ativa, especialmente aquilo que a literatura militar chama de *deception operations*, utilizadas para desorientar e induzir ao erro um inimigo através do uso de logro, engano, dolo, ocultação e dissimulação, fazendo-o produzir uma análise consistente mas equivocada da situação.<sup>73</sup>

Embora *grosso modo* esses três componentes da área de segurança de informações contenham medidas de defesa contra operações de inteligência adversárias que podem ser classificadas num gradiente que vai das mais defensivas (criptografia ou uso de *firewalls* eletrônicos, por exemplo) para as mais ofensivas (tais como “cegar” um sensor de imagens com a utilização de *laser*, forjar um fluxo de mensagens para *deception* ou manipular agentes duplos...), na verdade a principal razão para diferenciá-las entre si é de natureza organizacional. Segundo George Jelen (1992:391), as culturas organizacionais das áreas de contramedidas de segurança (SCM), contra-

inteligência (CI) e segurança de operações (Opsec) evoluíram separadamente ao longo do século XX, e as tentativas de integração das três numa doutrina de segurança informacional (infosec) ainda são muito recentes e controversas. Em particular, ainda é muito comum a literatura referir-se à contra-inteligência para designar o conjunto de funções descritas nessa seção, invertendo o uso dos termos e considerando infosec uma parte do trabalho de contra-inteligência. Isso é mais comum ainda entre os autores norte-americanos e nos países mais influenciados por aqueles autores.<sup>74</sup>

Na verdade, saber se a segurança de informações (infosec) é parte da contra-inteligência ou vice-versa é a face menos importante do problema, pois não se trata tanto da escolha de nomes e sim da clareza que se deve ter ao escolhê-los, clareza sobre as especificidades operacionais, as responsabilidades organizacionais e os fins a que se destina cada componente que está sendo estudado. De modo geral, as funções de contra-inteligência são alocadas sob a responsabilidade das organizações de inteligência exterior e interna (também chamada de inteligência doméstica ou de segurança), enquanto as funções de segurança são alocadas sob a responsabilidade de organizações civis e militares especializadas em soluções de segurança. Por sua vez, opsec é uma das missões e objetivos das seções de operações nos estados-maiores das organizações militares. Assim, o melhor é sempre procurar respeitar a evolução peculiar de cada componente num determinado país, procurando aumentar o grau de coordenação e sinergia entre eles. Até porque cada um deles tem suas próprias complexidades internas.

Por exemplo, tal como apresentada aqui, a noção de contra-inteligência remete ao esforço mais geral de obtenção de inteligência sobre as capacidades, intenções e operações dos serviços de inteligência adversários. Como esse foco em suas contrapartes só pode ser atingido tendo em vista o contexto mais geral em que operam aqueles serviços, contra-inteligência tende a constituir um inteiro subciclo das operações de inteligência, especialmente por causa da diversidade de fontes tecnológicas e humanas utilizadas na obtenção de um escopo variado de informações que precisam ser analisadas e incorporadas aos acervos de conhecimento das organizações de inteligência “positiva”, mas também das instituições responsáveis pela área de segurança de informações (infosec) de um país ou organização. Por isso mesmo, contra-inteligência poderia ser considerada apenas uma das chamadas disciplinas defensivas da área de infosec, muito mais do que inteligência “ofensiva” propriamente dita.

No entanto, 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 da 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 um país. O resultado dessa dupla missão da contra-inteligência é que ela pertence simultaneamente à função de inteligência e à função de segurança de um país ou organização.<sup>75</sup>

Aceitando-se a premissa de que a atividade de inteligência é em grande parte definida pelo conflito informacional com os sistemas de segurança adversários, pode-se pensar na atividade de contra-inteligência como um subconjunto do conflito principal, como aquelas *matreshskas*, as bonecas russas de encaixe. Utilizando uma situação extrema para ilustrar o argumento, a dinâmica operacional tende a tomar a forma de uma série de conflitos aparentemente intermináveis, com os serviços de inteligência de um lado (digamos, A) tentando suplantar as redes de segurança de outro (digamos, B) e sendo, por sua vez, assediados pelos serviços de contra-inteligência do adversário (B), que precisam penetrar os serviços de inteligência de A para descobrir o que eles querem e o que eles sabem, o que leva então os serviços de contra-inteligência de A a tentar se infiltrar nos serviços de contra-inteligência de B para tentar garantir a segurança de suas próprias operações de inteligência (de A) no jogo principal, e assim sucessivamente.<sup>76</sup> Como no mundo real os conflitos entre inteligência e segurança, contra-inteligência e inteligência, contra-inteligência e contracontra-inteligência não acompanham essa tendência de “descida” aos extremos, o que impede que tais regressões sejam infinitas e garante a centralidade do conflito principal são os objetivos políticos e a limitação dos recursos que podem ser dedicados.<sup>77</sup> Ainda assim, essa é realmente uma das áreas mais nebulosas e esoréticas na práxis dos serviços de inteligência contemporâneos.<sup>78</sup>

Finalmente, é preciso lembrar que os serviços de inteligência podem fornecer valiosas contribuições para a segurança informacional (infosec) de seu próprio país ou organização, pois afinal eles são os especialistas na superação das redes de proteção adversárias, e ganhos ofensivos traduzem-se em aprendizado defensivo. 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 aumentem a segurança informacional das forças amigas. Em algumas áreas de coleta de inteligência, como sigint, isso é tão intenso que a própria organização também é a principal responsável pelo provimento de segurança das comunicações (comsec). O inverso é verdadeiro, ou seja, melhores capacidades defensivas no conflito informacional também ajudam na obtenção de inteligência, mas de forma muito menos direta, apenas liberando recursos e aumentando a confiabilidade do sistema para os usuários finais responsáveis pelos processos de tomada de decisão nas áreas de política externa, defesa e policiamento.

Ainda que as ameaças de inteligência sejam mais difíceis de se identificar no atual contexto internacional, o que necessariamente obriga a uma redefinição das missões de contra-inteligência, os temas associados à segurança informacional (infosec) são cada vez mais centrais e deveriam ser pensados a partir de suas interações com a área de inteligência como um todo.

## Operações encobertas

As chamadas operações encobertas recebem nomes distintos e abarcam atividades variadas em diferentes países, mas têm sido amplamente utilizadas pelas principais potências internacionais ao longo do século XX, sendo ainda mais controversas do que as operações de inteligência mais convencionais. Nos Estados Unidos, são chamadas de ações encobertas (CA, ou *covert actions*), na União Soviética eram abarcadas pelas chamadas medidas ativas (*aktivnye meropriiatii*) e, na Inglaterra, atendem pelo singelo nome de ações políticas especiais (*special political actions*).<sup>79</sup> Embora não seja possível desenvolver aqui uma análise mais completa da *rationale* e dos problemas associados a esse tipo de atividade, pelo menos dois aspectos merecem um breve comentário. O primeiro aspecto diz respeito aos tipos de operações compreendidos pelo conceito, enquanto o segundo remete para a relação existente entre tais operações encobertas e as atividades de coleta, análise e contra-inteligência discutidas até aqui.<sup>80</sup>

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.

As duas características principais das operações encobertas enquanto recurso de poder são, segundo Mark Lowenthal (2000:111-113) e Abram Shulsky (1992:83-85), o seu caráter instrumental para a implementação de políticas e o requisito de plausibilidade na negação da autoria (*plausible deniability*). A primeira característica enquadra as operações encobertas enquanto ferramentas coercitivas na implementação de uma política externa, tal como o são, por exemplo, os embargos econômicos ou o leque de opções relativas ao uso ou à ameaça de uso da força. A segunda característica enfatiza a negação da autoria, mais do que a clandestinidade da operação em si mesma. É possível classificar as operações encobertas segundo a escala e a intensidade do uso de meios de força e o grau de plausibilidade da negação de autoria. Quanto maior a escala das operações e o papel do uso da força, menor é a probabilidade de que a negação da autoria da operação seja plausível. Quatro tipos de operações encobertas podem ser destacados.

O primeiro tipo é o mais extremado, envolvendo o apoio a grupos já existentes (ou o 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, munições, explosivos e equipamentos até um engajamento mais direto em logística, treinamento, inteligência e forças combatentes especializadas em operações especiais (*special ops*). Exemplos históricos desse tipo de operações incluem, entre muitos outros, a guerra “secretaria” conduzida pelos Estados Unidos no Laos (1960/75) e a campanha britânica de contra-insurgência na Malásia (1950).

Um segundo grupo de operações encobertas 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. Exemplos de operações desse tipo são os golpes de Estado patrocinados pela CIA no Irã (1953) e na Guatemala (1954), a campanha norte-americana de desestabilização do governo Allende no Chile (1970/73), o assassinato de lideranças palestinas pelos serviços secretos israelenses nos anos 1980 ou o afundamento do navio *Rainbow Warrior*, do grupo Greenpeace, pelos serviços secretos franceses em 1985.

O terceiro tipo envolve operações de sabotagem econômica e política contra forças adversárias ou, por outro lado, o fornecimento de assistência secreta a governos e forças aliadas, tais como partidos políticos, organizações não-governamentais, meios de comunicação etc. A campanha da CIA para evitar a vitória dos comunistas nas eleições italianas de 1947 é um exemplo desse tipo de operação, assim como o são a venda clandestina de armas para o Irã (conduzida pela presidência dos Estados Unidos em 1986, com a intermediação israelense e saudita), o treinamento das forças de segurança e inteligência dos regimes pós-revolucionários do Iêmen do Sul e de Moçambique, nos anos 1970, pelo serviço de inteligência exterior da Alemanha Oriental, ou ainda a ajuda do Partido Comunista da União Soviética a cerca de 100 partidos e grupos aliados em países estrangeiros até a década de 1980.

Por sua vez, o quarto tipo de operações encobertas abrange um conjunto de medidas para tentar influenciar as percepções de um governo ou mesmo da 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. Esse é o tipo mais comum de operação encoberta, e existem inúmeros exemplos, talvez os mais famosos sejam as rádios Free Europe e Liberty, estabelecidas clandestinamente pela CIA na

Europa em 1949 e 1951, respectivamente, e transferidas em 1973 para um novo órgão federal do governo norte-americano, o Board of International Broadcasting.<sup>81</sup>

A intensidade do recurso aos vários tipos de operações encobertas variou de país para país ao longo da Guerra Fria e, aparentemente, declinou de modo geral na primeira década após o colapso da União Soviética. Segundo a estimativa de John Hedley (1995:5), operações encobertas representavam cerca de 2% das atividades e gastos da CIA na primeira metade da década de 1990.<sup>82</sup> Segundo Jeffrey Richelson (1999:349-360), as operações norte-americanas mais importantes em anos recentes estiveram dirigidas contra os governos de Iraque, Líbia e Iugoslávia, além daquelas voltadas para o suporte a governos aliados no combate a insurgências, e ainda operações de guerra informacional (IW), sabotagem e ações paramilitares no combate a grupos transestatais nas áreas de narcotráfico, terrorismo e proliferação de armas de destruição maciça (WMD). Em 1998, o Congresso dos Estados Unidos aprovou o Iraq Liberation Act, uma ampliação das operações encobertas para a derrubada do regime de Saddam Hussein que, naquele ano, chegou a um orçamento de US\$97 milhões.<sup>83</sup>

A principal *rationale* para a utilização das operações encobertas é o cálculo de custos e benefícios associados a um envolvimento aberto de um governo ou organização em processos políticos e/ou militares instáveis e importantes, ou quando a diplomacia é insuficiente e o uso aberto da força pode ser contraproducente ou arriscado. Tal “economia de meios” como justificativa para o recurso às operações encobertas, no entanto, parece estar muito mais ligada à flexibilidade e à proteção política (*plausible deniability*) prometidas pelos serviços secretos para os governantes ou líderes da organização. Mesmo em operações de larga escala, como o suporte norte-americano aos *contras* na Nicarágua e aos *mujahedins* no Afeganistão durante os anos 1980, ainda que as operações em si mesmas fossem largamente “abertas” o governo de Washington podia seguir negando seu envolvimento oficial em fóruns internacionais e junto à opinião pública e meios de comunicação. Mas, independentemente dos cálculos políticos e dos problemas de execução desse tipo de atividade, ainda resta problematizar a sua relação com as demais atividades na área de inteligência.

Afinal, se inteligência é entendida como um *input* informacional para processos de decisão e implementação das políticas externa, de defesa e de provimento de ordem pública, operações encobertas certamente não têm primariamente uma função informacional. A alocação dessas atividades sob a responsabilidade dos serviços de inteligência em muitos países resulta de escolhas históricas e também da “capacidade instalada” das agências de humint para gerir contatos e segredos em territórios estrangeiros. Nesse caso,

uma visão mais restritiva do conceito de inteligência torna mais fácil compreender tal associação. Por outro lado, certamente há algo de arbitrário nessa ligação operacional entre espionagem, humint e operações encobertas. Como exemplo dessas escolhas e/ou acidentes históricos, basta lembrar que na tradição britânica o serviço secreto conduziu operações encobertas (além da espionagem propriamente dita) desde sua criação no começo do século. Mesmo assim, durante a II Guerra Mundial o governo britânico alocou as operações encobertas de tipo paramilitar sob a responsabilidade de um Special Operations Executive (SOE), enquanto a propaganda clandestina era feita pelo Political Warfare Executive (PWE), estando ambas as organizações fora do comando do serviço de inteligência. E, nos Estados Unidos, somente depois de 1952 foram alocadas em uma mesma agência governamental a espionagem internacional e a execução de operações encobertas (no que é hoje o Diretório de Operações da CIA).<sup>84</sup>

Na maioria dos países que possuem tais capacidades, as operações encobertas são responsabilidade dos serviços de inteligência, que obtêm das tropas especiais de elite das Forças Armadas os recursos humanos e materiais que lhes faltam internamente na medida em que as operações de influência afastam-se do terreno da propaganda e aproximam-se das ações paramilitares e de guerrilha. A condução dessas operações tende a impactar a dinâmica operacional das funções mais diretamente informacionais da área de inteligência em níveis variados, além de ser um tipo de missão que contribui para a cristalização de uma divisão entre duas culturas organizacionais bastante distintas, entre as pessoas de “ação” (chamadas pejorativamente de *knuckle-draggers*, ou “gorilas”, nos Estados Unidos) e as pessoas de “análise” (chamadas pejorativamente de *weenies*, ou “fracotes”, no mesmo país).

Embora esse seja o menor dos problemas causados pelas operações encobertas sobre a política internacional, é um tema que afeta diretamente as dinâmicas operacionais da área de inteligência enquanto objeto de estudo da ciência política.

## A função da inteligência

Discutidas as quatro dinâmicas operacionais mais importantes que caracterizam as atividades de inteligência no Estado contemporâneo, uma síntese do que foi discutido até aqui pode ser oferecida como resposta à seguinte pergunta: por que os governos têm serviços de inteligência?

A resposta mais óbvia e direta é que os governantes esperam maximizar poder através do desenvolvimento de capacidades de inteligência. De modo geral, a literatura destaca oito utilidades principais que os governos teriam para

esses sistemas, que seriam também a principal justificativa pública utilizada para a sua manutenção. Em primeiro lugar, esperar-se-ia que a inteligência contribuisse para tornar o processo decisório governamental nas áreas relevantes de envolvimento (política externa, defesa nacional e ordem pública) mais racional e realista, ou seja, menos baseado em intuições e convicções preconcebidas e mais baseado em evidências e reflexão. Em segundo lugar, que o processo interativo entre *policymakers* (responsáveis pelas políticas públicas, sejam eles funcionários de carreira, dirigentes nomeados ou políticos eleitos) e oficiais de inteligência produzisse efeitos cumulativos de médio prazo, aumentando o nível de especialização dos tomadores de decisões e de suas organizações. Em terceiro lugar, que a inteligência pudesse apoiar diretamente o planejamento de capacidades defensivas e o desenvolvimento e/ou a aquisição de sistemas de armas, de acordo com o monitoramento das sucessivas inovações e dinâmicas tecnológicas dos adversários. Em quarto lugar, que apoiasse mais diretamente as negociações diplomáticas em várias áreas, não tanto afetando a definição da política externa mas propiciando ajustes táticos derivados da obtenção de informações relevantes. Em quinto lugar, que a inteligência fosse capaz de subsidiar o planejamento militar e a elaboração de planos de guerra, bem como suportar as operações militares de combate e outras (operações de paz, assistência, missões técnicas etc.). Em sexto lugar, 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. Em sétimo lugar, sistemas de inteligência 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*. Finalmente, sistemas de inteligência serviriam para preservar o segredo sobre as necessidades informacionais, as fontes, fluxos, métodos e técnicas de inteligência diante da existência de adversários interessados em saber tais coisas.<sup>85</sup>

Por mais incompleta e telegráfica que seja essa lista, ela implica um papel menos “dramático” do que se poderia pensar para a atividade de inteligência enquanto dimensão do poder estatal. Claro que casos como o do telegrama Zimmerman ou a ruptura dos códigos alemães na II Guerra têm impacto direto sobre o curso dos acontecimentos históricos, mas eventos assim são relativamente raros.<sup>86</sup> Normalmente, a atividade de inteligência visaria a otimizar a posição internacional de um país ou organização, não a transformá-la radicalmente.<sup>87</sup>

Mesmo na guerra, onde o impacto da inteligência é mais imediato, também predominam os efeitos de otimização. A superioridade informacional proporcionada pelas dinâmicas operacionais da atividade de inteligência per-

mite, ao menos em tese, uma gestão mais eficiente dos recursos humanos e dos materiais, aumenta a sobrevivência das forças em combate (*survivability*) e contribui para o bom desempenho das funções de comando. Implica dizer que a capacidade de inteligência de uma força armada precisa ser avaliada em termos de seu valor absoluto (grau de aproximação em relação a algum tipo de critério sobre o que seria a realidade) e relativo (contraste com a inteligência disponível para os comandantes das forças inimigas).

Embora inteligência seja apenas uma das dimensões que afetam a *performance* do comando na guerra, ela pode constituir um fator crítico na condução das operações, pois permite agilizar o ciclo de tomada de decisões e resposta dos comandantes das forças amigas, ao mesmo tempo que opera desorganizando moral e analiticamente o ciclo de tomada de decisões do comando inimigo, reduzindo sua capacidade de resposta às iniciativas e eventualmente destruindo sua vontade de seguir lutando. Em particular, inteligência superior é um fator crítico na guerra de comando e controle ( $C^2$  warfare), na medida em que cria fricção e aumenta a entropia no chamado ciclo OODA (*observe-orient-decide-act*) das forças inimigas.<sup>88</sup>

Por vezes, no entanto, a atividade de inteligência também causa efeitos transformadores sobre a própria natureza das operações militares.<sup>89</sup> A *Blietzkrieg* alemã contra a França, em 1940, bem como o impacto da ruptura dos códigos de comunicação alemães no mar do Norte, em 1915/18, ou no Atlântico, em 1943/45, que alteraram a dinâmica da guerra naval, ou ainda o papel da inteligência de imagens no uso da artilharia e do bombardeio desde a II Guerra Mundial até a Guerra da Iugoslávia de 1999, são todos exemplos de efeitos transformadores da natureza dos engajamentos, efeitos que foram além da mera otimização do uso de recursos escassos.<sup>90</sup> É importante destacar, porém, que tais efeitos de “transformação” resultam tanto ou mais da eventual qualidade superior dos processos de análise, produção e disseminação de inteligência do que da mera quantidade de informações coletadas. Pelo contrário, o excesso de informações captadas por uma infinidade de sensores e canalizadas através das múltiplas instâncias de comando pode contribuir para sobrecarregar as instâncias de comando e planejamento.<sup>91</sup>

Para David Kahn (1995:95), a função predominante de otimização de recursos materiais e psicológicos seria uma das três características centrais da inteligência, observável nas áreas civil e militar. As outras duas características seriam mais visíveis no âmbito militar e envolveriam, por um lado, o reconhecimento do papel auxiliar da inteligência em relação à capacidade combatente e, por outro, a associação eletiva entre a defesa e a inteligência.

Segundo George O’Toole (1990:39-44), dessa “lei de Kahn” desdobram-se quatro corolários: 1. A ênfase na defesa tende a ser acompanhada pela ênfase na inteligência. 2. A ênfase no ataque tende a ser acompanhada pela ênfase

na contra-inteligência para garantir segurança operacional e surpresa. 3. Em situações de impasse e equilíbrio de forças os dois lados tendem a enfatizar a busca de inteligência. 4. As operações ofensivas que adquirem características defensivas tendem a aumentar a ênfase na inteligência.<sup>92</sup>

Sem recusar completamente essa hipótese, Michael Herman (1996) chama a atenção para evidências históricas que poderiam enfraquecer-lhe a universalidade. Por exemplo, a qualidade superior da inteligência de que dispunham os alemães na invasão da Noruega em 1940, ou os japoneses no ataque contra a frota norte-americana do Pacífico em Pearl Harbor em 1941, ou ainda, e de modo mais geral, a superioridade da inteligência aliada a partir da metade da II Guerra, situações que evidenciam que a inteligência pode favorecer tanto o ataque quanto a defesa. Mais ainda, Michael Herman afirma que a superioridade em inteligência reflete em parte uma superioridade militar já existente. Afinal, imagens são mais bem obtidas pelo lado que possui superioridade aérea, assim como são as forças vitoriosas no campo de batalha que tendem a extrair mais informações úteis de prisioneiros de guerra e documentos capturados, bem como é o exercício do comando do mar que potencializa a obtenção de material criptográfico crucial para a decodificação e a decifração de sinais. Não se trata de substituir o entendimento equivocado de que a inteligência é a arma do fraco pelo argumento simétrico (e igualmente equivocado) de que a inteligência sempre favorece o forte. Trata-se, sim, de destacar que o desenvolvimento de capacidades de inteligência é demorado e depende das experiências prévias de cada país.

Em resumo, inteligência não garante a vitória num confronto entre vontades nem pode dizer o que vai ocorrer no futuro. Como ocorre em qualquer sistema de informação, os fluxos de inteligência são parcialmente estruturados e se prestam a um gerenciamento bastante incerto. Além disso, a complexidade técnica e os grandes volumes de informações processados dificultam a integração das etapas do ciclo da inteligência e o atendimento ágil das necessidades dos usuários. Finalmente, os riscos associados às contramedidas de segurança e às operações de contra-inteligência obrigam a coleta de inteligência a conviver com uma forte dose de segredo, auto-refreamento e redundância, que impõe limites muito claros à agilidade e também à transparência na condução das operações.

Embora possa ser decisiva em certos momentos especiais na guerra e na paz, em geral os governos contam com a inteligência para reduzir a incerteza nas decisões sobre política externa, defesa nacional e ordem pública, para aumentar a segurança nacional e para posicionarem-se melhor no sistema internacional.

## Notas

1. Até meados da década de 1980, a maioria dos trabalhos sobre inteligência era de natureza histórico-descritiva ou exposés jornalísticos. Embora existam trabalhos mais

antigos de excelente qualidade e memórias escritas por ex-oficiais de inteligência bastante educativas, o clima político-ideológico da Guerra Fria, a dificuldade de separar as análises e informações razoavelmente isentas sobre inteligência da mera desinformação mais ou menos sofisticada, bem como os limites impostos por pesadas restrições de segurança, foram fatores que contribuíram para a decisão de concentrar a revisão bibliográfica no período 1985-2000. Mesmo os trabalhos mais recentes raramente são de natureza teórica ou comparativa. Considero o livro do autor inglês Michael Hetman (1996) como o melhor trabalho atualmente disponível internacionalmente sobre inteligência e um marco na literatura dos *intelligence studies*. O exercício realizado nesse capítulo é fortemente influenciado por aquele trabalho. Para um primeiro detalhamento das plataformas e sistemas de coleta utilizados pelos Estados Unidos, ver Richelson (1999). Um excelente texto sobre inteligência e operações militares, ainda que um pouco desatualizado em relação à tecnologia, é o de Kennedy (1983). Para uma visão geral das características operacionais, sugiro começar por Lowenthal (2000) e Shulsky (1992). Sobre sistemas e dinâmicas de trabalho na área de análise em inteligência na chamada era da informação, ver Berkowitz & Goodman (2000).

2. Cada uma dessas áreas gera seu próprio corpo de literatura especializada. Para um balanço das várias abordagens sobre informações e processos de tomada de decisão governamental, ver a parte 3 (Decision Analysis) do livro de Parsons (1995:245-455). Sobre o uso rotineiro de especialistas, bancos de dados e sistemas de informação nos diversos ramos da administração pública, ver Barker & Peters (1992). Sobre a chamada “inteligência de negócios” da área empresarial, ver principalmente Kahaner (1996), Combs & Moorhead (1992) e Cronin & Davenport (1991). Não apenas a terminologia, mas parte das técnicas e mesmo dos recursos humanos na área de inteligência empresarial é oriunda do governo, especialmente nos Estados Unidos. Para uma noção mais empírica sobre como operam essas empresas, ver a página da Open Sources Solutions Inc. <<http://www.oss.net>>. Finalmente, sobre o conceito de inteligência social, ver Davidson (1988) e Durant (1991).

3. Sims (1995:4).

4. Ver, por exemplo, a literatura cada vez mais central sobre a teoria econômica da informação e os textos sobre economias “baseadas no conhecimento”. Em particular, destaca-se o trabalho seminal de Arrow (1984). Uma síntese útil das proposições de Arrow sobre a informação como um bem econômico de tipo especial pode ser encontrada em Albuquerque (1996:131-162). Na fronteira entre economia e sociologia da informação, ver Dedijer & Jéquier (1987) e Varlejs (1995). O trabalho sociológico mais importante sobre as causas estruturais e culturais do mau uso da informação nas organizações ainda é o de Wilensky (1967). No caso da ciência política, ver, por exemplo, Milner (1997) e Krehbiel (1992).

5. Shulsky (1995:26).

6. Herman (1996:36-133).

7. Os limites entre a dissidência legítima e a criminalização da contestação são muitas vezes tênues, mesmo nas poliarquias mais institucionalizadas. Definir o “inimigo público” (nas diversas faces do desordeiro, criminoso, subversivo, espião, terrorista, traidor etc.), longe de ser um sólido ponto de partida para as agências de imposição da lei, é parte do conflito inerente a qualquer sociedade moderna. Para um primeiro

aprofundamento, ver as partes II (National Security and Human Rights), III (Criticism, Dissent, and National Security) e IV (National Security and the Legal Process) do livro de Lustgarten & Leigh (1994). E também o excelente livro do cientista político britânico Peter Gill (1994), que focaliza exatamente o impacto dos serviços de inteligência de segurança (conhecidos na América Latina até o começo da década de 1990 como serviços de informações) sobre o funcionamento das instituições democráticas e os direitos civis.

8. Nesse sentido é que o Departamento do Tesouro, o Departamento do Comércio, a Environmental Protection Agency (EPA), a Drug Enforcement Administration (DEA) e os centros de controle de doenças (CDCs), especialmente o de Atlanta, são usuários ou “clientes” dos serviços norte-americanos de inteligência, embora o grau de prioridade desses usuários seja menor do que, digamos, a presidência ou o NSC. Cf. Sims (1995:9).

9. Sobre o nexo entre políticas de segurança nacional e inteligência, ver inicialmente Godson (1986).

10. Sobre o papel da diplomacia na gênese dos serviços de inteligência exterior (*foreign intelligence*), ver Herman (1996:9-15). Sobre o *status legal* dos diplomatas e embaixadas, com considerações sobre os aspectos de coleta de inteligência e segurança, ver o capítulo 7 (The role of diplomacy: a traditional tool in changing times) de Henderson (1998).

11. Para o papel do radar na batalha da Inglaterra, ver Stares (1991). Sobre sigint na batalha do Atlântico, ver Hinsley (1993). Ambos os autores consideram o radar a mais importante e revolucionária inovação na área de informações durante a II Guerra Mundial.

12. O conceito de *information warfare* (IW) resulta da tentativa de integração e expansão das operações de guerra eletrônica, guerra de comando e controle (C2 warfare) e disciplinas defensivas em inteligência. Por analogia com a guerra terrestre ou marítima, a guerra informacional compreende o conjunto de ações ofensivas e defensivas conduzidas no ambiente informacional para controlar o *cyberspace*. Ciberespaço é aqui entendido como o “lugar” onde interagem computadores, programas, sistemas de comunicação e equipamentos que operam via irradiação de energia no espectro eletromagnético. Porém, menos por um “lugar” ou um conjunto classificável de ações, a guerra informacional define-se melhor por seus objetivos: obter e manter superioridade informacional na batalha ou na guerra. Ações tão diferentes entre si como um ataque aéreo a uma central de telecomunicações, operações de sigint, missões aéreas para reconhecimento do campo de batalha ou a implantação clandestina de códigos de computador com “bombas lógicas” poderiam ser parte de uma campanha de guerra informacional. Destaque-se que essas operações de IW não devem ser tomadas como configurando uma “guerra” à parte. A guerra permanece una e indivisível enquanto realidade; o que está em jogo é a perspectiva – ainda não consolidada ou atestada como mais útil do que a preocupação com esse tema por organizações combatentes já consolidadas – de criação de uma “arma” ou especialidade combatente de informações. Sobre o tema, ver Libicki (1995).

13. Reduções de assinaturas térmicas e acústicas, bem como o uso de tecnologias *stealth* são cada vez mais importantes para a defesa e o ataque em operações de combate, mas isso não diz respeito ao grau de fragilidade das fontes. Cf. Dunnigan (1993).

14. A literatura sobre o “ciclo da inteligência” é imensa e em geral repetitiva. Essa versão desagregada em 10 etapas é uma composição de todas as versões que conheço. Uma definição em cinco etapas (direção-coleta-análise-disseminação-avaliação) é adotada como padrão pela Otan, pelo Departamento de Defesa dos Estados Unidos e pelos países-membros da Junta Interamericana de Defesa (JID/IADB), inclusive o Brasil. A definição-padrão pode ser encontrada no *Dictionary of military and associated terms*, elaborado para o US Joint Chiefs of Staff. Esse dicionário está disponível também na Internet em: <<http://www.dtic.mil/doctrine/jel/doddict>>. Uma versão que agrupa os 10 passos em quatro componentes pode ser encontrada em Krizan (1999:7-11). A versão adotada aqui, com dois estágios essenciais separados organizacionalmente, aparece formulada em Herman (1996:39-47).

15. Sobre a noção de ciclo em políticas públicas, ver Parsons (1995:77-83).

16. Para um exemplo mais antigo das listas de requerimentos norte-americanas (chamadas de KIQs – *key intelligence questions* – até a década de 1980 e depois de NITs – *national intelligence topics*), ver Berkowitz & Goodman (1991:47-174). Para uma noção sobre os requerimentos de inteligência soviéticos, ver Andrew & Gordievsky (1991). Obviamente, requerimentos de inteligência em operações militares e policiais, especialmente nas fases de planejamento, tendem a ser muito mais estruturados. Além das baterias iraquianas de mísseis Scud, o comando integrado das forças aliadas na Guerra do Golfo estabeleceu 27 alvos prioritários para as atividades de inteligência no teatro e para as organizações nacionais dos países aliados. Para uma avaliação positiva desses requerimentos e também para um comentário sobre sua rápida obsolescência uma vez iniciadas as operações de combate, ver US Congress (1993b). Para um comentário sobre as prioridades estabelecidas pela PDD-35 (Presidential Decision Directive) assinada pelo presidente Clinton em 1995, que enfatizava os chamados *hard targets* (Cuba, Irã, Iraque, Líbia e Coréia do Norte) e temas transestatais (proliferação, mercado de armas convencionais, narcóticos, crime organizado e terrorismo), ver Lowenthal (2000:43).

17. Ver, principalmente, Odom (1997:9) e Godson, Schmitt & May (1995:232-242).

18. As melhores discussões sobre o processo de trabalho e os relacionamentos entre usuários, gestores, coletores e analistas na área de inteligência como um todo são encontradas no capítulo 16 (*The production process*) de Herman (1996:283-304) e no capítulo 3 (*The intelligence process and the information revolution*) do livro de Berkowitz & Goodman (2000:58-98).

19. Johnson (1985:181-198).

20. Essa apresentação-padrão das cinco disciplinas da área de coleta aparece em praticamente todos os livros e textos. Mesmo sendo algo repetitivo e superficial em relação ao material disponível, creio ser necessário destacar pelo menos as fontes, características e plataformas típicas em cada disciplina. Como a maioria dos livros simplesmente repete a mesma fórmula, para um aprofundamento posterior recomenda-se alguns autores que realmente acrescentam algo novo e/ou detalham algum aspecto relevante: Herman (1996:36-99), Lowenthal (2000:53-74), Shulsky (1992:11-43) e Richelson (1999:150-290).

21. Além dos textos mais gerais sobre o ciclo da inteligência já mencionados nas notas anteriores, vale citar dois trabalhos específicos sobre humint que podem ser úteis: o mais interessante de todos, inclusive pela qualidade visual e pela informação histórica,

é Melton (1996). Um outro texto, menos interessante porém mais abrangente e razoavelmente atualizado, é o de Laffin (1996). Outras referências podem ser encontradas na bibliografia de referência ao final do trabalho. Especialmente sobre o *tradecraft* da espionagem, são bastante úteis as memórias de vários atores envolvidos em diferentes momentos do último século. É bastante óbvio, no entanto, que esse tipo de fonte deve ser tratado com cuidados adicionais em relação aos cuidados que se deve ter com fontes memorialísticas em geral.

22. Um exemplo dramático da importância de redes de agentes ou colaboradores situados na base da pirâmide informacional (e que a literatura descreve um tanto equivocadamente como *low level assets*) é a rede de informantes sobre os horários, cargas e rotas dos trens no território ocupado pela Alemanha durante a I Guerra Mundial, numa operação chamada Dame Blanche. As redes de inteligência britânicas e aliadas na Bélgica, Países Baixos e na França ocupadas chegaram a ter mais de 20 postos de observação em 1916. Cf. Richelson (1995:21-24).

23. Segundo Abe Shulsky (1992:16-17), o principal agente norte-americano na Alemanha durante a II Guerra Mundial foi Fritz Kolbe, um funcionário do Ministério do Exterior alemão que era responsável pela seleção de todos os despachos diplomáticos vindos das embaixadas e representações alemãs, para garantir que o ministro recebesse qualquer documento importante, diplomático ou militar. Kolbe foi um *walk-in* que se voluntariou primeiro para trabalhar para os britânicos, que não lhe deram crédito por temerem um “agente provocador”. Apesar de alguma desconfiança inicial, Kolbe foi controlado pelo OSS e, entre 1943 e 1945, entregou mais de 1.500 documentos secretos alemães aos norte-americanos.

24. Para um tratamento mais detalhado sobre os perfis de agentes potenciais, ver o capítulo 4 (*Espionage and counterespionage*) de Kennedy (1983:60-75).

25. Por exemplo, o principal agente soviético da CIA e do SIS britânico durante a Guerra Fria foi o coronel Oleg Penkovsky, do GRU, um alto deserto que se voluntariou e permaneceu em seu posto até ser descoberto e executado em 1963. Cf. Richelson (1995:274-279).

26. Como se sabe, o HVA conseguiu colocar um agente como secretário particular de Willy Brandt, o chanceler alemão ocidental que teve que renunciar ao cargo em 1974, depois da descoberta e prisão de Günter Guillaume. Tão importante e bem-sucedida quanto a infiltração de Guillaume foi o recrutamento de secretárias e outros funcionários menos graduados com acesso a uma infinidade de documentos secretos, não apenas no governo da Alemanha Ocidental, mas também na Otan. Sobre as concepções do trabalho de inteligência nos países do campo soviético, ver a autobiografia de Marcus Wolf, ex-diretor do serviço de inteligência exterior da Alemanha Oriental, o Hauptverwaltung Aufklärung (HVA). Cf. Wolf & McElvoy (1997).

27. Embora com dimensões que variam desde alguns indivíduos até centenas de quadros (como a estação da CIA em Saigon durante a Guerra do Vietnã), tipicamente uma estação da CIA numa embaixada norte-americana no exterior conta com oficiais do diretório de operações (DO), oficiais do serviço de monitoramento de mídia estrangeira (FBIS) e oficiais do escritório de ligação com serviços de inteligência estrangeiros. Além da CIA, as operações de humint norte-americanas sob cobertura oficial também contam, nos escritórios de aditância militar (Defense

Attaché System), com elementos especializados em coleta de humint subordinados ao Defense Humint Service da agência de inteligência do Pentágono (DIA). Dependendo do caso, pode haver elementos uniformizados sob controle operacional da NSA. Nos países em que as operações norte-americanas de *law enforcement* são relevantes, pode haver elementos de coleta de humint sob controle direto do FBI e da DEA. Ver Richelson (1999:258-262).

28. A partir dos anos 1930, as redes soviéticas de espionagem formadas por oficiais sem cobertura diplomática adquiriram um grau de eficiência e profissionalismo inédito na história da espionagem. Na Europa ocupada pela Alemanha nazista, a mais destacada dessas redes foi a Rote Kappelle (orquestra vermelha), dirigida por Leopold Trepper e Victor Sukolov. No entanto, o mais importante agente soviético naquela época foi Richard Sorge, um russo educado em Berlim e Hamburgo (onde obteve um PhD em ciência política no começo dos anos 1920). Operando primeiro para a III Internacional e depois para o GRU, Sorge cumpriu missões na Alemanha, Inglaterra, Escandinávia e China. Depois de construir uma estória de cobertura atuando como jornalista em Berlim, o GRU enviou Sorge para Tóquio em 1933. Lá, a partir de suas conexões com a embaixada alemã e com altos membros do governo japonês, Sorge foi capaz de informar sobre as intenções japonesas e de assegurar a Stálin e ao comitê central que o Japão não atacaria a União Soviética. Em 1941, a contra-inteligência japonesa detectou um dos principais agentes controlados por Sorge, o jornalista Hotsumi Ozaki, preso, torturado e executado juntamente com Richard Sorge em 1942. Cf. Richelson (1995:87-95) e Melton (1996:38-39). Ver também, para uma apreciação mais completa da capacidade analítica dos serviços de inteligência soviéticos antes e durante a II Guerra Mundial, bem como sobre as relações entre a área de inteligência e a liderança em torno de Stálin, Erickson (1984:375-423).

29. Nas áreas de inteligência de segurança (*security intelligence*), inteligência policial (*law enforcement intelligence*) e inteligência externa sobre terrorismo, muitas vezes a única fonte de informação relevante são os informantes e/ou agentes infiltrados nas organizações-alvo. Sobre o uso de informantes e obtenção de humint nessas áreas, ver o capítulo 4 (Gathering information) do livro de Gill (1994:135-178). Ver também, especialmente sobre uso de fontes humanas em inteligência policial, o volume coletivo da International Association of Law Enforcement Intelligence Analysts (Ialeia), Peterson (2000).

30. No caso dos Estados Unidos, a CIA esteve envolvida no desenvolvimento de projetos pioneiros nas áreas de inteligência de imagens e de sinais através de seu diretório de ciência e tecnologia (DS&T). Cf. Richelson (1995, *passim*).

31. Para uma reconstrução histórica da trajetória da disciplina de sigint, a referência obrigatória é o monumental trabalho de Kahn (1996).

32. Como salienta Matthew Aid: “*For example, in recent years a new generation of 128-bit encryption systems have been developed by private companies in US and elsewhere that offer a degree of encryption protection for commercial users that is several tens of thousands of times greater than the previously available 40-bit and 56-bit encryption systems. (...) NSA also has found in the last decade that some foreign military forces, particularly in Europe, have begun using new telecommunications technologies, such as speed spectrum links, laser point-to-point communications, fast frequency-hopping technology, tactical satellite communications, increased usage of*

*millimeter wave communication systems, data compression techniques, burst transmitters, imbedded decoy signals, encryption at all levels, and greater use of low-probability-of-intercept communications systems, such as walkie-talkies and even cellular telephones".* Ver Aid (2000:1-32).

33. Os diversos usos civis e militares do espectro de radiação eletromagnética para comunicação ocorrem a partir da designação de bandas de freqüência. A freqüência de uma transmissão é medida pelo número de oscilações por segundo, uma medida chamada Hertz. Assim, um quilohertz (1kHz) equivale a mil ciclos por segundo, 1 megahertz (1MHz) equivale a 1 milhão de ciclos por segundo etc. No nível mais baixo da escala de freqüências encontra-se a banda de freqüência que corresponde à audição (entre 20Hz e 20kHz). As bandas de freqüência utilizadas para a comunicação de longa distância através de sinais de televisão, rádio, radares, equipamentos de navegação e microondas vão de menos de 10kHz até algo entre  $10^2$ MHz e  $10^3$ MHz (indo, portanto, de *extremely low* até *extremely high*, subdivididas em ELF, VLF, LF, HF, VHF, UHF, SHF e EHF). Apenas para efeito de comparação, vale lembrar que radiações eletromagnéticas que correspondem a sinais de *laser*, infravermelho e luz visível encontram-se em bandas de freqüência entre  $10^3$ MHz e  $10^6$ MHz, enquanto os raios acima do espectro da luz visível, tais como os raios ultravioleta, raios x e os raios gama (liberados através de explosões nucleares, por exemplo), encontram-se em bandas de freqüência entre  $10^6$ MHz e  $10^{13}$ MHz.

Outro parâmetro importante para a obtenção de inteligência de sinais e também imint é o comprimento de onda que caracteriza a transmissão e os sensores necessários para sua captura. Sendo o comprimento de onda igual à distância entre uma onda e o mesmo ponto da próxima onda, na medida em que aumenta a freqüência diminui o comprimento de onda. A designação das bandas de freqüência corresponde a um certo número de canais. Por exemplo, comunicações em HF (de 3 a 30MHz) têm cerca de 300 canais de ondas longas, em VHF (de 112 a 135MHz) existem cerca de 2.300 canais de ondas médias e em UHF (entre 225MHz e 400MHz) são 1.750 canais de ondas curtas. Para um contraste entre os comprimentos de onda típicos da área de sigint e outros, microondas têm entre 0,03 e 3cm, a luz visível apresenta comprimentos de onda entre 0,38 e 0,7μm (um micron equivale a  $10^{-6}$  metros) e raios ultravioleta têm comprimentos de onda entre 0,03 e 0,38μm. Para mais detalhes, ver Kennedy (1983:76-95). Para uma abordagem integrada das várias dimensões de guerra eletrônica (EW), ver Browne & Thurbon (1998).

34. Os textos da comissão do Parlamento europeu que investigou o Echelon estão disponíveis em: <<http://www.loyola.edu/dept/politics/intel.html>>. As estações de interceptação do tráfego de Satcoms mencionadas no texto estão localizadas em Sugar Grove (West Virginia), Yakima (Washington), Sabana Seca (Porto Rico), Menwith Hill (Inglaterra), Bad Aibling (Alemanha) e na base aérea de Misawa (Japão). Além dessas seis estações operadas pela NSA, existem outras quatro, operadas pelos países signatários do pacto de cooperação na área de sigint assinado em 1948, chamado Ukusa. Essas quatro estações são localizadas em Morwenstow (Inglaterra), Leitrim (Canadá), Kojarena (Austrália) e Waihopai (Nova Zelândia). Em termos mais gerais, o pacto Ukusa visa a divisão de tarefas e o compartilhamento de informações (especialmente sigint) entre os governantes dos cinco países-membros. Consta que os Estados Unidos seriam responsáveis pela América Latina, maioria da Ásia, Rússia asiática e parte norte da China. A Austrália seria responsável pela vigilância de seu entorno regional – Indonésia, Indochina,

parte sul da China – e a Nova Zelândia cobriria o oeste do Pacífico. Caberia ao Reino Unido a África e a parte européia da Rússia, enquanto o Canadá cobriria as regiões polares da Rússia. Além da National Security Agency (NSA), as principais agências de inteligência de sinais envolvidas no acordo Ukusa são o Government Communications Headquarters (GCHQ) britânico, o Defence Signals Directorate (DSD) australiano, o Communications Security Establishment (CSE) canadense e o Government Communications Security Bureau (GCSB) da Nova Zelândia. O trabalho mais detalhado sobre os acordos entre os países anglo-saxões na área de sigint ainda é o de Richelson & Ball (1985).

35. Aid (2000:17-18).

36. No caso norte-americano, algumas das maiores estações de interceptação de Satcom são utilizadas também como estação de controle das missões dos satélites de sigint. Essas estações são operadas conjuntamente pela NSA e pela CIA e localizam-se em Menwith Hill (Inglaterra), Bad Aibling (Alemanha), Buckley Air National Guard Base (Colorado-US) e Pine Gap (Austrália). O principal centro de gerenciamento norte-americano dos satélites de sigint fica no quartel-general da NSA em Fort Meade (Maryland). A Marinha dos Estados Unidos opera três estações fixas de interceptação, localizadas em Diego Garcia, Guam e no estado do Maine. Essas estações processam as informações recebidas pela frota de satélites de vigilância oceânica (Parcae), também utilizados para a vigilância de alvos terrestres. Os comandos unificados centrais contam, desde meados da década de 1990, com três centros regionais de operações de sigint, localizados em San Antonio, Texas (para atender às necessidades do Southcom e do Centcom), Fort Gordon-GA (para atender o comando europeu e o Centcom na Europa, Oriente Médio, norte da África e Golfo Pérsico) e Kunia-HI (Pacom). Atualmente, cerca de 45 postos secretos de escuta são operados conjuntamente pela CIA e NSA em embaixadas norte-americanas em capitais no exterior. Além dessas estações fixas, as três forças armadas dos Estados Unidos utilizam 81 aeronaves especializadas em coleta de sigint (inclusive os EP-3E da Marinha, um dos quais colidiu com um caça chinês e esteve no centro da crise diplomática entre os dois países em 2001). Outras 38 aeronaves podem ser equipadas e convertidas rapidamente (inclusive U-2 que são utilizados primariamente para imint). Finalmente, a Marinha utiliza 61 navios equipados com centros de coleta e processamento de sigint (entre os quais há 11 *destroyers* da classe Arleigh Burke, 27 *cruisers* da classe Ticonderoga, cinco porta-helicópteros, seis navios de comando anfíbios da classe Wasp e outros 13 *destroyers*), além de recursos adicionais instalados nos submarinos nucleares de ataque da classe Los Angeles e nos submarinos de ataque remanescentes da classe Sturgeon. Para mais detalhes sobre as plataformas norte-americanas, ver Richelson (1999:185-205) e Aid (2000:14-17). Para uma visão geral da situação da área de sigint na União Soviética à época de seu colapso, ver Ball & Windrem (1989a) e (1989b).

37. Além dos satélites-espiões de imint e sigint, as Forças Armadas norte-americanas utilizam atualmente frotas próprias ou terceirizadas de satélites de navegação (Navstar Global Positioning Systems – Navstar GPS), comunicação (Defense Satellite Communications Systems – DSCS), mapeamento & geodesia (Landsat 7) e mesmo meteorologia (Defense Meteorological Support Program – DMSP). Incluindo os gastos da Nasa com lançamentos de foguetes e ônibus espaciais para orbitar satélites de uso militar, mais a parte da CIA no orçamento do NRO, bem como os gastos dos usuários com estações de terra para controle, o orçamento espacial para fins de segurança nacional chegava a mais de US\$25 bilhões/ano nos Estados Unidos em 1997.

Para uma introdução ao uso do espaço para coleta de inteligência (reconhecimento e vigilância), ver Kennedy (1983:96-119). Para um tratamento mais comprehensivo e bastante acessível dos diversos usos do espaço para fins militares, ver Dutton (1990).

38. Parâmetros orbitais ajudam a entender as funções dos diversos tipos de satélites-espionas: reconhecimento, vigilância eletrônica, alerta nuclear avançado, vigilância oceânica, interceptação de comunicações, *tracking* de satélites, relés de comunicação etc. Cf: <[www.fas.org/spp/military/program/index.html](http://www.fas.org/spp/military/program/index.html)>. Para uma explicação sintética sobre os principais parâmetros orbitais (altitude, ângulo de inclinação, *ground tracks*, velocidade orbital, período orbital etc.), ver o capítulo 1 de Dutton (1990:9-29).

39. Note-se que órbitas de satélites sofrem perturbações decorrentes da forma irregular da Terra (um esferóide oblato com massa extra nas regiões equatoriais). São perturbações decorrentes da rotação do plano orbital sobre o eixo polar (regressão nodal), da rotação do eixo maior (apsidial), da atração causada por inúmeros campos magnéticos, do impacto de micrometeoros e da ação do vento solar. Um outro efeito decisivo sobre as órbitas é, portanto, sobre o tempo de vida útil dos satélites é que, mesmo sob a baixa densidade do ar na atmosfera em alturas orbitais, a atmosfera terrestre continua a dragar os satélites a cada passagem pelo perigeu (o ponto mais próximo da Terra em um dado plano orbital). A uma altitude orbital de cerca de 88km de perigeu a energia cinética gerada pela dragagem atmosférica produz calor suficiente para queimar o satélite na reentrada. Portanto, o período orbital mais curto suportado equivale a 89 minutos. Em resumo, para manter uma órbita qualquer, e órbitas geossíncronas em especial, os satélites precisam de constantes ajustes por parte dos foguetes propulsores da espaçonave. Os problemas técnicos e científicos associados são de extrema complexidade. Cf. Dutton (1990:18-51).

40. US Congress (1998a). Disponível na internet em: <[www.nro.odci.gov](http://www.nro.odci.gov)>.

41. Além da bibliografia já mencionada nas notas anteriores, ver Oxlee (1997). Ver também o capítulo sobre imint em Richelson (1999:241-256).

42. Segundo Michael Herman (1996:72-73), embora tenha sido menos reconhecida do que os esforços na área de criptologia, a interpretação das fotos obtidas pelos esquadrões de reconhecimento das forças aliadas na Europa foi um componente decisivo da superioridade de inteligência com a qual contavam os aliados a partir da segunda metade da guerra. Ao final da guerra, a principal organização anglo-americana de imint, conhecida como Allied Central Interpretation Unit, processava 25 mil negativos por dia, possuindo então um acervo de mais de 5 milhões de negativos e mais de 40 mil relatórios de interpretação fotográfica em seus arquivos. Atualmente, a principal organização responsável por análise e processamento de imagens no sistema de inteligência britânico é o Jaric, um centro subordinado ao Estado-maior integrado. Nos Estados Unidos a área de imint é menos centralizada do que a área de sigint, que se estrutura em torno da NSA. Enquanto o NRO e a Força Aérea controlam a contratação e o desenvolvimento de satélites, na década de 1990 uma série de elementos organizacionais anteriormente localizados na CIA e nas Forças Armadas foi consolidada numa agência governamental especializada em cartografia militar digitalizada e produção/interpretação de imagens: a Nima (National Imagery and Mapping Agency). Além dessas agências, há que se considerar também o papel da organização responsável pelo desenvolvimento de plataformas e sistemas de imint aerotransportados, o Daro (Defense Airborne Reconnaissance Office).

43. Para um breve histórico da aviação de reconhecimento até o desenvolvimento de satélites-espiões, ver os capítulos 2 e 3 do livro de Burrows (1988).

44. As especificações originais do U-2, que entrou em operações em 1956, podem ser comparadas com as atuais a partir dos dados disponíveis na página da internet da Federation of American Scientists em: <[www.fas.org/irp/program/collect/u-2.htm](http://www.fas.org/irp/program/collect/u-2.htm)>. Os aviões U-2 atuais (U-2S/ST) têm velocidade máxima de 510mph, altitude máxima de 90.000f e alcance de 3.500 milhas. Os modelos básicos coletam imagens utilizando vários sensores distintos: radares, eletroópticos e termais/infravermelhos. Apesar da grande altitude de vôo, a assinatura de radar do U-2 é clara e detectável, e a frota norte-americana atual de 35 U-2 está sendo repotencializada para diminuir a assinatura e aumentar a capacidade dos motores, sensores e geração elétrica da aeronave, que deve permanecer em operações até 2020. Os U-2 voaram mais de 800 missões durante a Guerra do Golfo (1990/91), além de operarem nas diversas intervenções das forças norte-americanas no Oriente Médio, Leste asiático e Balcãs até a presente data. Cerca de 100 aviões desse tipo já foram produzidos em diversas versões, a maioria equipada com sensores de imint e sigint (pelo menos uma versão foi equipada para retransmissão de dados de inteligência dos satélites – U-2R – e outra foi desenvolvida para uso civil para a Nasa, sob a denominação de ER-1).

Outras plataformas aerotransportadas no arsenal norte-americano incluem um número não conhecido de aviões de espionagem SR-71 Blackbirds, cerca de 200 P-3C da Marinha utilizados para imint, além de outros aviões modificados e equipados com sistemas de câmeras e sensores de imagens, desde caças F-14, aeronaves de reconhecimento EO-5 do Exército e mesmo alguns C-130.

O SR-71 entrou em operações em 1964 e permanece até hoje como o avião mais veloz e de maior altitude no mundo. Fabricado a partir de uma liga de titânio e com um design específico para redução da assinatura de radar, o SR-71 é menos vulnerável à interceptação e foi um precursor do uso de tecnologia *stealth* (invisível). Atualmente, as câmeras fotográficas do SR-71 podem vasculhar 160,9 mil km<sup>2</sup> por hora. Sua velocidade máxima é de 2.193mph (Mach 3.31) e sua altitude máxima é de 85.000f. Devido ao altíssimo custo de construção e de operação, os SR-71 nunca chegaram a substituir os U-2.

Especialmente depois da Guerra do Golfo, o Pentágono passou a investir pesadamente em *drones* (aviões sem piloto, chamados também de UAVs) para o reconhecimento avançado do território inimigo. Os modelos mais importantes no arsenal daquele país são os Pioneer (equipados com infravermelho e câmeras de TV), os Predators (com alcance de 500 milhas náuticas e equipado com sensores SAR e infravermelho) e os Global Hawks (com autonomia de vôo de 20 horas e 3.500 milhas náuticas de alcance). Ver Richelson (1999:161-167).

45. Apesar da má qualidade das fotos obtidas, a primeira passagem de um satélite Corona norte-americano sobre o território soviético obteve uma cobertura de 1,6 milhão km<sup>2</sup>, bem mais do que a soma obtida por quatro anos de sobrevôos com os U-2. O texto mais recente de Burrows, onde ele sistematiza os principais marcos históricos norte-americanos e soviéticos/russos no desenvolvimento de satélites de imint, foi publicado na internet há poucos anos; ver Burrows (1999), disponível em: <<http://webster.hibb.no/asf>>.

46. Resolução é uma das principais medidas num sistema de coleta de imagens. Quanto menor o valor da resolução de imagem, maior a precisão permitida pela interpretação. Uma resolução de um metro não quer dizer que o sistema óptico empregado só

pode ver coisas de um metro de tamanho ou maiores, mas sim que não se consegue distinguir entre duas coisas diferentes que estejam a menos de um metro de distância entre si. Há que se considerar também diferentes graus de precisão requeridos para detecção, reconhecimento, identificação, descrição e produção de inteligência técnica de diferentes tipos de alvos (praias, pontes, campos de pouso, foguetes, navios, submarinos, aviões, tanques, concentrações de tropas etc.). Uma fragata, por exemplo, requer 15m de resolução para ser detectada do espaço, 4,5m para sua classe poder ser reconhecida, 15cm para ser identificada individualmente (“assinatura”) e 5cm de resolução para que se possa obter inteligência sobre detalhes técnicos a partir das fotos. Como regra geral: “*The angular resolution capability of any surveillance device is directly proportional to the wavelength of the incoming signal (light or radar etc.) and inversely proportional to the aperture diameter of the collection device (lens or antenna)*”. Dutton (1990:96). Portanto, pode-se esperar uma resolução melhor de sensores ópticos (cuja largura de onda no espectro eletromagnético está na faixa de 0,5 mícron) do que de sensores infravermelhos (10 mícrons), mas isso depende dos diâmetros das lentes e da largura das antenas.

Os satélites comerciais de imagens norte-americanos Landsat 4 e 5, lançados no começo da década de 1980 e ainda em operações, podem prover imagens de 178km por 164km de *swath width* com 30m de resolução. Um acordo assinado em 1993 entre a Nasa e o NRO para o desenvolvimento de um Landsat 7 com sensores multiespectrais e resolução de 5m tem sido relatado pela imprensa como inefetivo até o momento. Por sua vez, os satélites comerciais franceses Spot (Système Probatoire d’Observation de la Terre), orbitados a partir de 1986, possuem capacidade para gerar imagens fotográficas com 10m de resolução e imagens multiespectrais com 20m de resolução. Embora a resolução do Spot seja melhor do que a dos sistemas Landsat, a cobertura de área é bem menor, com uma *swath width* de 58km por 58km. Em 1999, ambas as empresas (norte-americana e francesa) prometiam resoluções de 1m para o começo do novo século. A partir de 1992, os satélites comerciais russos PECYPC (equipados com sistemas de câmara KVR-1000) passaram a oferecer ao mercado imagens com resolução de 2m. Embora a barreira de 1m de resolução para imagens comerciais provavelmente já tenha sido ou esteja para ser quebrada ainda nesta década pelos satélites comerciais russos e europeus, os controles baseados em critérios de segurança nacional para a venda de imagens com melhor resolução ainda são fortes, e tais vendas são aprovadas caso a caso. Ver Burrows (1999:15-18).

47. Atualmente, os Estados Unidos operam dois tipos de satélites-espionas dedicados à coleta de imint. O primeiro tipo (Keyhole/Crystal) é formado pelos três satélites conhecidos como KH-11 *advanced*, lançados entre 1992 e 1996. Com órbitas circulares mais elevadas, de 250km por 998km, e ângulo de inclinação de quase 98°, os satélites KH-11 *advanced* cobrem uma quantidade muito maior de alvos, alguns dos quais até quatro vezes por dia. São equipados com sensores eletróópticos, infravermelhos e termais, além de sistemas para identificação métrica das imagens produzidas. Com uma vida útil de cerca de oito anos, a substituição das atuais espaçonaves em órbita deverá ser feita na primeira metade da década de 2010. Obviamente, a amplitude de cobertura e a resolução das imagens produzidas pelos KH-11 *advanced* são segredos de Estado. Mas, baseados em capacidades de gerações anteriores de satélites-espionas norte-americanos, estima-se que a resolução atual seja inferior a 10cm. As imagens coletadas por esses três “big birds” são enviadas através de satélites relés de comunicação para a estação principal de controle da missão, em Fort Belvoir, no estado da Virgínia. O segundo tipo de satélite

(Lacrosse/Vega) é composto por três espaçonaves que empregam sistemas avançados de imagem por radar, ao invés dos sensores infravermelhos e eletroópticos do programa Keyhole, o que permite a obtenção de imagens mesmo quando os alvos estão encobertos por nuvens (caso de grande parte da Europa oriental e da Rússia asiática durante o inverno no hemisfério norte). Lançados com 57° ou com 68° de inclinação em órbitas de 643km de altitude, os satélites Vega orbitados depois de 1997 têm resolução muito maior do que modelos anteriores, chegando a 90cm. Os dados coletados pelos satélites Vega também são transmitidos em formato digital através de satélites relés em órbitas elípticas, e a principal estação de controle desses satélites é localizada em White Sands, no estado de New Mexico; cf. Richelson (1999:157-159). Sobre parâmetros orbitais, ver os capítulos já citados em Dutton (1990). Ver ainda Jasani (1990).

Para as sucessivas gerações de satélites norte-americanos, ver Burrows (1986 e 1999). Para uma breve descrição dos satélites comerciais e dos satélites russos, chineses, franceses, japoneses, israelenses e sul-africanos, ver Richelson (1995 e 1999). Para uma introdução geral ao sensoriamento remoto, ver Campbell (1987).

48. O valor das evidências visuais para a obtenção e a produção de inteligência depende não apenas da resolução das imagens, mas também da velocidade e da amplitude da área que se pode cobrir, da agilidade com que se pode processar as imagens para passá-las aos fotointérpretes, da fração de tempo necessária para a obtenção de cada tipo de imagem e da capacidade de ampliação das imagens sem distorção informacional. Com exceção da resolução e da capacidade de ampliação (itens nos quais as plataformas aerotransportadas são superiores aos satélites), de modo geral as imagens digitais transmitidas através de satélites relés ou diretamente para as estações de controle em terra são superiores em todos os aspectos, principalmente quando combinadas com dados de elevação de terreno e outros bancos de dados cartográficos e georreferenciados. Ver Richelson (1999:170-171).

49. É útil lembrar que um equipamento fotográfico pode utilizar filme quimicamente preparado ou sensores eletroópticos. Enquanto uma câmera convencional registra as variações dos níveis de luminosidade refletidos por todos os objetos separados de uma cena (sendo que a quantidade de objetos é uma função da resolução angular), um sensor eletroóptico converte as variações nos níveis de luminosidade em sinais elétricos. Um valor numérico é atribuído a cada um desses sinais, chamados de elementos pictóricos, ou pixels. Com esse processo, uma imagem analógica é transformada em digital e pode ser transmitida eletronicamente para pontos distantes, onde receptores podem decodificar e reconstruir os sinais em formato analógico. Após o processo estar completo, fotografias e vídeos podem ser analisados para fins de produção de inteligência. Ver Richelson (1999:151).

50. Como já foi observado em nota anterior, quanto "menor" o valor da resolução, melhor para a interpretação. Na medida em que a resolução de uma imagem é diretamente proporcional ao comprimento de onda do sinal recebido e inversamente proporcional ao diâmetro da abertura do sensor (lente ou antena), para se obter uma imagem com resolução de 1m a partir de satélites em altitudes orbitais de 250km, sensores eletroópticos capazes de detectar sinais com comprimento de onda no espectro de luz visível (cerca de 0,5 mícron) precisariam de lentes de 12cm de diâmetro, enquanto sensores termais capazes de detectar sinais com comprimento de onda no espectro infravermelho (10 mícrons) precisariam de lentes de 2,5m para obter a mesma resolução. Entretanto, como o comprimento de onda de sinais de radar é medido em centímetros, seria neces-

sária uma antena de 7,5km de diâmetro para se obter uma resolução de um metro. Ora, mesmo tendo conseguido contornar a evidente dificuldade surgida daí através da simulação do comprimento da antena com o movimento do próprio satélite (uma técnica chamada de SAR, ou Synthetic Aperture Radar), a resolução das imagens de radar era até meados da década de 1990 centenas de vezes pior do que a resolução das imagens eletroópticas. Segundo Dutton (1990:108), imagens SAR com resolução de 25m eram possíveis a partir de radares equipados com satélites-espionas no começo da década de 1990. Entretanto, segundo Richelson (1999:155), os atuais sistemas de coleta de imagem através de radar utilizados pelos satélites Vega norte-americanos, orbitados depois de 1997, conseguem resoluções de até 90cm (*sic*).

51. US Government (1998), apud Davis (1996).

52. A interpretação de imagens é caracterizada por simultaneidade, percepção gestáltica e apurado senso de espacialidade (afinal, ao contrário de letras, fonemas ou mesmo palavras numa sentença, não se pode “ler” pixels individualmente). Para um argumento enfático sobre as dificuldades associadas à educação de analistas militares na arte de interpretação de imagens (uma vez que analistas militares tendem a ser treinados para apoiar-se em procedimentos lógicos de seqüenciamento, descrição, análise e abstração), ver Marshall (1999:57-84). Além das referências que constam na bibliografia do artigo de Marshall, um ponto de partida para maiores aprofundamentos poderiam ser os artigos da revista especializada *Photogrammetric Engineering & Remote Sensing*.

53. Ver a tabela de alvos das operações norte-americanas de coleta de imint apresentada por Jeffrey Richelson (1999:155-157), onde se destacam alvos militares, instalações físicas de grande porte (pontes, palácios presidenciais, fábricas etc.) e concentrações humanas significativas (tropas, refugiados etc.). Aceitando por um instante a tabela de Richelson como referência, os países prioritariamente vigiados pelos Estados Unidos ao longo da década de 1990 foram Argélia, Bósnia, China, Coréia do Norte, Croácia, Cuba, Índia, Iraque, Israel, Jugoslávia, Laos, Líbano, Líbia, Paquistão, Ruanda, Rússia e Ucrânia.

54. Nos Estados Unidos, a área de masint é coordenada desde 1993 pelo Central Masint Office, um componente da agência de inteligência do Pentágono, a DIA. Cf. US Congress (1996).

55. Sobre os satélites de vigilância de Nudet (nuclear detonations), Cf. Ziegler & Jacobsen (1995).

56. US Government (1997a) apud Richelson (1999:235).

57. Berkowitz & Goodman (2000:1-29).

58. Richelson (1999:274-279).

59. Na literatura norte-americana sobre o tema, a prescrição sobre a separação entre inteligência e *policymaking* remete ao influente livro de Kent (1949). Perspectiva semelhante pode ser encontrada ainda hoje em Berkowitz & Goodman (1991).

No entanto, resta cada vez menos do otimismo liberal sobre o papel da inteligência nos processos de tomada de decisões governamentais. Seria mesmo esperável uma visão mais realista sobre a relação entre governantes e conhecimento, pelo menos depois que Herbert Simon modificou suas posições sobre as precondições institucionais para um processo de tomada de decisões mais racional. Ou depois que Charles Lindblom escreveu seus

livros incrementalistas e pluralistas sobre o processo de tomada de decisão como “*muddling through*”, ou depois da teoria comportamental da firma de March & Olsen (1995) ou, mais influentes hoje em dia, depois dos modelos econômicos de decisão baseados em “*bounded rationalities*”, derivados da teoria dos custos de transação e da teoria sobre as relações entre “*principals and agents*”. São exemplos do impacto dessas diversas abordagens na literatura sobre inteligência os trabalhos de Heyman (1985), Hulnick (1986), Hibbert (1990) e Herman (1991). Ver também Lowenthal (1992:157-168).

60. A confusão entre as duas coisas (“informar para tornar melhor o processo decisório” e “aconselhar sobre a melhor decisão”) perpassa o influente trabalho sociológico de Wilensky sobre inteligência organizacional, onde ele define como informação útil aquela que é clara, compreensível, confiável, válida, adequada e “*wide-ranging, because the major policy alternatives promising a high probability of attaining organizational goals are posed or new goals suggested*”. A sugestão de objetivos organizacionais não me parece ser uma função que deva ser atribuída às organizações de inteligência, uma vez que isso embute um risco claro de renúncia dos responsáveis pela tomada de decisões. Os elementos de barganha política e construção coletiva que caracterizam o processo de construção dos objetivos organizacionais não deveriam ser substituídos pela consulta às organizações de inteligência, convertidas assim em oráculos; cf. Wilensky (1967:viii). Por outro lado, exigências de maior proximidade entre inteligência, tomada de decisões e planejamento de políticas no governo norte-americano na década de 1990 levaram a CIA a reorientar seus produtos analíticos na direção da sugestão de cursos de ação específicos, conforme, principalmente, Davies (1992).

61. Para uma discussão crítica da noção de “falha de inteligência” com base em alguns dos casos históricos antes mencionados, ver Lowenthal (1985:43-56). Para uma discussão mais geral sobre falhas analíticas em inteligência, ver Herman (1996:240-256).

62. No caso dos Estados Unidos, as principais organizações de análise e produção de relatórios de inreligência são o diretório de análise (DI) da CIA, o diretório correspondente na DIA, o INR do Departamento de Estado e o NIC do ODCAI. Para uma visão do estado-da-arte atual na reflexão sobre análise e produção de inteligência no âmbito da CIA, ver Davies (1995). Ver também o livreto eletrônico do diretório de análise (DI) da CIA com recomendações sobre os processos de trabalho na área de análise: <<http://www.odci.gov/cia/di/toolkit>>. Ver ainda a monografia de Heuer Jr., (1999). Um livro mais extenso sobre o processo de elaboração das chamadas “estimativas nacionais” de inteligência nos Estados Unidos (os produtos analíticos produzidos no vértice da IC através do sistema de analistas do NIC) é o de Ford (1993).

63. Ver, por exemplo, o material de divulgação da CIA/ODCI. US Government (1999a).

64. Para uma discussão sobre os temas substantivos e os métodos analíticos norte-americanos no contexto pós-Guerra Fria, a qual leva em conta as possibilidades introduzidas pelas novas tecnologias de informação e comunicação (TICs), ver o capítulo 4 (The problem of analysis in the new era) em Berkowitz & Goodman (2000:99-123).

65. Sobre os problemas de avaliação de efetividade, eficiência e eficácia nos processos produtivos da área de inteligência, ver a parte V (Evaluation and Management) do livro de Herman (1996:281-338). Um artigo muito interessante e útil, sobre critérios para a escolha de software de banco de dados e aplicativos na área de inteligência policial, é o de Olligschlaeger (2000:171-191).

66. Sobre o impacto potencial das análises e dos produtos de inteligência no processo de tomada de decisões, vale reproduzir um trecho de Michael Herman: “*Intelligence's ideal is to transfer its own analyses, forecasts and estimates of probabilities to the user's consciousness in toto. But it is doing well if it ever gets near it. The decision-taking black box works through selectivity. (...) Intelligence's justification is that it influences action in useful ways. But these uses are very varied: some reports are used immediately, while others are useful in the distant future; many more reports influence decisions through their cumulative effects; others still have long-term educational or psychological value. Warning surveillance is a precaution against what may never happen. Much intelligence is never used at all. In all these ways it is like other information. Nevertheless the effect is to optimize national strength and international influence, on varying scales*”.

Herman (1996:155).

67. Para uma crítica mais ou menos recente sobre a má distribuição de inteligência para os usuários finais, especialmente na área de imint, ver novamente US Congress (1993).

68. Martin (1999:53-56). Embora todo o livro de Frederick Martin sobre o Intelink seja útil para se compreender a dinâmica operacional das agências de inteligência norte-americanas, depois de uma visão geral sobre as várias camadas do Intelink (capítulo 2), vale destacar os capítulos que lidam mais diretamente com os problemas de segurança decorrentes da construção de redes fechadas a partir de padrões e protocolos abertos (capítulos 3-5), bem como os capítulos que tratam das categorias de serviços e ferramentas disponíveis para os usuários nas áreas de pesquisa, trabalho colaborativo, tradução simultânea, implementação de metadados, publicação eletrônica, comunicação e treinamento (capítulos 6-7).

69. A breve discussão desse ponto na seção Segurança de informações e contra-inteligência deste livro não faz jus à sua importância para o estudo das atividades de inteligência. A abordagem proposta baseia-se também aqui em Herman (1996:165-199). Um outro artigo importante para esclarecer a relação entre a disciplina de contra-inteligência e as áreas de inteligência externa (*foreign intelligence*) e de infosec é o de Jelen (1991/92:381-399). Para uma introdução sistemática aos temas de segurança nas redes de computador na área de inteligência, ver o livro já citado de Frederick Martin (1999:65-167).

70. Por segurança informacional (infosec) entenda-se algo bem mais limitado do que as noções muito mais abrangentes de “segurança nacional” e “segredo governamental”, as quais serão discutidas com o nível de abstração adequado no capítulo 3 deste livro. É preciso atenção também para não confundir as operações de segurança informacional com a chamada área de inteligência de segurança (*security intelligence*), também chamada de inteligência doméstica ou interna, a qual é dedicada à obtenção e à análise de informações sobre as chamadas “ameaças internas” à segurança nacional. Ver Herman (1996:165-167).

71. Jelen (1991/92:389-390).

72. Sobre a integração das medidas regulares de Infosec/SCM no planejamento de operações defensivas de guerra informacional (IW), ver Alberts (1996).

73. Para uma introdução à literatura especializada sobre *deception*, ver Daniel & Herbig (1982). Referências adicionais podem ser encontradas em Shulsky (1992:252-253n).

74. Um exemplo típico dessa abordagem é o capítulo 5 (*Spy vs. Spy*), bastante completo e instrutivo, por sinal, do livro de Shulsky (1992:111-144). No Brasil, utiliza-se comumente o termo contra-inteligência para designar a “proteção ao conhecimento” ou a “segurança orgânica” das organizações de inteligência. Pelas razões apresentadas nesta seção, creio que esse entendimento induz a uma perda de foco no que consiste, afinal, o cerne das operações de contra-inteligência: neutralizar e comprometer o ciclo de inteligência de um adversário naquelas operações em que somos o seu alvo. Até que ponto seria recomendável alocar todas as medidas de SCM, CI e opsec sob um “guarda-chuva” organizacional chamado infosec eu ainda não sei, mas até onde pude compreender das leituras realizadas isso é impossível em função das especificidades técnicas e culturais, especialmente da área de contra-inteligência *stricto sensu*.

75. Para um tratamento mais extenso do tema da contra-inteligência na mesma direção que Shulsky (1992), ver os capítulos 3 (*Building and rebuilding: counterintelligence since World War II*) e 5 (*Offensive defense: principles of counterintelligence*) do livro de Godson (1995).

76. A analogia utilizada por Michael Herman (1996:180) para explicar essa dinâmica é com a luta pelo comando do ar. Assim como uma força aérea precisa derrotar a força aérea adversária para poder utilizar todo o seu poder ofensivo, a contra-inteligência precisa neutralizar os aviões inimigos antes que eles decolem, ou então deve derrotá-los no ar, como uma precondição para o estabelecimento do “comando do ar”.

77. Para uma exposição sintética da formulação clausewitziana sobre a limitação concreta da guerra e a lógica conceitual de subida aos extremos, ver o capítulo 3 (*Os fundadores do pensamento estratégico*) do livro de Proença Jr., Diniz & Raza (1999:54-90).

78. Além dos romances de John Le Carré, muitos dos quais tematizam o mundo de sombras morais dos oficiais de contra-inteligência, a história do século XX tem seu quinhão de exemplos reais, entre os quais destacam-se os casos de Kim Philby (o espião soviético que chegou a ser o chefe da contra-inteligência no SIS britânico no final dos anos 1960) e Aldrich Ames (o espião soviético que chegou a ser chefe da seção soviética da unidade de contra-inteligência da CIA norte-americana nos anos 1980 e 1990). Hulnick (1995).

79. No caso dos Estados Unidos, a primeira referência às *covert actions* na legislação federal aparece apenas em 1974 (*The Hughes-Ryan Amendment*, Section 662 do *Foreign Assistance Act of 1962 as amended – 22, USC. 2242*), não obstante o crescimento das operações encobertas da CIA no exterior desde 1947. Atualmente, as operações encobertas são reguladas pelo *National Security Act of 1947 as amended*, bem como pelas diretrizes constantes na *Executive Order 12.333 of 1981*. A definição soviética de medidas ativas é retirada de Shultz & Godson (1984:193). O termo britânico é encontrado, por exemplo, em Godson & Robertson (1987:37-46).

80. A maior parte das referências sobre operações encobertas refere-se às experiências norte-americanas. Vários livros importantes sobre política externa e/ou sobre inteligência possuem um capítulo sobre o tema: Lowenthal (2000:106-119), Shulsky (1992:83-109), Holt (1995:135-167), Johnson (1996:60-88), Berkowitz & Goodman (2000:124-146), ou ainda Richelson (1999:349-373). Para um tratamento mais extenso em termos de exemplos, mas bastante comprometido com a defesa do “valor das operações encobertas”, ver os capítulos 2 (*Steps and missteps: covert action since 1945*) e 4 (*Handmaiden of policy: principles of covert action*) de Godson (1995).

81. Para uma história crítica e bastante completa das operações encobertas dos Estados Unidos até a década de 1980, ver Prados (1996). Para o caso francês, ver Porch (1995). Sobre as operações soviéticas, ver Richelson (1986). Também pode ser de algum interesse a descrição dos requerimentos informacionais e diretrizes operacionais soviéticos, realizada pelo historiador britânico e pelo ex-espião do SIS na KGB, Oleg Gordievsky. Ver Andrew & Gordievsky (1990).

82. Obviamente essa estimativa pode estar muito deflacionada. Afinal, trata-se de operações encobertas, sobre as quais supostamente ninguém deveria saber coisa alguma. Ver Hedley (1995).

83. Sobre o processo decisório e os problemáticos mecanismos de *accountability* das operações encobertas nos Estados Unidos, ver Holt (1995:135-167).

84. Sobre o caso britânico, ver Andrew (1986b). Sobre a emergência das operações encobertas nos Estados Unidos e sua posterior consolidação organizacional, ver o capítulo 2 deste livro.

85. Nos Estados Unidos, uma diretriz presidencial de 1995 (PDD-35) delimita quatro tipos básicos de operações de inteligência: 1. suporte a operações militares (SMO); 2. suporte às políticas públicas; 3. suporte à imposição da lei (“*law enforcementintelligence*) e 4. contra-inteligência (CI). Embora tal delimitação tenha sido funcional para o governo norte-americano durante a racionalização do processo orçamentário promovida em 1996, do ponto de vista operacional ela é excessivamente restritiva. Por isso optei por descrever as expectativas típicas dos usuários e não apenas as dinâmicas operacionais. Para a descrição das quatro operações da PDD-35, cf. [<www.fas.org/irp/ops>](http://www.fas.org/irp/ops).

86. Telegrama interceptado durante a I Guerra Mundial pela organização criptológica da Marinha Real britânica (*Room 40*), no qual a Alemanha propunha ao México que atacasse os Estados Unidos em troca da reconquista dos territórios perdidos na guerra de 1844, caso a Alemanha vencesse a guerra. A revelação do conteúdo do telegrama foi um dos fatos que levou os Estados Unidos a entrarem na guerra do lado dos britânicos e franceses. Cf. Richelson (1995:43-46).

87. Sobre o impacto geral da inteligência sobre a capacidade do Estado na guerra e na paz, ver o capítulo 8 (*Intelligence and national action*) de Herman (1996:137-155).

88. O acrônimo OODA (*observe-orient-decide-act*) descreve uma seqüência de passos fundamentais no ciclo da práxis. Tempo é o elemento crítico na execução de um ciclo de observação-orientação-decisão-ação e, numa confrontação entre dois atores, aquele que executa o ciclo OODA com maior agilidade tem uma vantagem evidente sobre o oponente. A imagem utilizada por Proença jr. & Diniz (1998:66n) para ilustrar a importância da agilidade com que cada lado reage à mudança é a de uma luta de boxe, onde um dos contendores opera com um ciclo OODA longo, movendo-se em câmara lenta, enquanto o outro opera com um ciclo OODA curto, movendo-se em velocidade normal. A atividade de inteligência é decisiva para as etapas de observação (“*visualizing*”) e orientação (“*situational awareness*”) do ciclo OODA, não apenas no interior de cada ciclo mas, também, em função do aprendizado organizacional permitido pela função de inteligência, na melhoria de desempenho do ciclo ao longo do tempo. A melhoria do desempenho dos processos de tomada de decisão a partir da

capacidade de aprendizado gerada por sistemas e processos de inteligência é um dos fatores de aumento da taxa de sobrevivência das forças em combate ("survivability"). Para uma avaliação das novas capacidades de visualização do campo de batalha surgidas desde a II Guerra Mundial, em sua relação com o desiderato da dominância sobre o ciclo OODA adversário, ver McDonald (1997).

89. Sobre inteligência e performance das estruturas de comando e controle (C2), ver Stares (1991). Para uma discussão recente sobre a formulação clausewitziana a respeito, ver Ferris & Handel (1995).

90. Para uma discussão detalhada sobre inteligência e operações militares em três guerras (Guerra Civil dos Estados Unidos, I Guerra Mundial e II Guerra Mundial), ver os diversos ensaios do volume organizado por Handel (1990). Ver, em especial, o longo ensaio introdutório do próprio Handel (p. 1-95).

91. Por isso: "*The technology challenge lies in building filters at all levels to sort massive amounts of data by type, time, and spatial orientation to meet the critical requirements of the commander. Only by limiting information requirements can commanders approach becoming a unitary actor at lower levels and fully exploit the advantages of faster decision cycles*". Ver McDonald (1997:167).

92. Kahn (1995). A sistematização anterior da proposição teórica de Kahn foi feita por O'Toole (1990:39-46). O'Toole baseia-se nas conclusões de um livro anterior de David Kahn, sobre os serviços de inteligência alemães durante a II Guerra. Ver Kahn (1978).

## Capítulo 2

# **Inteligência: perfil organizacional**

*The intelligence and security activities of the nations (...) are the products of many factors – national interests, international obligations (...), the technology available for intelligence collection, and the resources a particular nation can afford to devote to intelligence and security activities.*

Richelson (1988:307).

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, a defesa nacional e a garantia da ordem pública de um país. Serviços de inteligência são órgãos do Poder Executivo que trabalham prioritariamente para os chefes de Estado e de governo e, dependendo de cada ordenamento constitucional, para outras autoridades na administração pública e mesmo no Parlamento. São organizações que desempenham atividades ofensivas e defensivas na área de informações, em contextos adversariais onde um ator tenta compelir o outro à sua vontade. Nesse sentido, pode-se dizer que essas organizações de inteligência formam, juntamente com as Forças Armadas e as polícias, o núcleo coercitivo do Estado contemporâneo.<sup>1</sup>

Serviços de inteligência não são meros instrumentos passivos dos governantes, agentes perfeitos de sua vontade ou mesmo materializações de um tipo ideal de burocracia racional-legal weberiana. Antes de mais nada, porque sua atuação impacta as instituições e o processo político de muitas formas e porque essas organizações têm seus próprios interesses e opiniões acerca de sua missão. Embora o tema da intervenção dos serviços de inteligência e de segurança na vida política mais geral seja de grande interesse, tratar os serviços de inteligência como variáveis independentes que influenciam as instituições políticas tende a ser um esforço frustrante quando se sabe tão pouco sobre a origem e o desenvolvimento desses serviços.<sup>2</sup> Por isso, no texto que se segue, os serviços de inteligência serão considerados variáveis dependentes. Como não existem ainda estudos sistemáticos sobre o processo através do qual os serviços de inteligência chegaram ou poderiam

chegar a tornar-se organizações dotadas de “valor e estabilidade”, ou seja, instituições, o procedimento expositivo adotado procurará responder sistematicamente à pergunta sobre a origem, o desenvolvimento e a atual configuração organizacional dos sistemas nacionais de inteligência, mas sem deixar de explicitar as lacunas existentes no conhecimento a respeito.<sup>3</sup>

## O Estado moderno e a função de inteligência

As primeiras organizações permanentes e profissionais de inteligência e de segurança surgiram na Europa moderna a partir do século XVI. Tais organizações surgiram no contexto da afirmação dos Estados nacionais como forma predominante de estruturação da autoridade política moderna.<sup>4</sup>

Como se sabe, o processo de afirmação dos Estados nacionais europeus foi marcado por importantes conflitos sociais, descontinuidades históricas e uma intensa competição entre os Estados nacionais e desses Estados com outros tipos de unidades políticas, particularmente os impérios, as cidades-estado e as ligas de cidades. A melhor explicação disponível sobre essa dinâmica é fornecida por Tilly (1996).<sup>5</sup>

O argumento de Tilly pode ser resumido assim: a posse concentrada de meios de coerção foi utilizada por grupos sociais previamente dominantes na ordem feudal, em alguns casos aliados à burguesia ascendente nas cidades, para aumentar a população e o território sobre os quais pretendiam exercer poder. A gênese desse processo está relacionada a pressões impostas pelos califados árabes e pelas movimentações de povos na estepe oriental da Europa, que forçaram os governantes europeus a redefinirem competitivamente suas bases de dominação política e sua infra-estrutura econômica. Quando uma coalizão que tentava expandir sua base de recursos encontrou grupos com meios de força comparáveis e que tornavam muito elevados os custos da dominação, a guerra foi o mecanismo de resolução do impasse.

Conquistadores transformaram-se em governantes quando tentaram exercer um controleável sobre as populações e territórios cada vez mais extensos, única forma de garantir um acesso regular aos bens e serviços ali produzidos. Nas diversas regiões da Europa e depois do mundo os governantes mais poderosos fixaram os termos da guerra, e coube aos governantes menos poderosos escolher entre a acomodação e o esforço extenuante de preparação para a guerra.

Para todos os governantes, a guerra e a preparação para a guerra dependiam da extração de recursos essenciais (dinheiro, soldados, provisões, armas etc.) que suas populações não estavam dispostas a entregar sem compensações ou, no mínimo, o fariam a um elevado custo político. Assim, além dos limites estabelecidos pela dinâmica conflitiva entre as diversas

unidades políticas mais ou menos similares, a forma de organização política interna de cada Estado foi condicionada pela organização das principais classes sociais e, principalmente, pelos conflitos entre os grupos sociais e de alguns daqueles grupos sociais (especialmente proprietários e trabalhadores) com as elites políticas governantes. Na medida em que os custos da guerra aumentaram e os conflitos sociais intensificaram-se com a industrialização, os construtores de Estados (*State-builders*) foram compelidos a barganhar direitos políticos e favores econômicos por recursos, que variaram desde impostos até a prestação de serviço militar. Essa barganha foi em grande medida tornada irreversível por sua fixação legal e transformação em costume quase-legal, e esteve na gênese do que hoje se chama cidadania.

No entanto, o tipo de Estado que predominou em cada período e região dependeu da combinação entre diferentes taxas de acumulação e concentração de meios de coerção (controlados pelos governantes) e diferentes taxas de acumulação e concentração de capital (controlado por agentes privados). Em diferentes regiões da Europa os governantes utilizaram estratégias extractivas e de dominação que podem ser caracterizadas como de intensa aplicação de coerção (áreas de poucas cidades e predominância agrícola) ou como de intensa inversão de capital (áreas de muitas cidades e predominância comercial, com produção voltada para o mercado). As diferentes estratégias de intensa coerção e de “coerção capitalizada” poderiam ajudar a entender, ainda que remotamente, as diferenças doutrinárias e organizacionais entre os primeiros serviços de inteligência e segurança surgidos, por exemplo, na Rússia e na Inglaterra no século XVI.

A variação na escala da guerra e a formação, a partir do século XVII, de um sistema europeu de Estados soberanos foram dois fatores determinantes para a vantagem comparativa daqueles Estados que apresentaram trajetórias de “coerção capitalizada”. Segundo Charles Tilly (1996:45-88), esse tipo de trajetória ocorreu quando coalizões de burocratas, capitalistas e estadistas foram mais eficientes na gestão da guerra, beneficiaram-se de instituições jurídicas e administrativas mais fortemente racionalizadas, mantiveram-se mais estavelmente associados às classes sociais internas através da constitucionalização do exercício do poder e estiveram mais intensamente envolvidos na construção de infra-estrutura econômico-social, provimento de serviços e adjudicação de conflitos.

Ao cabo desse processo, já bem avançado o século XIX, os diversos tipos de Estados começaram a convergir para o que passou então a ser reconhecido como o modelo de Estado nacional soberano, caracterizado pela autoridade exclusiva e constitucionalmente delimitada sobre um território e uma população, bem como pelo monopólio do uso legítimo da força. Eventualmente, o resultado desse processo levou à prolongada hegemonia dos

Estados capitalistas com sistemas políticos democráticos no sistema internacional, primeiro com a Inglaterra e depois com os Estados Unidos.<sup>6</sup>

Este é um tipo de narrativa sobre o surgimento e a mudança institucional que combina uma dinâmica evolutiva (a guerra como mecanismo de seleção) com uma forte ênfase intencional (interação entre grupos sociais delimitados produzindo consequências mais ou menos desejáveis sobre normas e organizações adaptativas). Como lembra Robert Goodin (1996:24-37), é inegável que o acaso e os acidentes também jogam um papel no desenho institucional de políticas, mecanismos sociais e sistemas. Porém, mesmo nos casos em que esse papel é mais evidente é difícil isolar o puro acaso daquilo que são as consequências não-intencionais de ações perfeitamente racionais ou, por outro lado, daquilo que são resultados agregados de interações entre diversos atores, resultados esses que diferem das intenções iniciais de qualquer ator em particular. É extremamente difícil precisar a exata combinação entre acaso, evolução e intencionalidade no desenho inicial e na trajetória de qualquer organização ou procedimento, seja ele o Estado moderno ou os serviços de inteligência.<sup>7</sup>

Feita a ressalva, assumo provisoriamente que o surgimento dos serviços de inteligência modernos foi predominantemente um fenômeno causado por atos intencionais. Os reis e ministros dos Estados europeus modernos, em seu processo de competição com outros governantes e no esforço de implementar sua dominação sobre territórios e populações cada vez mais amplos, mobilizaram recursos e criaram organizações especializadas na obtenção de informações. A criação de 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 associados à obtenção de informações.

Do ponto de vista das explicações disponíveis sobre por que organizações e instituições surgem, a construção de serviços de inteligência pode ser interpretada em parte como um resultado direto do puro cálculo estratégico de governantes perseguindo fins previamente dados (vencer a guerra e ampliar sua dominação) e, em parte, como uma resultante mais ou menos imprevisível do esforço desses mesmos governantes para adequarem seus fins a um contexto situacional que precisava ser mais bem compreendido e no qual seu próprio papel enquanto sujeitos políticos interessados era pouco claro.<sup>8</sup> Num contexto internacional altamente competitivo, incerto e marcado por altos custos de obtenção de informações necessárias à compreensão das intenções e capacidades de outros atores relevantes, os governantes modernos lançaram mão de vários instrumentos que pudessem reduzir tais custos, desde casamentos e outras formas de alianças dinásticas até o uso de serviços secretos.

Dada a trajetória de afirmação do Estado moderno descrita por Charles Tilly, proposições adicionais sobre a natureza das novas organizações de inteligência deveriam considerar não apenas sua função primária (prover informações), mas também as funções secundárias associadas ao uso dessas informações para a dominação e a maximização de poder em diferentes períodos e contextos nacionais. Nesse sentido, os serviços de inteligência modernos teriam surgido com uma dupla face, informacional e coercitiva a um só tempo. Essa dupla natureza (informacional e coercitiva) caracteriza ainda hoje os sistemas nacionais de inteligência existentes. É preciso reconhecer, porém, que há pouca evidência histórica disponível para ilustrar essa suposição, especialmente em relação aos séculos XVI-XVIII. Mesmo do ponto de vista teórico, os dois autores contemporâneos mais importantes que mencionam algo a respeito tendem a enfatizar características e funções opostas.

Por um lado, Anthony Giddens (1987:178) discute como o controle governamental de informações relevantes sobre a população e os recursos de cada país foi crucial para a gênese e a consolidação da autoridade soberana do Estado nacional, tanto no plano interno como no plano internacional ou sistêmico:

*(...) modern societies have been ‘information societies’ since their inception. There is a fundamental sense, as I have argued, in which all states have been ‘information societies’, since the generation of state power presumes reflexively unmonitored systems reproduction, involving the regularized gathering, storage, and control of information applied to administrative ends. But in the nation-state, with its peculiarly high degree of administrative unity, this is brought to a much higher pitch than ever before. (...) Records, reports and routine data collection become part of the day-to-day operation of the state, although of course not limited to it.*

Por outro lado, Charles Tilly (1996:72) mencionou o papel dos serviços de inteligência enquanto um meio direto de coerção:

Governantes (...) enfrentaram alguns problemas comuns, mas o fizeram de modo diferente. Forçosamente, distribuíram os meios de coerção de forma desigual por todos os territórios que tentaram controlar. Na maioria das vezes, concentraram a força no centro e nas fronteiras, tentando manter a sua autoridade entre um e outro por meio de grupos coercivos secundários, leais aplicadores locais de coerção, patrulhas volantes, e pela disseminação de órgãos de inteligência.

Note-se que Tilly enfatiza a função coercitiva em detrimento do papel informacional dos órgãos de inteligência, enquanto Giddens fala da importância dos sistemas de informação indiferenciadamente, sem atentar para o que há de específico no caso dos serviços de inteligência.<sup>9</sup> Como o foco de ambos é o Estado moderno e não os serviços de inteligência, é compreensí-

vel que tenham destacado apenas a faceta do fenômeno que servia mais imediatamente a seus propósitos.

No caso do comentário de Tilly, entretanto, há dois riscos mais sérios. Em primeiro lugar, tratar os serviços de inteligência genericamente como organizações repressivas impede que se compreendam suas especificidades (o papel central do segredo e do conhecimento) em relação às principais organizações de força do Estado, tais como as Forças Armadas e as polícias. Em segundo lugar, há o risco de se tratar os serviços de inteligência contemporâneos como se fossem a mera continuidade das primeiras organizações modernas, que teriam surgido totalmente prontas e imutáveis como resultado da vontade de poder de despotas iluminados.<sup>10</sup>

Na verdade, 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. É justamente essa diversidade de funções e perfis organizacionais que torna equivocado caracterizar os serviços de inteligência exclusivamente como organizações de força do Estado. Como parte do núcleo coercitivo do Estado contemporâneo, os serviços de inteligência desempenham um papel predominantemente informacional, com algumas funções diretamente coercitivas sendo exercidas por unidades específicas no sistema.

Além da descontinuidade histórica e da diversidade de funções exercidas por diferentes componentes dos sistemas nacionais, um outro problema na caracterização dos modernos serviços de inteligência é que as macrofunções desempenhadas por eles são apenas uma parte da explicação sobre por que eles surgiram e qual é seu perfil organizacional atual. A outra parte da explicação é política, não funcional. Para Amy Zegart (1999:42), o desenho inicial e o desenvolvimento posterior de organizações na área de segurança nacional seriam fortemente condicionados por três fatores, em ordem decrescente de importância: as escolhas estruturais feitas no surgimento da agência; os interesses e preferências cambiantes dos atores relevantes; os eventos externos que, dependendo da intensidade e do *timing*, podem forçar a mudança organizacional.

A formação dos sistemas nacionais de inteligência acompanhou as linhas mais gerais da delimitação de identidades nacionais, da construção do Estado (*State-building*), da institucionalização democrática, da utilização de sistemas de informação e de usos de meios de força na era moderna. Mas, para ir além da contextualização proporcionada pelo livro de Charles Tilly, seria necessário conhecer não apenas os resultados contingentes de inúmeros conflitos político-burocráticos no momento do surgimento de cada organização, mas também como os atores relevantes modificaram seus interesses, preferências e cálculos de custo e benefício diante dos eventos decisivos.

vos que marcaram a trajetória de cada organização. Seria preciso, também, ser capaz de reconhecer os diferentes ritmos da formação de sistemas nacionais em cada país e, dentro de cada país, como o “crescimento institucional” variou para cada tipo de organização.<sup>11</sup>

Lamentavelmente, isso está muito além do que o estágio atual da pesquisa nessa área permite. É possível, no entanto, dar um passo além e especificar melhor as matrizes organizacionais dos atuais serviços de inteligência. Para isso, na próxima seção serão utilizados dados referentes a diferentes países e a diferentes momentos históricos para a composição de um primeiro esboço interpretativo.

## Origens: diplomacia, guerra e policiamento

O surgimento dos sistemas nacionais de inteligência está associado, segundo Michael Herman (1996:2-35), ao lento processo de especialização e diferenciação organizacional das funções informacionais e coercitivas que eram parte integral da diplomacia, do fazer a guerra, da manutenção da ordem interna e, mais tarde, também do policiamento na ordem moderna. Embora as primeiras organizações surgidas em cada uma dessas matrizes tenham desaparecido e as organizações atuais tenham uma escala de operações muito maior e mais complexa do que seus precedentes históricos, pode-se obter uma visão mais concreta da dupla natureza dos serviços de inteligência analisando-se cada uma dessas três matrizes organizacionais separadamente.<sup>12</sup>

### *Diplomacia e inteligência externa*

As relações diplomáticas permanentes que se tornaram comuns na Europa entre os séculos XVI e XVII, seguindo os passos da diplomacia renascentista, serviam tanto para a representação e a negociação dos interesses coletivos das unidades políticas quanto para a obtenção e a comunicação de informações.<sup>13</sup> Aliás, foi somente em meados do século XVII que as três grandes potências europeias da época (Inglaterra, França e Espanha) passaram a contar com arquivos diplomáticos organizados e utilizáveis para a recuperação de informações. As chancelarias também passaram a coletar novas informações, tanto ostensivamente como por meios encobertos.

No caso da Inglaterra, desde que Francis Walsingham tornou-se secretário de Estado de Elizabeth I, em 1573, uma das funções mais importantes da secretaria passou a ser o controle do que era chamado então de *the intelligence*. O termo não significava apenas a provisão de informações extraordinárias sobre potências inimigas (especialmente sobre a frota espanhola antes de 1587) ou conspiradores internos (como os jesuítas e outros, perseguidos com base no Treason Act de 1351), mas incluía também um suprimento regular de notícias internacionais e informações sobre o mundo.<sup>14</sup>

A maior parte dessas notícias era relativamente rotineira e não provinha de fontes secretas, embora isso deva ser relativizado porque a própria distinção moderna entre domínio público e secreto não era clara naquele período. Até o surgimento dos jornais privados e do advento da liberdade de imprensa, os governos tendiam a ver toda informação sobre a população, a administração e os recursos do país como propriedade real, portanto secreta em alguma extensão.<sup>15</sup> Assim, os governos consideravam aceitável que seus embaixadores residentes em outros países tentassem obter aquelas informações por todos os meios disponíveis, inclusive recrutando espiões e interceptando clandestinamente as mensagens de terceiros. Isso não foi alterado substancialmente sequer pelas novas práticas introduzidas depois da Paz de Westfália (1648). Na Inglaterra, as redes de agentes controladas quase pessoalmente pelo secretário de Estado continuaram a existir muito depois da morte de *sir* Walsingham em 1590, tanto sob Cromwell como depois da restauração e da Revolução Gloriosa (1688), indicando que as novas atividades eram tomadas como necessárias à afirmação da autoridade do Estado nacional emergente, e não meramente um capricho dos diferentes regimes políticos.

O próprio aumento do tráfego diplomático, juntamente com o surgimento de serviços de correio na Europa moderna, demandou um uso regular de cifras e códigos secretos de escrita (criptografia) para proteger as comunicações entre as chancelarias e suas embaixadas. Com isso, surgiram as primeiras organizações especializadas na interceptação clandestina e na decodificação (criptologia) de mensagens, as chamadas “câmaras negras” (*black chambers*).<sup>16</sup> Não obstante a notável continuidade histórica do *cabinet noir* francês, instituído por Henrique IV em 1590 e famoso sob a direção do cardeal Richelieu no século seguinte, o exemplo inglês é mais típico, inclusive, pela descontinuidade entre as primeiras organizações e os serviços de inteligência atuais.

Em 1782, com a separação das funções do secretário de Estado em dois escritórios distintos, o Foreign Office para os assuntos exteriores e o Home Office para os assuntos internos da Inglaterra, essa divisão das funções antes atribuídas ao secretário de Estado refletiu-se na divisão da atividade de inteligência ao longo das mesmas linhas, interna e externa. Além disso, a própria coleta de informações sobre o exterior foi dividida em duas atividades separadas, a espionagem e a criptologia, sendo que o escritório secreto de criptologia foi transferido para o serviço postal inglês, onde os despachos diplomáticos e a correspondência considerada sensível continuaram regularmente sendo interceptados, copiados, reenviados e, quando necessário e possível, decodificados até 1844. No final do século XVIII o Parlamento britânico passou a votar uma verba secreta anual para financiar as operações de inteligência do Foreign Office e do Secret Office and Deciphering Branch

(criptologia), dinheiro empregado também para comprar apoios políticos e militares no continente.<sup>17</sup> Aquele Secret Service Fund foi administrado pelo War Office até o começo do século XX, quando se formaram as atuais agências britânicas de inteligência.

Desdobramentos organizacionais desse tipo continuaram a ocorrer mais tarde e, de modo geral, as funções secretas de negociação, conspiração, inteligência e espionagem exercidas desde a época elisabetana pela diplomacia britânica, assim como pela francesa, austríaca, piemontesa, prussiana ou russa, estão na origem dos serviços especializados formados entre a segunda metade do século XIX e os anos iniciais da Guerra Fria.

Há, no entanto, diferenças cruciais na escala das atividades e na dimensão das organizações. Enquanto a agência central de criptologia do governo britânico nos dias de hoje, os Government Communications Headquarters (GCHQs), empregava 6.076 funcionários e tinha um orçamento de centenas de milhões de libras esterlinas em 1995, o Secret Office and Decyphering Branch possuía no seu auge, durante o século XVIII, um total de nove empregados, e só passou a ter um modesto orçamento regular a partir de 1782. Além da escala comparativamente diminuta das operações de coleta, a análise e a validação das informações obtidas eram feitas de forma completamente *ad hoc*. Não havia *staffs* separados e especializados de analistas, pois a própria atividade de inteligência não se separava da formulação e da implementação de políticas e linhas de ação. Para acompanhar a formulação sintética de Michael Herman (1996:13), pode-se dizer que para os reis e seus ministros a atividade de inteligência era parte integrante das funções regulares do estadista, sendo inseparável do exercício do poder.

A separação progressiva entre as funções de inteligência e de formulação e implementação de políticas (*policymaking*) foi tão lenta quanto a separação entre as atividades diplomáticas legítimas e as operações secretas de influência e espionagem. Em 1939, por exemplo, o embaixador francês em Berlim ainda dispunha de fundos secretos destinados à compra de informações.<sup>18</sup> Em tese, porém, hoje em dia são dois ramos separados e especializados da ação estatal no plano internacional. Dado que a maioria dos alvos dos serviços de inteligência é externa, deriva daí uma acentuada disputa burocrática pelo controle dos fluxos de informação do exterior para os governantes. É bem conhecida a rivalidade existente entre a CIA e o State Department nos Estados Unidos, o que também ocorre entre o Secret Intelligence Service (SIS) e o Foreign and Commonwealth Office (FCO) na Grã-Bretanha.<sup>19</sup>

Atualmente, muitos países mantêm organizações de inteligência subordinadas aos seus ministérios de relações exteriores para apoiar especificamente o acompanhamento de crises, negociações de acordos, tratados internacionais etc. Esse é o caso do Bureau of Intelligence and Research (INR)

do Departamento de Estado norte-americano, que faz parte do sistema de órgãos de inteligência do governo dos Estados Unidos, embora não realize operações próprias de coleta de informações (a não ser aquelas ostensivamente disponíveis ao público nos países com representação diplomática dos Estados Unidos). O INR recebe informações coletadas por outras agências e as analisa para o secretário de Estado. Na Inglaterra, o departamento de análise e pesquisa do FCO cumpre funções semelhantes, embora não seja membro formal do sistema nacional de inteligência daquele país.

Além de ter gerado suas próprias organizações específicas de inteligência, a diplomacia moderna também esteve na origem remota de muitas das chamadas agências nacionais de coleta de inteligência externa (*foreign intelligence*). Nacional, nesse contexto, indica apenas que se trata de organizações que respondem diretamente ao primeiro-ministro, ao presidente ou ao secretário-geral e que prestam serviço para o governo como um todo, e não somente para um ministério específico.

São exemplos desse tipo de organização a CIA norte-americana e o SIS britânico, citados anteriormente, bem como a Direction Générale de la Sécurité Extérieure (DGSE) francesa, o Ha-Mossad le Modiin ule-Tafkidim Meyuhadim (Mossad) israelense, o atual Sluzhba Vneshney Rasvedki (SVR) russo, o Servizio per le Informazioni Generali e Sicurezza (Sisde) italiano ou ainda o Bundesnachrichtendienst (BND) alemão. Muitos outros serviços poderiam ser citados, mas bastam alguns exemplos de organizações mais conhecidas e ainda atuantes hoje em dia.<sup>20</sup>

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. Eles diferem bastante de um país para outro em termos organizacionais, na escala de operações e pela composição predominantemente civil ou militar de seus oficiais de inteligência. Mas isso não impede que cada um desses serviços veja a si próprio como *primus inter pares* dentro do sistema de inteligência de seus respectivos países. Por outro lado, a despeito de suas raízes na diplomacia secreta presente na trajetória de qualquer Estado antigo ou moderno, há uma grande descontinuidade histórico-organizacional entre as primeiras redes modernas de agentes à maneira da Inglaterra elisabetana e os atuais serviços de inteligência exterior, que surgiram e se desenvolveram somente no século XX.

Nesse sentido, embora a primeira imagem quando se fala de serviços de inteligência remeta às organizações responsáveis por humint, tais como o SIS e o Mossad, na maioria dos países esse componente dos sistemas nacionais de inteligência não é o maior, o mais antigo ou o que produz maior volume de informações de valor crítico. Por exemplo, as organizações mili-

tares de inteligência surgiram já na segunda metade do século XIX, tendo se tornado muito maiores e mais numerosas do que os serviços de inteligência exterior. Essa segunda matriz de origem dos atuais serviços de inteligência será considerada a seguir.

### *Guerra e inteligência de defesa*

No caso da guerra, o registro da presença de atividades de inteligência é muito mais antigo. Relatos sobre o uso de espiões militares remontam ao velho testamento da Bíblia,<sup>21</sup> assim como figuram prescritivamente no manual de Sun Tzu sobre a arte da guerra,<sup>22</sup> o *Ping-fa*, escrito na China no começo do século IV aC. Na verdade, o reconhecimento do campo de batalha e do inimigo sempre foi considerado um elemento essencial da capacidade de comando do general. Entretanto, desde a época dos *speculatores* utilizados pelas legiões romanas de César até os corpos de guias usados pelos franceses e britânicos durante as guerras napoleônicas, a inteligência militar foi exercitada num contexto institucional que Martin van Creveld (1985:17-57) chamou de a “idade da pedra do comando”.<sup>23</sup>

Foi somente com as mudanças radicais introduzidas na área militar durante o período da Revolução Francesa e de Napoleão que começou a mudar o significado da inteligência para o comando.<sup>24</sup> O quartel-general móvel de Napoleão, pelo menos desde 1805, consistia em três elementos principais e independentes entre si, a *maison* privada do próprio imperador, o *État Majeur de l'Armée* e o quartel-general administrativo. Paradoxalmente, o órgão mais importante para o comando da Grande Armée era a *maison*, à qual estava subordinado um *bureau* de estatística encarregado da inteligência estratégica sobre os inimigos, bem como um *bureau* topográfico, encarregado de recolher as informações das várias fontes e prepará-las, inclusive cartograficamente, para que Napoleão as estudasse diariamente. As fontes de informação eram diversas, desde mapas, jornais e livros, passando por informantes e espiões plantados em cada cidade importante, até correspondências interceptadas e decodificadas pelo *cabinet noir* (criado em 1590). A inteligência operacional durante as campanhas era obtida também pelas patrulhas de cavalaria das unidades e passada para o *bureau* topográfico através do Estado-maior, que incluía em sua organização uma seção para interrogar prisioneiros, camponeses e desertores. O próprio imperador tinha uma rede pessoal de fontes de inteligência, seus *officiers d'ordonnance* e generais ajudantes que ele enviaava em missões especiais. Entretanto, embora organizados numa escala maciça como nunca antes havia existido, os métodos e as tecnologias de inteligência disponíveis para Napoleão permaneciam em grande medida os mesmos da Antigüidade.

Além de imperador e comandante militar, Napoleão era seu próprio oficial de inteligência. Como destaca van Creveld (1985:68), essa capacidade de Napoleão para analisar e processar informações pessoalmente, eliminando muitos passos e camadas organizacionais intermediárias, ajuda a explicar a velocidade e a decisão da forma napoleônica de fazer a guerra e comandar a *Grande Armée*. Por outro lado, alerta Creveld, isso também poderia induzir a tomadas de decisão repentinas, baseadas em desejos mais do que em análise, em segundos pensamentos ou mesmo na falta de pensamento adequado.

Apesar desses problemas, a mudança na utilização da inteligência foi parte integrante da revolução nas estruturas de comando iniciada pelas guerras napoleônicas e que duraria praticamente até o final da I Guerra Mundial. Ao longo do século XIX, a mobilização de exércitos com milhões de soldados e a construção de grandes marinhas, as novas tecnologias de armamentos e de propulsão, o uso de ferrovias e telégrafos (mais tarde rádios), enfim, a nova escala e a complexidade da gestão do fenômeno bélico modificaram profundamente as estruturas de comando, controle, comunicações e inteligência (C<sup>3</sup>I) das Forças Armadas.<sup>25</sup>

O modelo mais influente de estruturação do comando foi o do Estado-maior geral prussiano, que começou a afirmar-se desde 1815 e alcançou grande prestígio internacional após as vitórias da Prússia sobre a Áustria (1866) e a França (1870). Como lembra Martin van Creveld (1985:57): “*It was not until the middle of the nineteenth century that the traditional coup d’oeil with its implications of immediate personal observation gave way to the German-derived ‘estimate of the situation’, implying map study and written reports*”.

A inteligência militar no século XX reteve algo dessa nova exigência de científicidade e abrangência destacada por van Creveld. Em comparação com a linha evolutiva derivada da diplomacia secreta dos séculos XVI a XVIII, pode-se dizer que a inteligência militar acrescenta à conspiração e à espionagem uma nova dimensão, a da 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.<sup>26</sup>

No começo do século XX, a maioria dos países europeus havia adotado alguma versão de Estado-maior geral que incluía esferas de responsabilidade formalmente separadas em seções (operações, planejamento, inteligência, logística, comunicações etc.). Cabe notar, entretanto, a observação de Creveld de que, mesmo no caso prussiano, na prática ainda não havia uma especialização completa de funções divididas entre as seções de operações, doutrina

e inteligência. Isso teria implicado, pelo menos até a I Guerra Mundial, significativa superposição das atribuições dessas seções no Estado-maior geral alemão. De modo geral, a experiência da I Guerra Mundial forçou uma maior especialização, principalmente quando às funções de inteligência exercidas pelos *bureaus* militares de estatística e de topografia desde a primeira metade do século XIX somaram-se as novas seções de “exércitos estrangeiros” (*foreign armies*), responsáveis pelo estudo das Forças Armadas dos inimigos potenciais ou efetivos.

O relativo atraso da Inglaterra e dos Estados Unidos na adoção do modelo de estados-maiores gerais refletia diferenças constitucionais e políticas, mas também o tamanho bem menor de suas Forças Armadas até meados do século XIX. Isso se refletiu na demora na criação de *staffs* e unidades militares de inteligência. No caso inglês, por exemplo, somente depois da Guerra da Criméia (1853/56) foram enviados adidos militares permanentes para outros países para observar as Forças Armadas. Ao mesmo tempo, foi criado um Topographical and Statistical Department subordinado diretamente ao War Office. Em 1873, aquele departamento foi renomeado como Intelligence Branch, seguido da criação de um departamento separado de inteligência para o subcontinente indiano em 1878. Por sua vez, o almirantado (*Admiralty*) criou um comitê de inteligência em 1882, no mesmo ano em que a Marinha dos Estados Unidos criava a mais antiga organização de inteligência ainda em atividade naquele país, o Office of Naval Intelligence (ONI). No caso britânico, em 1887 foram nomeados pela primeira vez diretores de inteligência no War Office e no Admiralty. A criação de um Estado-maior geral após a guerra dos Bôeres (1899-1902) amalgamou o cargo de diretor de inteligência militar (DMI) com o de diretor de operações militares (DMO), num movimento pendular que reflete a instabilidade da nova função de inteligência destacada por Creveld, um indicador de que a institucionalização dos serviços de inteligência ainda estava distante. A posição autônoma do diretor de inteligência no War Office britânico só voltou a ser restaurada como função independente em 1915.<sup>27</sup> Mesmo então a separação não era completa, e a inteligência de sinais (sigint) derivada de interceptação e decodificação de mensagens permaneceu insulada das outras fontes de informações até bem depois da batalha da Jutlândia.<sup>28</sup> As disputas pelo controle dos fluxos informacionais e a precária especialização/coordenação das equipes de analistas foram um problema para a inteligência militar até pelo menos a II Guerra Mundial, como atesta o exemplo norte-americano em Pearl Harbor.<sup>29</sup>

Mesmo levando em conta essa separação lenta entre inteligência e as funções de planejamento e operações, as organizações permanentes e especializadas de inteligência militar tornaram-se parte estável das estrutu-

ras de comando, controle e comunicações das Forças Armadas bem antes que surgissem as organizações nacionais de inteligência externa.

Depois da II Guerra Mundial, além do *staff* da seção de inteligência do Estado-maior geral, em cada força singular foram sendo criadas unidades especializadas ou *staffs* de inteligência para os níveis inferiores de comando da força. Além disso, muitos países que possuem ministérios da Defesa e uma maior integração das Forças Armadas criaram também agências de inteligência de defesa (*defense intelligence*) para apoiar os Estados-maiores integrados (*joint*) e os ministros.<sup>30</sup> São exemplos atuais dessa nova “camada” organizacional o Glavnoye Razvedyvatelonoye Upravlenie (GRU) russo, a Defense Intelligence Agency (DIA) norte-americana, o Servizio per le Informazioni e la Sicurezza Militare (Sismi) italiano, o Agaf Modiin (Aman) israelense e o Defence Intelligence Staff (DIS) britânico.

Com exceção do GRU, instituído entre 1918 e 1924, as demais organizações mencionadas datam do segundo pós-guerra. Cada uma dessas organizações centrais de inteligência de defesa apresenta uma escala e abrangência de capacidades operacionais nas áreas de coleta e análise de informações no exterior que é comparável à dos serviços nacionais de inteligência exterior de seus países. Em função disso, é conhecida a rivalidade entre a DIA e a CIA, no caso dos Estados Unidos, ou entre o Aman e o Mossad, no caso de Israel, para citar apenas dois exemplos. Quando se somam a essas organizações centrais de inteligência de defesa os recursos e agências de inteligência das marinhas, exércitos, forças aéreas e outras forças singulares e comandos integrados (*joint commands*), fica evidente que o componente militar dos sistemas nacionais de inteligência é de longe o maior e mais complexo do ponto de vista organizacional, correspondendo a algo entre 50 e 80% de todos os recursos de inteligência de qualquer país.<sup>31</sup>

Uma descrição satisfatória das relações entre esses órgãos centrais de inteligência militar e as demais organizações, centros e unidades de cada força singular em vários países exigiria um livro inteiro.<sup>32</sup> Sobre o significado da formação de subsistemas de inteligência militar para a configuração final dos sistemas nacionais e a agilidade no ciclo das atividades de inteligência, serão feitas algumas considerações adicionais na próxima seção, “Lógica de expansão dos sistemas de inteligência”. Antes, porém, é preciso destacar ainda uma outra matriz organizacional dos serviços de inteligência contemporâneos.

### *Policiamento e inteligência de segurança*

A terceira matriz histórica dos serviços de inteligência contemporâneos se distingue das duas anteriores por sua ênfase nas chamadas ameaças internas à ordem existente. Trata-se da inteligência de segurança (*security*

*intelligence*), conhecida também como inteligência interna ou doméstica. As origens das atuais organizações de inteligência de segurança remontam ao policiamento político desenvolvido na Europa na primeira metade do século XIX, decorrente da percepção de ameaça representada por movimentos inspirados na Revolução Francesa e pelo nascente movimento operário anarquista e socialista.

As forças especializadas em manutenção da ordem interna desenvolveram técnicas e recursos de vigilância, infiltração, recrutamento de informantes e interceptação de mensagens para a repressão política dos grupos considerados subversivos. Embora o temor da revolução popular tenha diminuído um pouco depois de 1848, o processo mais geral de profissionalização das polícias e a emergência de unidades de investigação criminal continuaram ampliando as capacidades de detecção, captura, interrogação, periciamento técnico, vigilância e armazenamento de informações sobre novas áreas criminais e segmentos populacionais.<sup>33</sup> A “cientificização” do combate ao crime a partir do século XIX estendeu-se ao policiamento político e à repressão contra a “subversão”.

Conforme Jeffrey Richelson (1986:1-4), a primeira organização permanente voltada para a obtenção de inteligência sobre os “inimigos internos” visando a sua repressão foi a terceira seção do departamento de segurança do Estado, instituída na Rússia imperial em 1826. Os dois precedentes mais importantes da terceira seção foram a Oprichnina (1565/72), a cavalaria negra instituída pelo primeiro czar de todas as Rússias, Ivan, o Terrível, bem como a organização Preobazhensky (1697-1729), criada por Pedro I para investigar, prender, interrogar sob tortura e aplicar penas contra traidores e outros suspeitos de crimes contra o czar e o Estado. Embora a repressão mais ou menos sistemática dos dissidentes e críticos seja um traço característico de todos os Estados, o policiamento político organizado foi uma especialidade russa na era moderna. Na segunda metade do século XIX, a dinastia Romanov contratou o prussiano Wilhelm Stieber para reorganizar a polícia política. Depois do atentado à bomba que matou o czar Alexandre II em 1881, a Okhrannoye Otdyelyenye (conhecida como Okhrana) consolidou-se como uma força policial “especializada”, independente tanto dos ministérios do Interior e do Exterior quanto dos incipientes recursos de inteligência das Forças Armadas. Considerada mais cruel do que eficiente, inclusive por seus adversários bolcheviques, de qualquer modo a polícia secreta do czar tornou-se o símbolo de toda uma era. A experiência russa da Okhrana também nos ajuda a entender a persistente associação entre inteligência e repressão política ao longo do século XX.

Embora organizações como a Okhrana russa ou a Sûreté Générale francesa (instaurada ainda sob Napoleão Bonaparte<sup>34</sup>) inicialmente não condu-

zissem operações de espionagem e obtenção de inteligência contra alvos estrangeiros, a busca de informações e a perseguição de adversários do regime no exílio rapidamente estenderam o policiamento político ao exterior. Em 1870, a Sûreté tinha mais de 60 agentes operando em estações em Viena, Amsterdã, Hamburgo e outras cidades europeias. A primeira base permanente da Okhrana no exterior data de 1882, menos de um ano após sua reorganização.<sup>35</sup> Além de caçar revolucionários russos exilados, a Okhrana também passou a tentar monitorar as atividades de órgãos de segurança e inteligência estrangeiros, tais como a própria Sûreté, atuando em território russo.

Como resultado dessa dinâmica, no começo do século XX já havia considerável superposição de missões e alvos entre as polícias políticas e as organizações de inteligência voltadas para o exterior, que naquela época ainda eram principalmente militares. As polícias políticas controlavam redes próprias de agentes recrutados nas embaixadas estrangeiras situadas nas capitais de seus países, interceptavam comunicações dos grupos dissidentes e das embaixadas estrangeiras, além de tentarem estabelecer redes de agentes e informantes em outros países.<sup>36</sup>

Principalmente depois da I Guerra Mundial e da Revolução Russa, as polícias políticas e serviços secretos de cada país passaram a vigiar regularmente as atividades dos serviços de inteligência estrangeiros dentro do território nacional. Com isso, além da inteligência de segurança (*security intelligence*) propriamente dita, essas organizações especializaram-se também em contra-espionagem e contra-inteligência (*counterintelligence*). Com o processo de descolonização durante a Guerra Fria e com o terrorismo nos anos 1970, certas operações de suporte à contra-insurgência, contramedidas defensivas e antiterrorismo foram acrescentadas ao leque de missões desse tipo de organização. Nas últimas duas décadas, o crime organizado, o tráfico de drogas e os crimes eletrônicos (incluindo fraude financeira e lavagem de dinheiro) adquiriram tal importância na agenda de segurança de alguns países que a busca por informações extrapolou os limites da rotina da investigação criminal.<sup>37</sup>

Essa expansão das missões ocorreu de forma mais ou menos concomitante com a transformação dos antigos serviços secretos e polícias políticas em serviços de inteligência de segurança (*security intelligence*), principalmente nos países democráticos. Não há, entretanto, nada parecido com um modelo organizacional internacionalizado nessa área.

Em alguns países, as organizações de *security intelligence* são separadas organizationalmente das polícias e da inteligência externa. Atualmente, organizações como o Canadian Security Intelligence Service (CSIS), a Direction de la Surveillance du Territoire (DST) francesa, o Bundesamt für Verfassungsschutz (BfV) alemão e o Sherut ha'Bitachon ha'Klali (Shin Bet) israelense exemplificam essa separação.<sup>38</sup> Já em outros países, a inteligência

interna ou de segurança é um departamento especializado das próprias forças policiais. Esse é o caso dos Estados Unidos, com a divisão de segurança nacional (inteligência) do Federal Bureau of Investigation (FBI).<sup>39</sup>

Na prática, porém, pode-se dizer que em todos os países as missões de inteligência de segurança, contra-inteligência e inteligência policial dificilmente estão subordinadas a uma única agência. No Japão, por exemplo, essas atividades são compartilhadas de forma tensa pela Agência de Investigação e Segurança Pública (Koan Chosa Cho) e pela unidade de combate à subversão da Agência Nacional de Polícia (Keisatsu Cho).<sup>40</sup> Em alguns outros países, ainda, a inteligência interna ou de segurança chegou mesmo a desdobrar-se diretamente das Forças Armadas.<sup>41</sup>

Esse é precisamente o caso da Inglaterra. Como se sabe, a criação da polícia metropolitana de Londres em 1829 foi o primeiro passo na lenta consolidação de uma estrutura de forças policiais locais ao longo do século XIX na Inglaterra, onde as polícias tiveram pouca influência direta na formação do serviço de inteligência de segurança.<sup>42</sup> Segundo Michael D. Lyman (1999:63-98), embora fossem recrutados alguns informantes e a correspondência pessoal de suspeitos de subversão fosse interceptada, algum policiamento especializado contra ameaças internas só teria começado em 1883, com a criação de uma seção especial na polícia metropolitana de Londres para colher informações e reprimir os fenianos irlandeses.

Em 1909, com a criação do Secret Service Bureau subordinado ao War Office, a inteligência de segurança e a contra-espionagem passaram crescentemente para a esfera da seção doméstica do *bureau* militar (conhecida como MI-5, ou quinta seção da inteligência militar). Em 1931, a seção de inteligência exterior (MI-6) e a seção de inteligência doméstica (MI-5) do War Office foram separadas definitivamente em duas agências independentes, respectivamente o Secret Intelligence Service (SIS) e o Security Service (que permaneceu sendo conhecido como MI-5).<sup>43</sup> Após diversas batalhas burocráticas com a polícia metropolitana, as funções de inteligência de segurança foram completamente transferidas para o Security Service depois da II Guerra Mundial. Uma exceção importante foi a jurisdição sobre o combate ao Irish Republican Army (IRA), que permaneceu separada por vários ramos do governo britânico. Somente em 1992 o Secret Service (MI-5) passou a centralizar as operações de inteligência e repressão contra o IRA, mas mesmo assim só no restante do território britânico, pois no território da Irlanda do Norte o papel do MI-5 continua secundário em relação ao do *special branch* do Royal Ulster Constabulary (RUC).<sup>44</sup>

Refletindo o processo de expansão das missões dos serviços de inteligência interna (*security intelligence*) já mencionado, em 1999 as áreas de trabalho do Security Service britânico dividiam-se oficialmente em terroris-

mo relacionado com a Irlanda do Norte (30,5%); terrorismo internacional (22,5%); contra-espionagem (20,5%); segurança (11,5%); crimes graves (7%); proliferação de armas (3,5%); assistência a outras agências (4,5%).<sup>45</sup> Em comparação com anos anteriores, em que três quartos dos recursos do MI-5 eram dedicados ao contraterrorismo e ao IRA, a atual distribuição de prioridades enfatiza a contra-inteligência e o combate ao crime organizado. Isso resulta em parte da diminuição relativa da escala de conflitos na Irlanda do Norte e também da percepção britânica de que o país continua sendo alvo de operações de espionagem internacional.

O caso inglês apresenta, pois, diferenças de desenho organizacional e de *timing* em relação aos casos francês e russo, em que os serviços de inteligência de segurança surgiram das polícias secretas atuantes já na primeira metade do século XIX, mas também é diferente do caso norte-americano, em que a própria polícia federal (FBI) é a principal agência de inteligência de segurança, ou ainda em relação ao caso canadense, no qual um serviço de inteligência de segurança (CSIS) foi criado apenas em 1984 como uma resposta às investigações parlamentares sobre violações de direitos humanos cometidas pela divisão de segurança da Royal Canadian Mounted Police (RMPC).<sup>46</sup>

Talvez mais importante do que a especificidade do caso inglês seja o que ele tem em comum com os demais países em qualquer uma das três matrizes: a dificuldade de se estabelecer fronteiras organizacionais bem definidas nas diferentes áreas e missões de inteligência. Na próxima seção se poderá ver como isso está relacionado com a própria lógica de expansão recente dos serviços de inteligência e seus reflexos na configuração de diferentes tipos de sistemas nacionais.

## Lógica de expansão dos sistemas de inteligência

Três tipos diferentes de organizações especializadas foram destacados na seção anterior: inteligência externa (*foreign intelligence*), inteligência militar (*military intelligence*) e inteligência interna (*security intelligence*). Além desses componentes organizacionais principais, presentes na maioria dos Estados, a formação de sistemas nacionais de inteligência está associada a dois movimentos adicionais de expansão organizacional e especialização funcional que vêm ocorrendo nas últimas décadas: I. Um movimento de expansão vertical envolvendo a formação de subsistemas de inteligência policial e de inteligência militar. 2. Um movimento de expansão horizontal, com o surgimento de novas agências especializadas em diferentes disciplinas de coleta e análise ao longo do *continuum* operacional que caracteriza o ciclo da inteligência.

A expansão das missões dos serviços de inteligência interna (*security intelligence*), inicialmente restrita ao policiamento político de dissidentes e

mais tarde abarcando a contra-inteligência, o contraterrorismo e inteligência sobre o crime organizado, acabou por aproximar esses serviços das unidades investigativas das polícias encarregadas de dinâmicas criminais mais complexas, tais como o narcotráfico, fraudes financeiras, lavagem de dinheiro e outros crimes eletrônicos (*cybercrimes*). Em muitas polícias também existem agora unidades especializadas de inteligência sobre crime, utilizando informações coletadas de fontes diversas (inclusive imint e sigint) e métodos analíticos mais sofisticados (principalmente nas áreas de georreferenciamento de dinâmicas criminosas e de visualização de inter-relacionamentos de criminosos). Essa expansão vertical do uso de métodos e técnicas de inteligência para a base dos sistemas policiais, em combinação com uma maior integração e busca de sinergia entre as unidades de inteligência policial e as agências nacionais de inteligência de segurança, pode ser apontada como uma tendência na direção da formação de subsistemas de inteligência de segurança.<sup>47</sup>

Na Inglaterra, essa tendência de maior integração se traduz na formação de times mistos de agentes do Security Service com quadros das seções especiais (*special branches*) da polícia metropolitana de Londres e de outras 51 forças policiais regionais, além do *special branch* do RUC, responsável por inteligência e operações encobertas na Irlanda do Norte. O terrorismo, o crime organizado e a ameaça de espionagem são áreas que atravessam a tradicional dicotomia interno/externo. No caso britânico, isso implica o envolvimento eventual dos serviços de coleta de inteligência exterior (SIS e GCHQ), além do próprio FCO e do Tesouro, nesses comitês interagências.

Nos Estados Unidos também existem agora unidades de inteligência especializadas nos departamentos de polícia, destacando-se aí a divisão de inteligência do New York Police Department (NYPD/DI). Organizações constabulares (policiais) como a Guarda Costeira (US Coast Guard) também possuem unidades de inteligência que interagem, de um lado, com os serviços de inteligência da Marinha e dos Fuzileiros Navais, no âmbito do National Maritime Intelligence Center (NMIC), e, por outro lado, com o FBI e outras agências de “imposição da lei” (*law enforcement*), tais como a Drug Enforcement Administration (DEA) e o Immigration & Naturalization Service (INS). Dada a miríade de organizações policiais, constabulares e de *law enforcement* nos Estados Unidos, além dos mecanismos de divisão de poderes entre autoridades distintas, tanto no âmbito federal como nos 50 estados, no distrito federal, cidades e centenas de condados, o grau de integração vertical de um subsistema de inteligência de segurança, contra-inteligência e inteligência policial naquele país provavelmente é baixo. Mas a tendência de maior integração sem dúvida existe, e seu sinal mais visível está na criação de centros especializados com pessoal fornecido por várias agências e foco de ação nas áreas de delimitação jurisdicional mais difícil. Exemplos desse tipo

de estrutura são o National Drug Intelligence Center (NDIC), o National Counterintelligence Center (Nacic), o El Paso Intelligence Center (Epic), situado no Novo México e dedicado ao problema da imigração ilegal, e a Financial Crimes Enforcement Network (Finncen).<sup>48</sup>

Um fenômeno semelhante de verticalização de capacidades nacionais ocorre na área de inteligência militar. Como foi mencionado na seção anterior, nos países em que foram criados comandos integrados (*joint commands*) e estruturas mais desenvolvidas de suporte nos ministérios de Defesa isso tendeu a ser acompanhado da criação de agências centrais de inteligência de defesa. Em alguns casos, a criação dessas agências não significou que o Exército, a Marinha e a Aeronáutica deixassem de manter suas próprias organizações centralizadas responsáveis pela produção de inteligência para o Estado-maior e o comandante de cada força. Além das organizações centrais de inteligência em cada força, compõem ainda o subsistema de inteligência militar as unidades militares especializadas, por vezes em nível de batalhão ou até mesmo brigadas, no caso da força terrestre, ou de esquadrões e alas, no caso da força aérea, que atendem às necessidades de inteligência dos níveis inferiores de comando.

No caso dos Estados Unidos, o que ocorreu depois da Guerra do Golfo (1990/91) foi um aumento relativo na integração do subsistema de inteligência militar, através de medidas de consolidação organizacional, da clarificação de linhas de comando e de novas doutrinas de emprego com ênfase no suporte à capacidade de combate das forças e na *performance* dos comandos integrados (*joint commands*). Em termos de consolidação organizacional, pode-se mencionar o caso da Marinha daquele país, que possuía em 1991 sete organizações distintas de inteligência e em 1993 já havia transferido os recursos e atribuições para apenas duas que restaram, o próprio Office of Naval Intelligence (ONI) e o Naval Security Group Command (NSGC), responsável por inteligência de sinais (sigint) e segurança de comunicações (comsec).<sup>49</sup> Esse tipo de consolidação organizacional, embora com menor intensidade, ocorreu também nas outras forças singulares. A maior clarificação de linhas de comando é mais visível no caso do Exército. Por um lado, o novo National Ground Intelligence Center (NGIC) consolidou em 1995 os recursos e as atribuições de três organizações anteriormente separadas, empregando civis e pessoal uniformizado de unidades numeradas responsáveis por diretórios específicos do centro (por exemplo, o 902nd MI Group para a contra-inteligência e o 203rd MI Battallion para a análise de material bélico estrangeiro). Todas as unidades especializadas de inteligência e segurança do Exército subordinam-se agora ao comandante-em-chefe do Intelligence and Security Command (Inscom). Por seu turno, o próprio comandante do Inscom reporta-se ao *army deputy chief of*

*staff for intelligence* em todos os assuntos de inteligência. Apenas na área de inteligência de sinais e de segurança de comunicações há uma duplidade nas linhas de comando, pois o comandante do Inscom reporta-se também diretamente ao diretor da National Security Agency (NSA).

Aliás, foi na área de sigint que os Estados Unidos parecem ter obtido o maior grau de integração vertical dos recursos militares de inteligência. Na condição de principal autoridade nacional na gestão da disciplina de inteligência de sinais, o diretor da NSA exerce simultaneamente a função de chefe do Central Security Service (CSE), o que significa basicamente que ele tem autoridade orçamentária sobre os gastos das forças singulares com recursos de criptologia/criptografia e mantém controle operacional (*opcon*) sobre os comandos e unidades de segurança de comunicações e interceptação de sinais do Exército (Inscom), da Marinha (NSGC), da Força Aérea (AIA) e dos Fuzileiros Navais (ACSC<sup>41</sup>). Por outro lado, esse tipo de integração, baseada na definição de “gerentes nacionais” responsáveis por certas disciplinas em inteligência, também podetia ser um exemplo do segundo movimento de expansão organizacional teferido antes.<sup>50</sup>

Afinal, além das três matrizes históricas e da formação de subsistemas de inteligência policial e militar, os sistemas nacionais de inteligência atualmente existentes resultam também de uma expansão “horizontal”, decorrente de especializações funcionais crescentes e, no limite, da separação organizacional ao longo do *continuum* coleta-análise de informações.

A especialização principal se deu nas técnicas e tecnologias adequadas às diversas fontes de informação. Novos métodos de coleta e processamento, novas plataformas e sistemas modificaram as estruturas de custos e a composição da força de trabalho envolvida na atividade de inteligência. No que hoje se chama de coleta de informações de fontes especializadas (*single source collection*), por exemplo, existem atualmente órgãos ou unidades especializadas em obter informações a partir de fontes humanas (humint), a partir da interceptação e decodificação de comunicações e sinais eletromagnéticos (sigint), a partir da produção e processamento de imagens fotográficas ou multiespectrais (imint), da mensuração de assinaturas e outras características técnicas (masint), bem como da coleta de fontes ostensivas, como jornais, televisão, internet e livros (osint). No subsistema de inteligência de segurança mencionado anteriormente há organizações especializadas em contra-inteligência, em medidas defensivas de segurança, em inteligência interna (*security intelligence*) e inteligência policial. Finalmente, uma vez traçada a linha burocrática, orçamentária e legal que estabelece quais órgãos governamentais fazem parte oficialmente dos sistemas nacionais de inteligência, é preciso levar em conta também as agências situadas na periferia dos subsistemas de inteligência e segurança militar e policial, ou mesmo os recursos temporariamente alocados sob controle operacional das agê-

cias, por exemplo, adidos militares, laboratórios de análise, contatos diplomáticos, aviões e navios em missões de coleta de informações etc.

Devido ao grande volume de informações coletadas por plataformas tecnológicas e organizações diversas, a produção de inteligência “finalizada” sobre um alvo ou tema passou a ser um problema crescente e levou à criação, em alguns países, de organizações dedicadas apenas à análise e à avaliação (*all-sources analysis and assessments*) das informações coletadas de fontes diversas por organizações especializadas em cada tipo de fonte ou “disciplina” da área de coleta.

O duplo movimento de expansão vertical e horizontal dos serviços de inteligência gerou demandas gerenciais e de coordenação impensáveis mesmo durante a II Guerra Mundial e boa parte do período da Guerra Fria. Obviamente, o grau de complexidade organizacional de cada sistema nacional de inteligência varia muito, indo desde sistemas com dezenas de agências, como os Estados Unidos e a Rússia, até países como Canadá e Itália, que têm apenas duas organizações principais de inteligência e segurança. Entretanto, a própria idéia de que os recursos e capacidades de inteligência de um país formem “sistemas organizacionais” implica a suposição de que são gerenciados de forma mais ou menos integrada. Uma camada organizacional bastante recente no processo de “crescimento institucional” dos sistemas de inteligência são as instâncias de coordenação, gestão de recursos e supervisão das políticas nacionais para o setor. A justificativa principal para incluir essas instâncias de coordenação num tipo ideal de organização dos sistemas nacionais de inteligência não é simplesmente o fato de elas existirem em Londres ou Washington, mas sim a percepção de que têm a exercer um papel crescente também em outros países.<sup>51</sup>

Até aqui, tratou-se de descrever a lógica de expansão da atividade moderna de inteligência desde suas matrizes na diplomacia, no fazer a guerra e no policiamento até a formação de sistemas nacionais de inteligência mais ou menos complexos. No restante desta seção serão apresentadas duas direções possíveis para uma futura explicação mais completa das causas dessa expansão.

A primeira abordagem relaciona o desenvolvimento das organizações de inteligência com o fortalecimento mais geral das capacidades institucionais do Estado, sustentando basicamente que uma “oferta” maior de serviços de inteligência depende bastante da maior ou menor disponibilidade de recursos em cada país. A segunda abordagem relaciona o surgimento e o desenvolvimento das organizações de inteligência com os atributos específicos das organizações de segurança nacional em regimes democráticos, que seriam bastante diferentes das demais burocracias governamentais voltadas para assuntos internos dos países.

Embora bem mais sofisticada do que a afirmação grosseira do parágrafo anterior, a tese de David Bayley (1975:349-351) sobre a formação dos

sistemas nacionais de polícia exemplifica bem esse tipo de abordagem. Por sistemas nacionais de polícia o autor entende diferentes arranjos institucionais para o provimento de ordem pública, a garantia da observância às leis e a proteção da vida e do patrimônio da população. Assumindo como premissa que cada caso nacional é único, Bayley analisou através de estudo histórico-comparativo quais seriam as variáveis mais importantes na explicação dos atributos de cada sistema policial e também por que as características atuais (em 1975) mais importantes dos sistemas nacionais de polícia emergiram em determinados períodos históricos relativamente bem determinados na Inglaterra (1829/89), França (1667-1700), Alemanha (1742-1871) e Itália (1815/70).<sup>52</sup>

As sete variáveis independentes analisadas por Bayley foram o papel do crescimento populacional e sua distribuição ao longo do *continuum* rural-urbano, a extensão da criminalidade e da insegurança entre a população, a Revolução Industrial e/ou outras transformações sociais ou econômicas desse porte, a ocorrência de revoluções e/ou outras transformações políticas desse porte, a presença de ameaças externas ou a ocorrência de guerras e mobilizações militares e, finalmente, o impacto de uma ideologia qualquer (absolutismo, liberalismo, nacionalismo, socialismo etc.).

Segundo esse autor, as características bastante diferentes dos sistemas policiais na Inglaterra, França, Alemanha e Itália não foram determinadas pelo crescimento populacional, grau de urbanização, taxas agregadas de criminalidade, ritmos de industrialização ou por alguma ideologia específica. As variáveis mais importantes teriam sido institucionais e políticas, desde a erosão das bases comunitárias da autoridade até as preferências dos atores mais poderosos em relação às demandas por lei e ordem, passando pela maior ou menor resistência popular à penetração do governo e pela transformação interna na organização do Estado. De todas essas, a associação mais clara é aquela existente entre a expansão da capacidade do Estado e a emergência de sistemas nacionais de polícia. As transformações do Estado a que se refere Bayley estão relacionadas com a diminuição dos custos de extração de recursos da sociedade e com o aumento geral dos níveis de produção administrativa (*outputs*) e consolidação da autoridade política, o que teria permitido um aumento no nível de “oferta” de serviços policiais e o amadurecimento, entre 1660 e 1890, de sistemas nacionais de polícia na Europa.<sup>53</sup>

A ênfase excessiva nos recursos disponíveis e na evolução funcional dos sistemas policiais deixa muitas variáveis relevantes de lado (as preferências dos atores e as diferenças de desempenho institucional, por exemplo), mas a partir desse tipo de ênfase pode-se dizer, no mínimo, que a formação recente de complexos (e caros) sistemas nacionais de inteligência também correspondeu a um período de expansão geral das capacidades estatais nas últimas décadas.

Um indicador grosseiro dessa expansão é o crescimento do gasto público como parcela do PIB, seja do gasto público total ou, o que no caso é mais significativo, do gasto dos governos centrais. Segundo o World development report publicado pelo Banco Mundial em 1997, no período entre 1960 e 1995 o gasto governamental total nos países da OCDE subiu em média de um patamar inferior a 20% para quase 50% do PIB. Em 1994, somente o gasto dos governos centrais representava em média mais de 35% do PIB nos países da OCDE. No caso dos Estados Unidos, até a década de 1930 o gasto federal manteve-se num patamar de cerca de 4% do PIB, enquanto em 1995 ele já representava 22,1% do PIB. Em 1997, para um PIB de US\$8,11 trilhões, foram realizados naquele país gastos federais de US\$1,60 trilhão em valores correntes. Mais de 55% desses gastos foram feitos com serviços sociais (previdência, saúde, educação, habitação, serviços comunitários e bem-estar social), enquanto os gastos militares representaram cerca de 17% dos gastos federais totais (ou US\$258,3 bilhões). No século XX a curva de gastos sociais ultrapassou a curva de gastos militares nos Estados Unidos apenas ao final da década de 1960, e o crescimento médio dos gastos militares entre 1960 e 2000, já ajustada a inflação, manteve-se positivo apesar do declínio relativo após o final da Guerra Fria.<sup>54</sup>

Por sua vez, a curva de gastos com inteligência acompanhou a evolução dos orçamentos militares depois da II Guerra Mundial. Não há relação direta conhecida entre o PIB de um país e seus gastos com inteligência, mas parece haver alguma razão entre gastos com defesa e gastos com inteligência, embora essa proporção também varie significativamente. Como não há dados confiáveis sobre orçamentos de inteligência em nenhum país do mundo, antes de mais nada porque esses gastos são secretos e, mesmo nos casos em que o volume total de gastos é conhecido, as proporções alocadas para cada tipo de atividade e de organização são apenas estimadas por observadores externos aos governos.

No caso dos Estados Unidos e da União Soviética/Rússia, os gastos com inteligência chegaram a cerca de 10% dos gastos totais com defesa na década de 1980, recuando um pouco ao longo dos anos 1990. Michael Herman (1996:37) estima que os gastos com inteligência nos países da Europa ocidental oscilem entre 3 e 5% do total de gastos militares. Simplesmente não existem tais estimativas sobre os gastos consolidados com inteligência nos países mais industrializados do Terceiro Mundo ou da Europa oriental. Com todas essas restrições, assume-se aqui, em caráter provisório, um gasto nacional médio com atividades de inteligência em torno de 5% dos gastos nacionais com defesa. A diferença dos Estados Unidos e da Rússia em relação a todos os demais países deve-se à sua condição de superpotências durante a Guerra Fria e ao custo de desenvolvimento e manutenção de suas frotas de satélites-espiões.

Como regra geral, pode-se concordar com Michael Herman (1996:38-40) quando ele diz que a maior parte dos investimentos e do custeio na área de inteligência vai para as agências de coleta, enquanto a análise e a disseminação tendem a ser itens de despesa relativamente menores. Nos anos 1990, a diminuição dos orçamentos de inteligência foi significativamente menor do que a diminuição dos orçamentos de defesa, tanto nos países da Europa como nos antigos membros do Pacto de Varsóvia. Tampouco há indicações de que os gastos com inteligência tenham diminuído em qualquer país importante da Ásia, América Latina ou da vasta região que vai do norre da África até a Ásia central.

A segunda abordagem relevante para explicar a formação dos sistemas nacionais de inteligência é uma versão modificada do novo institucionalismo, desenvolvida por Amy Zegart (1999) ao analisar o surgimento e a evolução de três agências de segurança nacional dos Estados Unidos: o National Security Council (NSC), o Joint Chiefs of Staff (JCS) e a Central Intelligence Agency (CIA).<sup>55</sup> Segundo Zegart, o mesmo conjunto de premissas neo-institucionalistas sobre a importância das regras do jogo, sobre racionalidade e dilemas de ação coletiva, sobre custos de transação e sobre a natureza dos atores conduz a conclusões diferentes quando se trata de analisar agências de segurança nacional em contextos democráticos.<sup>56</sup>

Para diferenciar as agências governamentais internas (de regulação e/ou prestação de serviços) das agências de segurança nacional, a autora considera quatro variáveis fundamentais: densidade do ambiente formado pelos grupos de interesse na área de atuação de cada agência; disponibilidade de informações sobre as atividades de cada agência; autoridade do Legislativo ou do Executivo para o estabelecimento de diretrizes; grau de interdependência burocrática e clareza jurisdicional. Com base em evidências empíricas e num exercício taxonômico competente, Zegart estabelece uma dicotomia baseada em dois tipos opostos de agências governamentais.<sup>57</sup>

Em um extremo estariam as agências governamentais que atuam em áreas de políticas públicas reguladoras e distributivas. O meio ambiente social dessas áreas de políticas públicas é caracterizado por um grande número de grupos de interesse, poderosos e consolidados. Esses grupos encarregam-se de fornecer incentivos e sanções aos parlamentares para que eles se envolvam nas disputas sobre a estrutura e a atuação das agências de um dado setor. A disponibilidade de informações sobre as atividades da agência é alta, e os obstáculos para a obtenção dessas informações são de tipo administrativo. Para a terceira variável, Zegart destaca então o papel central do Congresso nas decisões sobre a criação, o desenho organizacional e o volume de serviços (*outputs*) das agências governamentais domésticas. A quarta variável é a mais problemática. Segundo a autora, agências governamentais voltadas para o público nacional

apresentam uma clara delimitação de funções (saúde, educação, transportes etc.) e têm grande independência operacional umas das outras.

No outro extremo estariam as agências de segurança nacional, caracterizadas em primeiro lugar pela fraca presença de grupos de interesse em seu ambiente de atuação. Mesmo nas áreas em que existem tais grupos (*lobby* de fabricantes privados de armamentos ou grupos de imigrantes, por exemplo), eles são relativamente menos numerosos, menos poderosos e orientados para resultados políticos específicos (ex.: obter um dado contrato para desenvolver um novo sistema de armas), e não para influenciar o desenho organizacional de uma agência ou o nível geral de gastos orçamentários de um setor.<sup>58</sup> Como muitas das atividades das agências de segurança nacional são conduzidas em segredo, existem barreiras legais e procedimentais para o acesso público às informações relevantes. Com custos de obtenção de informações mais altos e um ambiente rarefeito de grupos de interesse, há poucos incentivos positivos para os parlamentares participarem ativamente das disputas sobre a organização ou as ênfases operacionais das agências de segurança nacional. Finalmente, em relação ao grau de interdependência burocrática, ele seria bem maior na área de segurança nacional por causa da justaposição de temas e funções que impedem uma clara delimitação jurisdicional entre as diferentes agências do setor.

A partir dessa delimitação de características específicas das agências de segurança nacional, Amy Zegart faz três proposições que poderiam ser testadas através de pesquisas adicionais:<sup>59</sup> 1. Ao contrário do que ocorre com as demais agências governamentais, cuja criação é fortemente influenciada pelos grupos de interesse e pelo Congresso, no caso das agências de segurança nacional a decisão de criar uma nova agência, assim como as escolhas de seu desenho organizacional e suas regras de funcionamento, é fortemente concentrada no Poder Executivo. 2. Devido ao elevado grau de interdependência burocrática e por causa da precária delimitação de jurisdições, as agências de segurança nacional que já existem em um dado momento lutam entre si e com as equipes de assessores presidenciais para influenciar a definição presidencial sobre as missões, recursos e o desenho organizacional do novo órgão. O desenho final das novas agências que estão sendo criadas depende dos resultados desses embates. 3. Além de envolver-se pouco nas disputas em torno da criação de novas agências de segurança nacional, os parlamentares e o Congresso também procuram evitar o envolvimento em atividades de supervisão sobre as atividades dessas agências, pois lhes faltam os instrumentos e os incentivos para isso.

Deixando de lado por enquanto as implicações dessa terceira proposição para a discussão sobre os mecanismos de controle externo de agências de segurança nacional e sobre os impactos da instituição do segredo governamental no desenvolvimento dos serviços de inteligência (temas que serão discutidos no

capítulo 3, Segurança nacional, segredo e controle público), note-se que até aqui Zegart fala de agências de segurança nacional sem levar em conta as diferenças entre as próprias organizações desse tipo. Ao estudar os diferentes padrões de evolução das três agências na segunda metade do século XX (NSC para *policymaking*, JCS para comando das Forças Armadas e CIA para inteligência externa), Zegart conclui que três fatores, em ordem decrescente de importância, determinariam o desenho inicial e o desenvolvimento posterior de organizações na área de segurança nacional: 1. As escolhas sobre desenho organizacional e regras de funcionamento feitas na época da criação da agência. 2. Os interesses, opiniões e linhas de ação dos atores relevantes, que mudam ao longo do tempo através das próprias interações. 3. Os eventos externos que, dependendo da intensidade e do *timing*, podem forçar a mudança organizacional sem que os atores tenham controle sobre as variáveis ambientais.<sup>60</sup>

Quando contrastado com a abordagem histórico-estrutural de Bayley, o modelo institucional das “agências de segurança nacional” de Zegart adiciona à explicação sobre a expansão dos sistemas de inteligência as escolhas dos atores relevantes (grupos de interesse, legisladores, burocracias e governantes) e as condições de incerteza em que essas escolhas são feitas, que forçam cada ator a adaptar suas preferências aos constrangimentos impostos pelos demais atores e pelo ambiente. No caso dos serviços de inteligência e de segurança, seria preciso incorporar ao modelo as próprias dinâmicas operacionais que caracterizam a atividade, tais como discutidas no capítulo anterior. Como se trata de componente informacional de um conflito em que um ator tenta dobrar a vontade de outro, o surgimento e o padrão evolutivo de sistemas de inteligência também refletem essas interações adversariais com as organizações similares de outros governos ou mesmo de atores não-estatais.

Em síntese, os serviços de inteligência e de segurança foram criados e se desenvolveram porque os governantes pretendiam resolver certos problemas informacionais associados ao provimento de defesa nacional e ordem pública, mas em cada país e em cada área de especialização funcional a disponibilidade de recursos variou, a competição interburocrática por jurisdição foi mais ou menos aguda e a capacidade de um serviço de inteligência impor parâmetros às dinâmicas conflitivas entre organizações similares subordinadas a diferentes governos foi decisiva para a configuração final de cada sistema nacional.

Para um exemplo das possíveis configurações organizacionais dos sistemas nacionais de inteligência, na próxima seção serão mencionadas muito brevemente as principais agências norte-americanas e britânicas de inteligência.

## Organização dos sistemas nacionais de inteligência

Nas últimas três ou quatro décadas do século XX formaram-se sistemas governamentais de inteligência nos países mais importantes do mundo. Do-

tado de maior ou menor complexidade estrutural quando considerado de forma concreta, o desenho organizacional ideal-típico de tais sistemas envolve os seguintes componentes: alguma instância central de coordenação, uma ou mais agências principais de coleta de informações (normalmente imagens e sinais estão separados de humint e fontes ostensivas), alguma instância central de análise, unidades departamentais de análise com laços mais ou menos definidos com as organizações centrais de coleta de inteligência, poderosos subsistemas de inteligência de defesa e de segurança, algum órgão de formação e treinamento e, mais recentemente, órgãos mais ou menos colegiados para coordenação e instâncias de supervisão externa, seja no próprio Poder Executivo, no Legislativo ou, mais raramente, no Judiciário.

Utilizando algumas variáveis muito genéricas, tais como o grau de centralização da autoridade sobre as unidades do sistema, o grau de integração analítica da inteligência disseminada para os usuários, a maior ou menor separação entre as funções de inteligência e de *policymaking*, além da efetividade dos mecanismos de *accountability* no Poder Executivo e no Legislativo, seria o caso de se fazer comparações internacionais mais amplas para se tentar obter uma posição relativa dos casos analisados entre si e em relação ao desenho organizacional ideal-típico. Infelizmente, esse é um desafio que está além dos limites deste livro.<sup>61</sup>

Apenas como indicação polêmica para tratamento posterior, me parece que há pelo menos três tipos básicos de sistemas nacionais de inteligência:

- um modelo “anglo-saxão”, caracterizado por alta centralização da autoridade sobre as unidades do sistema, alto grau de integração analítica, média separação entre inteligência e política, além de média efetividade dos mecanismos de *accountability* e supervisão – nesse modelo poderiam ser incluídos os sistemas nacionais de inteligência e segurança de países como Estados Unidos, Grã-Bretanha, Canadá, Austrália, Nova Zelândia e, com muitos cuidados, Índia e África do Sul;
- um modelo “europeu continental”, caracterizado por média centralização da autoridade sobre as unidades do sistema, média integração analítica dos produtos de intel, alto envolvimento da atividade de inteligência com as instâncias de *policymaking* e, finalmente, uma baixa efetividade dos mecanismos de *accountability* e supervisão (*oversight*) – nesse modelo poderiam ser incluídos os sistemas nacionais de inteligência e segurança de países como França, Alemanha, Rússia, Polônia, Itália e, com muitos cuidados, Brasil e Argentina;
- 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* e, de forma ainda mais pronunciada do que no tipo “europeu continental”, uma baixa efetividade dos mecanismos de *accountability* e supervisão – nesse modelo poderiam ser incluídos os sistemas nacionais de inteligência e segurança de países como China, Japão, Coréia do Sul, Taiwan, Coréia do Norte e, com muitos cuidados, Indonésia e Vietnã.

Obviamente, há uma grande dose de arbitrariedade e impropriedade nessa caracterização grosseira. Repito aqui as ressalvas que fiz em nota à Introdução do trabalho: a forma mais corriqueira de classificação encontrada na literatura ainda consiste na dicotomia entre um modelo descentralizado com supervisão congressual (Estados Unidos) e um modelo centralizado sem controles públicos (União Soviética). Dada a evidente função ideológica dessa dicotomia, a classificação aqui proposta me parece claramente superior. Uma taxonomia mais refinada foi utilizada por Michael Herman (1996:4), na qual o autor inglês elabora um tipo ideal a partir da abstração de traços organizacionais e operacionais observados na experiência anglo-saxã, para em seguida analisar como as regularidades se aplicam aos diversos sistemas nacionais a partir de círculos concêntricos: mais intensamente no núcleo anglo-saxão, medianamente no caso da Europa ocidental e Israel e de forma bastante fraca no caso dos países comunistas e ex-comunistas. Embora o trabalho de Herman tenha o mérito de ser a melhor obra disponível sobre problemas teóricos da área de inteligência, seu teste dos “círculos concêntricos” não chega a ser realizado. Certo, tampouco há aqui qualquer teste efetivo da classificação triádica (anglo-saxão, europeu continental e asiático), mas a prefiro, pois a formulação de Herman parece ser um refinamento que não rompe no essencial com a dicotomia liberal da Guerra Fria.

Particularmente problemática na classificação aqui proposta é sua dificuldade em livrar-se da referência geográfica, que tende a ser bastante enganadora: o Paquistão e a Índia ficam na Ásia, mas seus aparatos de inteligência são bastante diferentes entre si. Além disso, o Paquistão é o principal aliado dos Estados Unidos na Ásia central e no subcontinente indiano, mas é a Índia que adota mais claramente o modelo anglo-saxão em seu sistema de inteligência. O caso de Israel, caracterizado por baixa centralização da autoridade sobre as unidades do sistema, baixa integração analítica dos produtos de inteligências várias agências, baixo envolvimento da atividade de inteligência com as instâncias de *policymaking*, alta responsividade das unidades do sistema aos governantes e média efetividade dos mecanismos de *accountability* e controle externo, é inclassificável nos três modelos disponíveis. Da mesma forma, uma virtual categoria de “outros” ficaria ainda com dezenas de países do Magreb/Machrek, países latino-americanos, africanos, asiáticos e da Europa oriental. Enfim, há uma enorme tarefa de pesquisa pela frente nessa área para quem puder realizar estudos comparativos adicionais.

Mesmo com essas evidentes dificuldades, adoto provisoriamente a classificação triádica a partir da constatação preliminar de que a estrutura organizacional e os procedimentos operacionais dos serviços de inteligência japoneses e chineses se parecem mais entre si do que o sistema japonês se parece com o anglo-americano ou que o sistema chinês se parece com o soviético-russo. De todo modo, assim como no caso das capacidades militares, em termos de recursos de inteligência há que se observar a enorme disparidade entre os casos norte-americano e russo e todos os demais sistemas nacionais de inteligência.<sup>62</sup>

O papel da escala de operações e dos volumes de recursos disponíveis, destacado na abordagem de Bayley sobre os sistemas policiais, pode ser mais bem visualizado através do contraste entre dois sistemas nacionais de inteligência pertencentes a um mesmo “modelo anglo-saxão”: Estados Unidos e Grã-Bretanha. As descrições sumárias desses dois casos encerram esta seção. Não ignoro as diferenças constitucionais e os diferentes contextos institucionais que influenciaram tão decisivamente a configuração dos sistemas de inteligência na monarquia parlamentarista inglesa e na república federativa e presidencialista norte-americana. Mas o foco aqui será apenas a apresentação direta de cada caso, destacando sempre que possível o volume de gastos e o número de funcionários empregados, pois constituem um indicador razoável da capacidade dos governos em uma determinada área. Mesmo isso, no entanto, esbarra no segredo que cerca a área de inteligência, pois não é possível uma qualificação mais precisa do perfil dos gastos dentro de cada programa ou agência, assim como da composição interna da força de trabalho empregada. Mesmo com tantas restrições, espera-se que a apresentação sumária dos dois casos ajude o leitor a ter uma idéia mais concreta do que são sistemas nacionais de inteligência e da variedade de configurações possíveis.<sup>63</sup>

### *Estados Unidos*

Nos Estados Unidos, a US Intelligence Community (IC) abrange 14 organizações principais, além das instâncias de coordenação ligadas ao diretor central de inteligência (DCI).<sup>64</sup>

O DCI ocupa legalmente o vértice do “sistema” e desempenha três papéis principais: coordena a IC, subordina a CIA e assessoria o presidente e o Conselho de Segurança Nacional na área de inteligência. O DCI possui dois adjuntos, um para a direção da CIA e, desde 1996, outro para o gerenciamento da comunidade. Estão ligadas também ao DCI quatro instâncias colegiadas superiores da IC: o National Intelligence Council (NIC), o National Foreign Intelligence Board (NFIB), o Intelligence Community's Executive Committee (IC/Excom) e o Community Management Staff (CMS). Pode-se dizer que

o NIC e o NFIB dão suporte ao DCI no seu papel de principal assessor governamental de inteligência, enquanto o CMS e o Excom apóiam o DCI na sua função gerencial de coordenador do sistema.

O principal componente da IC é formado por quatro agências nacionais de coleta de informações externas (*foreign intelligence*). Através do seu diretório de operações, a Central Intelligence Agency (CIA) é o principal serviço de espião-nagem, operações encobertas e humint. Na área de sigint e segurança de informações encontra-se a maior agência de inteligência do governo norte-americano, a National Security Agency (NSA). Por sua vez, a área de imint passou a ser coordenada por uma nova agência criada em 1996, a National Imagery and Mapping Agency (Nima). A quarta e mais cara agência nacional é o National Reconnaissance Office (NRO), responsável pelo desenvolvimento e pela aquisição de satélites de sigint, imint e outras plataformas e sistemas especializados para uso das Forças Armadas e das agências nacionais de coleta. A instância nacional para o trabalho de análise e produção de inteligência para o governo norte-americano é o diretório de inteligência (análise) da CIA. Relatórios anuais sobre temas e áreas vitais (*estimates*) são produzidos colegiadamente no National Intelligence Council (NIC) dirigido pelo DCI. No âmbito “ministerial”, o trabalho de análise é feito por escritórios de inteligência nos departamentos de Defesa, Estado, Tesouro, Justiça, Energia, Comércio e Transportes. Esses escritórios participam das instâncias colegiadas da IC e respondem administrativamente aos titulares dos órgãos aos quais eles servem.

O caso do Departamento de Defesa necessita um comentário adicional. Além de subordinar três das quatro agências nacionais de inteligência (Nima, NSA e NRO), o Pentágono conta ainda com a Defense Intelligence Agency (DIA) e seu diretório de operações, o Defense Humint Service (DHS), com o Defense Airborne Reconnaissance Office (Daro), com a Defense Threat Reduction Agency (DTRA), a Defense Information Systems Agency (Disa) e o Defense Security Service (DSS). Todas são consideradas agências de suporte ao combate, mas enquanto a DIA e o Daro têm missões primárias na área de inteligência, a DTRA, a Disa e o DSS têm suas missões primárias na área de segurança. Além dessas organizações centrais do Departamento de Defesa, o subsistema militar de inteligência é formado ainda pelo Army Intelligence and Security Command (Inscom) do Exército, pelo Office of Naval Intelligence (ONI) e pelo Naval Security Group Command (NSGC) da Marinha, pela Air Intelligence Agency (AIA) da Aeronáutica e pela Marine Corps Intelligence Activity (MCIA) dos Fuzileiros Navais. Capacidades orgânicas são também articuladas em torno dos Joint Intelligence Centers (JIC's) dos nove comandos centrais unificados (Atlântico, Central, Europeu, Pacífico, Sul, Espaço, Operações Especiais, Estratégico, Transportes), além de instituições de treinamento e formação acadêmica (em ní-

vel de graduação e mestrado) em inteligência, tais como o Joint Military Intelligence College (JMIC), a National Defense University (NDU) e a Naval Post-Graduate School (NPS).

A principal agência norte-americana nas áreas de contra-inteligência e de inteligência de segurança é o Federal Bureau of Investigation (FBI), através de sua divisão de segurança nacional. As Forças Armadas, a Guarda Costeira e o secretário de Defesa possuem suas próprias organizações de segurança e contra-inteligência. No âmbito do Departamento de Justiça e dos departamentos de polícia estaduais e locais já foi mencionada antes a formação de um subsistema de inteligência policial. Finalmente, a supervisão e o controle externos sobre a IC são exercidos pela presidência do país, através do Presidential Foreign Intelligence Advisory Board (Pfiab), pelos comitês de inteligência do Senado (Senate Select Committee on Intelligence – SSCI) e da Câmara (House Permanent Select Committee on Intelligence – HPSCI) e, muito indiretamente, pela mídia e pelo público.

Em termos orçamentários e de recursos humanos, os gastos com inteligência dos Estados Unidos representaram 1,6% do orçamento federal no ano fiscal de 1999. Mas essa percentagem representa valores absolutos realmente muito grandes para qualquer parâmetro internacional. O agregado orçamentário das atividades de inteligência norte-americanas foi oficialmente reconhecido no final de 1997, quando o Congresso aprovou US\$26,7 bilhões para o ano fiscal de 1998.

Na estimativa da Federation of American Scientists (FAS), a IC custou aos contribuintes norte-americanos cerca de US\$29,4 bilhões em 1996, distribuídos em três programas principais: o National Foreign Intelligence Program (NFIP), o Joint Military Intelligence Program (JMIP) e o Tactical Intelligence and Related Activities (Tiara). Com exceção de US\$3,2 bilhões para a CIA e de US\$700 milhões para a inteligência das demais agências civis (FBI, Justiça, Estado, Energia, Tesouro, Comércio etc.), ambas as cifras fazendo parte do NFIP, o restante todo seria de fundos executados e controlados pelo Departamento de Defesa. Ou seja, o Pentágono controla cerca de 75% das verbas do NFIP, 100% do JMIP e 100% do Tiara.<sup>65</sup>

Assumindo uma margem de erro de 5% na estimativa de 1996, a FAS estimava os orçamentos e o pessoal de algumas agências mais importantes naquele ano de referência da seguinte forma: escritório do DCI (278 funcionários e custo de US\$100 milhões); CIA (16 mil funcionários e US\$3,1 bilhões); DIA (8.500 funcionários e US\$850 milhões); NRO (1.700 funcionários e US\$6,2 bilhões de orçamento); NSA (21 mil funcionários e US\$3,6 bilhões); Inscom (13 mil efetivos e custo de US\$1 bilhão); ONI (16 mil efetivos e US\$1,2 bilhão); AIA (15 mil efetivos e US\$1,5 bilhão); Nima (9 mil funcionários e US\$1,2 bilhão), DSS (3 mil funcionários e US\$350 milhões); FBI (2.500 quadros na National Security

Division, com US\$ 500 milhões de orçamento); INR (300 funcionários e custo de US\$ 20 milhões) e DEA (mil agentes e US\$ 250 milhões).

Em resumo, nos Estados Unidos o Pentágono controla mais de 85% de todos os recursos humanos, organizacionais e financeiros da área de inteligência. O orçamento de inteligência nos Estados Unidos é maior do que o orçamento consolidado de defesa de um país como a França. Por isso, em futuras comparações internacionais é preciso considerar a escala operacional e o grau de complexidade organizacional dos sistemas nacionais como variáveis decisivas.

### *Grã-Bretanha*

Na Grã-Bretanha, a UK Central Intelligence Machinery (CIM) é formada por três serviços de inteligência principais, além das instâncias de coordenação no gabinete ministerial e de outros órgãos departamentais.<sup>66</sup>

Também ligada ao secretário do gabinete existe a figura de um coordenador de inteligência, que preside o Joint Intelligence Committee (JIC). É no âmbito do JIC que se dá o planejamento interdepartamental das operações de inteligência, a ligação com as agências de inteligência do exterior e, principalmente, a integração analítica e a produção final de relatórios de inteligência para as instâncias governamentais usuárias. O JIC possui um pequeno núcleo de análise central (*assessments staff*) e grupos interdepartamentais de análise organizados que funcionam como equivalentes britânicos do NIC para o trabalho analítico. Não há no caso britânico uma organização similar ao diretório de análise da CIA. Isoladamente, os principais corpos analíticos para assuntos de segurança nacional do governo britânico são o Defense Intelligence Staff (DIS) do Ministério da Defesa e o Research and Analysis Department do Ministério das Relações Exteriores e Comunidade Britânica (FCO).

A inteligência de imagens é coletada por unidades militares, e a produção e a análise são feitas pelo Joint Air Reconnaissance Intelligence Center (Jaric). O Jaric é subordinado ao DIS e ao Estado-maior conjunto das Forças Armadas, mas é a principal organização especializada em imint no governo britânico. A inteligência de sinais é coletada e processada pelo Government Communications Headquarters (GCHQ), a organização nacional de sigint subordinada ao secretário do FCO. A organização nacional de humint é o Secret Intelligence Service (SIS), que também passou a ser subordinado ao FCO desde 1994.

O Security Service (MI-5) é a principal organização de inteligência de segurança e de contra-inteligência, subordinada administrativamente ao Ministério do Interior (*Home Office*). O RUC e os *special branches* das polí-

cias também atuam nessa área, mas não fazem parte formal do CIM. Na área de criptografia e segurança de comunicações e computação a principal agência britânica é o próprio GCHQ, através do seu Communications Electronics Security Group.

No caso britânico, a supervisão e a coordenação do CIM são feitas pelo primeiro-ministro, através do Ministerial Committee on Intelligence Services (CIS), pelo secretário do Gabinete, através do Permanent Secretaries' Committee on the Intelligence Services (PSIS), e, desde 1994, pelo Intelligence and Security Committee, formado por parlamentares da Câmara dos Comuns e da Câmara dos Lordes. Além de se tratar de um comitê conjunto, a outra diferença do comitê parlamentar britânico em relação aos comitês noruegueses é que seus membros são indicados pelo primeiro-ministro, após consultar o líder da oposição.

Na Grã-Bretanha, o orçamento oficial de inteligência aprovado para o ano fiscal de 1999 foi de £706 milhões.<sup>67</sup> Diferentemente do agregado orçamentário norte-americano, esse total refere-se apenas ao orçamento das três agências principais de inteligência (SIS, GCHQ e MI-5). Em 1994, o mesmo orçamento foi de £974,5 milhões. A acentuada redução nos últimos anos reflete um redimensionamento das operações e do pessoal, mas principalmente a conclusão de algumas obras e prédios que estavam em construção, especialmente o novo quartel-general do SIS. Por outro lado, há muitos gastos que nos Estados Unidos são apropriados como parte do orçamento de inteligência e que não o são na Grã-Bretanha. O serviço de monitoramento da mídia internacional da BBC, por exemplo, custa cerca de £18 milhões ao ano. O equivalente desse serviço nos Estados Unidos é feito pelo Foreign Broadcast Information Service (FBIS), um serviço do Diretório de Ciência e Tecnologia (DS&T) da CIA.

Ainda que se leve isso em conta, os gastos britânicos com inteligência são muito menores que os norte-americanos, tanto em termos absolutos como percentualmente em relação aos gastos com defesa. As três agências principais do CIM têm juntas cerca de 10.500 funcionários, sendo 2 mil do SIS, 2 mil do MI-5 e cerca de 6.500 do GCHQ. Além dos funcionários diretamente contratados pelo GCHQ, a agência tem controle operacional sobre cerca de 3 mil militares de unidades envolvidas em operações de sigint. O número total de quadros das *special branches* das 52 forças policiais e constabulares britânicas chegava a 2.300 efetivos em 1994, mas não há dados consolidados sobre seu custo anual. Para o mesmo ano de referência, estima-se que os gastos britânicos com inteligência militar tenham sido de £190 milhões. Esse valor inclui o DIS e o Jaric, mas provavelmente não inclui os programas táticos semelhantes ao Tiara norte-americano. Somados os gastos militares e civis oficialmente reconhecidos, o orçamento britânico de inteligência estaria em torno de £1 bilhão, situando-se um pouco

acima da média internacional em termos de gastos com inteligência e muito abaixo dos gastos norte-americanos.

A despeito de diferenças de escala, os Estados Unidos e a Grã-Bretanha são exemplos da tendência mais geral de formação de sistemas de inteligência bastante complexos do ponto de vista organizacional e bastante diferenciados do ponto de vista funcional. Na seção final deste capítulo serão tecidas algumas considerações finais sobre os impactos dessa complexidade organizacional para o desafio institucional da agilidade.

## A agilidade como dilema

Em muitos países democráticos, os gastos públicos com os serviços de inteligência atualmente superam os gastos com representação diplomática. Por outro lado, os gastos com policiamento, defesa nacional ou ajuda internacional são bastante superiores aos gastos com inteligência. Isso indica que a inteligência continua sendo uma atividade “subsidiária”. Ainda assim, o peso institucional desses sistemas nos arranjos de política externa, defesa nacional e provimento de ordem pública não pode mais ser ignorado.<sup>68</sup>

Como foi discutido neste capítulo, as características organizacionais dos sistemas de inteligência resultam de processos específicos de construção de soluções para os desafios da área de segurança nacional. As políticas públicas nessas áreas relacionadas com a segurança nacional têm caráter menos distributivo do que em outras áreas de atuação de burocracias governamentais, e os *issues* principais dizem respeito, em tese, a bens públicos. Os grupos de interesse na sociedade são mais recentes e relativamente mais fracos do que em outras áreas (como negócios ou habitação, por exemplo). A informação sobre a atuação das agências governamentais de segurança nacional é menos disseminada em função das restrições de segurança e segredo. Além disso, essa é uma área onde historicamente predomina o Poder Executivo, com um envolvimento mais baixo e menos ativista do Poder Legislativo. Finalmente, as áreas de jurisdição e os temas de segurança nacional são inter-relacionados e as burocracias envolvidas (ex.: Forças Armadas, diplomacia, polícias e órgãos de inteligência) são mutuamente dependentes, muito mais do que as burocracias voltadas para temas domésticos, onde há menos justaposição de funções e atribuições. Todos esses fatores conjugam-se para baixar os incentivos que os parlamentares teriam para se envolver no desenho e na supervisão das agências de segurança nacional.

Dadas essas especificidades das agências de segurança nacional, Amy Zegart (1999) propõe duas teses úteis para o estudo dos processos de institucionalização de serviços de inteligência. Por sua própria natureza, as burocracias da área de segurança nacional tenderiam a ser criadas por iniciativa do Poder Executivo (com um papel secundário e sempre relutante do Parlamento), seu desenho

institucional refletiria as disputas entre as burocracias de segurança nacional e os interesses da equipe presidencial, com o Congresso exercendo um tipo de supervisão pouco sistemático e efetivo. Mas, se o Poder Executivo tem papel predominante na decisão de criar organizações de inteligência e se essas organizações respondem primordialmente aos governantes e não ao público ou seus representantes parlamentares, por que o desenho organizacional e o padrão evolutivo dos sistemas de inteligência dificultam uma resposta ágil às necessidades dos governantes, *policymakers* e comandantes militares?

A segunda tese proposta por Zegart fornece uma primeira indicação para esse aparente paradoxo: as escolhas estruturais feitas no nascimento de um órgão de segurança nacional tenderiam a durar no tempo, e só muito lentamente essas estruturas seriam alteradas pela mudança nos interesses correntes dos principais atores (*stakeholders*) e por eventos externos. O argumento da autora, resumidamente, descreve um clássico problema de relacionamento entre *principal* e *agent*: governantes eleitos (*principals*, ou “mandantes”) sofrem severos constrangimentos de tempo, conhecimento e controle sobre suas agendas políticas, e precisam realizar seus objetivos políticos contando com maioria congressual e apoio da opinião pública, que são difíceis de serem adquiridos e que não podem ser arriscados com disputas sobre coisas como o melhor desenho organizacional para uma agência burocrática qualquer. Agências de segurança nacional (*agents*, ou “agentes”) têm conhecimento especializado sobre áreas de “vida e morte” para o país, têm agendas mais delimitadas do que as dos governantes e têm fortes incentivos para participar ativamente do desenho organizacional e da definição das missões prioritárias dessas agências do setor.

Em sistemas altamente complexos e com cadeias de comando cruzadas, como a área de inteligência, isso impõe problemas de coordenação que limitam severamente a agilidade das respostas aos requerimentos de diferentes usuários (*principals*), desde os chefes de Estado e de governo até os *policymakers* e comandantes militares. Como o grau de interdependência burocrática na área de segurança nacional é maior, segundo Zegart, as disputas sobre jurisdição acrescentam mais uma dificuldade.

Para James Q. Wilson (1989:179-195), a busca por autonomia (entendida mais como jurisdição não-disputada sobre missões específicas e menos como liberdade para agir sem controles externos) é vital para qualquer organização governamental. Isso ocorre porque ganhos de autonomia diminuem os custos da manutenção organizacional na medida em que minimizam o número de atores externos interessados e os rivais burocráticos e, também, na medida em que isso maximiza as chances de a organização desenvolver um senso de missão mais coeso. Nesse sentido, a busca por autonomia tende a ser um objetivo tão ou mais importante para os dirigentes burocráticos do que a

absorção de novas tarefas ou a obtenção de maiores orçamentos, justamente porque a autonomia define os custos da aquisição e de uso dos recursos.<sup>69</sup>

No caso das Forças Armadas, de corpos diplomáticos, agências policiais e serviços de inteligência, é justamente a semelhança de muitas de suas tarefas informacionais e coercitivas que tende a tornar os conflitos por autonomia particularmente agudos e persistentes ao longo do processo de institucionalização, impondo sérios custos de coordenação que limitam a capacidade de ser ágil de qualquer serviço de inteligência.<sup>70</sup>

Diferentes sistemas nacionais de inteligência são mais ou menos institucionalizados, mais ou menos adaptáveis, complexos, autônomos e coerentes. Em síntese, mais ou menos ágeis. Como seu desempenho diferenciado tem consequências para a segurança nacional, é preciso retomar a questão deixada de lado neste capítulo sobre os possíveis efeitos de uma precária supervisão congressual para o desempenho dos serviços de inteligência e, de modo geral, para o segundo desafio associado à institucionalização: o desafio da compatibilização desses sistemas nacionais de inteligência com o princípio da transparência. Esses são os temas de fundo do próximo capítulo.

## Notas

1. Ainda hoje há um núcleo coercitivo nos Estados contemporâneos que garante os atributos centrais da soberania, sendo esta definida weberianamente enquanto autoridade exclusiva sobre um território e uma população; o fundamento último dessa autoridade repousa tanto sobre a legitimidade quanto sobre a posse concentrada de meios de força (Forças Armadas e polícias) e o monopólio da representação nacional no exterior (diplomacia). Os serviços de inteligência são organizações complementares para o exercício dessa capacidade coercitiva. A crescente complexidade do Estado moderno não autoriza a conclusão despropositada de Adam Przeworski, no de resto útil *Estado & economia no capitalismo* (1985), onde o autor afirma que o “Estado é um sistema complexo sem um centro fixo de coesão”, e cita uma afirmação ainda mais tola de Philippe Schmitter, segundo a qual o Estado capitalista contemporâneo constituiria “um complexo amorfó de órgãos governamentais com fronteiras muito mal definidas, desempenhando uma grande variedade de funções não muito diferenciadas”. Cf. Przeworski (1985:86). O Estado não é o “centro” da sociedade, como pretende a literatura estatista criticada corretamente, entre outros, por Charles Tilly (1996) e por Adam Przeworski (1999), mas disso não segue que esse sistema complexo não tenha um centro coesivo, um núcleo duro econômico e militar. Obviamente o Estado não é apenas isso, como aliás se pode verificar lendo o artigo de Thomson (1995: 213-233).
2. Para uma abordagem das instituições como variáveis independentes ou dependentes, ver os capítulos sobre o novo institucionalismo em Goodin & Klingemann (2000). Para uma discussão clássica sobre informações e *expertise* como recursos diferenciais que os burocratas têm para influenciar a política, cf. Weber (1993b). Ver principalmente os capítulos II (Domínio dos burocratas e liderança política) e IV (A direção burocrática na política externa).

3. A distinção entre organizações e instituições é fonte de confusão e polêmica na literatura especializada. Alguns autores preferem simplesmente deixar que o leitor escolha um entendimento tácito qualquer do que sejam instituições, o que impede qualquer operacionalização conceitual e testes heurísticos. Esta foi a posição adotada por Fernando Limongi em conhecida resenha publicada há alguns anos: Limongi (1994:3-38). Prefiro, para ser consistente com o ponto de partida adotado na Introdução, considerar como instituições simplesmente aquelas organizações e/ou procedimentos formais e informais que adquiriram valor e estabilidade para os atores envolvidos nas interações. Ver Huntington (1968:25-36) e Goodin (1996:21).

Devo registrar, porém, a formulação influente de Douglass North sobre o tema. Para North (1990), as organizações seriam os jogadores, enquanto as instituições seriam as regras do jogo (formais e informais). A explicação da mudança institucional seria obtida observando-se a interação ao longo do tempo entre escolhas organizacionais e diferentes conjuntos de constrangimentos institucionais. Vale aqui uma citação extensa desse autor: *"Institutions are the rules of the game in a society or, more formally, are the humanly devised constraints that shape human interaction. (...). In the jargon of the economist, institutions define and limit the set of choices of individuals. (...) Like institutions, organizations provide a structure to human interaction. Indeed when we examine the costs that arise as a consequence of the institutional framework we see they are a result not only of that framework, but also of the organizations that have developed in consequence of that framework. Conceptually, what must be clearly differentiated are the rules from the players. (...) Organizations include political bodies (political parties, the Senate, a city council, a regulatory agency), economic bodies (firms, trade unions, family farms, cooperatives), social bodies (churches, clubs, athletic associations), and educational bodies (schools, universities, vocational training centers). They are groups of individuals bound by some common purpose to achieve objectives. Modeling organizations is analyzing governance structures, skills, and how learning by doing will determine the organization's success over time. Both what organizations come into existence and how they evolve are fundamentally influenced by the institutional framework. In turn they influence how the institutional framework evolves"*. Ver North (1990:3-5).

Por outro lado, Elster (1989) propõe uma distinção entre instituições e normas sociais que poderia ser complementar à de North: "Para esse propósito, uma instituição pode ser definida como um mecanismo de imposição de regras. As regras governam o comportamento de um grupo bem definido de pessoas, por meio de sanções externas, informais, e com regras internalizadas. Um policial pode multar-me se eu jogar lixo no parque. Se não houver policial nas imediações, outras pessoas podem olhar-me ferozmente. Se não houver outras pessoas nas imediações, minha própria consciência pode ser impedimento suficiente. As instituições podem ser privadas ou públicas, dependendo da natureza das sanções". Elster (1994:174). À diferença das vertentes históricas e sociológicas de análise das instituições, a posição de Jon Elster é radicalmente individualista do ponto de vista metodológico: "Estive dizendo que as instituições 'fazem' ou 'pretendem' isso ou aquilo, mas falando estritamente, isso é bobagem. Apenas indivíduos podem agir e pretender. Se pensarmos em instituições como indivíduos em grande escala e esquecermos que as instituições são compostas de indivíduos com interesses divergentes, podemos ficar irremediavelmente perdidos. As noções, particularmente, de 'vontade popular', o 'interesse nacional' e o 'planejamento social' devem sua existência a essa confusão". Elster (1994:182). Esse é um alerta que deve ser levado em conta para que se evite a reificação dos objetos de pesquisa,

embora também seja necessário salientar que organizações como partidos, Estados e, no caso em tela, serviços de inteligência são atores coletivos irredutíveis à mera soma de suas partes individuais.

Para uma reavaliação do tema no contexto da sociologia, ver Prates (2000:123-146). Para uma crítica sociológica da “ambiguidade moral” envolvida na distinção entre normas, instituições e organizações, ver Perrow (1986:157-177).

4. Para uma revisão da agenda de pesquisa sobre os atributos da soberania, ver Thomson (1995:213-233). Sobre o papel da coerção e da informação na formação dos Estados nacionais, ver Giddens (1987). Na verdade, a literatura relevante sobre o Estado é imensurável, mas vale mencionar alguns outros trabalhos que oferecem sólidos pontos de partida. Sobre a evolução do Estado moderno, ver Strayer (1970) e também Poggi (1978). Para a relação entre capitalismo e sistema de Estados a partir do conceito de “ciclos sistêmicos de acumulação”, ver Arrighi (1996). Para uma exposição didática de teorias sobre o Estado contemporâneo, ver Dunleavy & O’Leary (1987). Para um balanço das teorias marxistas do Estado, ver Jessop (1990). Finalmente, vale confrontar ainda a revisão crítica das teorias do Estado feita por Przeworski (1985).

5. O trabalho mais recente de Tilly mantém a ênfase explicativa “centrada no Estado” no que diz respeito à direção da causalidade, mas se fortalece analiticamente ao reintegrar de forma mais sistemática no modelo a dinâmica internacional, a economia e os resultados contingentes de conflitos sociais; ver Tilly (1996). Versões anteriores menos desenvolvidas do modelo encontram-se em Tilly (1985). Ver ainda o trabalho anterior já mencionado, Tilly (1975:601-638). Para um contraponto crítico à abordagem recente de Charles Tilly, ver Spruyt (1996).

6. Ao cabo, o argumento de Tilly também é tautológico, não obstante sua tentativa explícita de evitar isso através de uma explicação de tipo genético-estratégico: sabemos que o Estado capitalista foi mais adaptativo e poderoso porque ele venceu os modelos concorrentes, e ele venceu os modelos de “intensa coerção” porque foi mais adaptativo e fundamentou-se em coalizões sociais mais poderosas. Para uma explicação macro-histórica sobre a dupla dinâmica formativa do mundo moderno (sistema de Estados e modo de produção capitalista), ver Arrighi (1996).

7. Robert Goodin (1999) menciona uma variante diferente de explicação evolutiva sobre a gênese e o desenvolvimento de instituições. Além dos mecanismos de seleção, ele usa a idéia “hegeliana” de contradição dialética como um mecanismo que força por si mesmo, independentemente da vontade dos atores, a evolução. Segundo o autor, a tensão entre uma Constituição que proclama os homens livres e iguais nos Estados Unidos e a instituição da escravidão, por exemplo, geraria inevitavelmente um *momentum* próprio de resolução da contradição, no caso, a Guerra Civil. Na situação aqui analisada dos serviços de inteligência, a tensão entre agilidade e transparência levaria, dependendo da profundidade da contradição entre os dois valores, a uma resolução sintética pela negação e destruição de um dos dois termos. Para uma crítica dessa linha de raciocínio, ver, além do próprio Goodin, que adota a perspectiva intencional/acional como central para uma teoria do desenho institucional, o texto de Pettit (1996:54-89).

8. Como se concebe a origem das instituições é um dos critérios utilizados para se distinguir as abordagens histórico-sociológicas da vertente da “escolha racional” (*rational*

*choice*) no chamado novo institucionalismo. Esse critério é complementar àquele que postula o caráter endógeno ou exógeno (em relação às interações políticas...) da formação das preferências dos atores. O que o caso dos serviços de inteligência na Europa moderna parece implicar é que ambos os critérios são falhos (assim como a própria separação entre explicação sociológica e econômica...), na medida em que tais serviços responderiam a imperativos estratégicos e a regras de adequação ao mesmo tempo. Isso reforça os argumentos de Elinor Ostrom sobre o caráter complementar dos dois tipos de explicação. Ver Ostrom (1991:237-243). Ver também Ostrom (1990). A distinção entre as três (ou quatro) vertentes diferentes do novo institucionalismo é feita precariamente por Hall & Taylor (1996). Ver também: Steinmo, Thelen & Longstreth (1992). Sobre as origens do *rational choice institutionalism* nos estudos legislativos, ver o artigo já mencionado de Limongi (1994). Um comentário bastante sensato sobre as tendências analíticas recentes nos estudos legislativos é oferecido no primeiro capítulo da tese de Melo (1999). Sobre o novo institucionalismo sociológico, ver March & Olsen (1984). Um desdobramento posterior desse artigo seminal é feito em March & Olsen (1989). Ver ainda Powell & DiMaggio (1991). Nesse volume, particularmente útil para a modelagem de estudos sobre surgimento e transformação de instituições é o artigo de Brint & Karabel (1991).

9. A ênfase no papel exclusivamente informacional dos serviços de inteligência aparece também na ciência política de corte funcionalista. Para Almond & Powell (1966), o conhecimento e a informação permeiam todas as capacidades [*capabilities*] dos sistemas políticos, tais como a capacidade extrativa, a regulativa e a distributiva, além de estarem no centro de duas delas, a capacidade simbólica e a capacidade de resposta aos *inputs* do sistema. Também desde uma perspectiva “cibernética” como a de Karl Deutsch (1966), seria a qualidade da informação que circula através dos canais de comunicações que responderia pela coesão social e, em última análise, pela possibilidade de congruência entre comandos e ações executadas: “*If politics requires a machinery of enforcement, and a set of habits of compliance, then politics is impossible without a flow of information to those who are expected to comply with the commands*”. Deutsch (1966:157). Aliás, justamente devido a essa ubiquidade da informação na sociedade e no Estado, creio que é mais produtivo e analiticamente mais relevante estudar fluxos informacionais e organizações claramente delimitados, como é o caso da atividade de inteligência por exemplo, do que pretender falar de “sociedades informacionais” ou de “era da informação”, que são expressões vazias de significado sociológico preciso.

10. Essa é a visão, por exemplo, de Norberto Bobbio: “não por acaso, a política dos *arcana imperii* caminhou simultaneamente com as teorias da razão de Estado, isto é, com as teorias segundo as quais é lícito ao Estado o que não é lícito aos cidadãos privados, ficando o Estado portanto obrigado a agir em segredo para não provocar escândalo (...). Diferentemente da relação entre democracia e poder oligárquico, a respeito da qual a literatura é riquíssima, o tema do poder invisível foi até agora pouquíssimo explorado”. Bobbio (1986:28-30). Embora o ponto de Bobbio seja normativo, a suposição de base em sua crítica é que o “governo invisível” seria algo herdado historicamente e não uma construção contemporânea dos próprios regimes e atores políticos liberais-democráticos.

11. A descrição da variação espaço-temporal do “crescimento institucional” é uma dimensão importante dos estudos sobre desempenho institucional, como destaca Robert

Putnam no capítulo introdutório de seu impressionante livro *Comunidade e democracia* (1996). Segundo o autor: "Nossa análise da evolução dos governos regionais em seus dois primeiros decênios inclui uma comparação 'antes e depois' que nos ajuda a avaliar o impacto da reforma institucional. Como a instituição e suas lideranças foram aprendendo e se adaptando com o passar do tempo – a 'biologia desenvolvimentista', por assim dizer, do crescimento institucional – é tema que se inclui em nossa pesquisa" Putnam (1996:26).

12. Esse primeiro exercício toma o roteiro de Herman (1996:2-35) e procura ampliar o uso de fontes bibliográficas que sustentem o argumento, mas é ainda nitidamente insuficiente, pois comparações internacionais sistemáticas precisariam estar baseadas em dados agregados e fontes arquivísticas para dar consequência ao programa de pesquisa descrito no texto já citado de Hasted (1991:55-72). Um exemplo do que deve ser feito em termos empíricos é o trabalho excelente em que David Bayley compara a emergência dos sistemas nacionais de polícia na Europa e tenta explicar os atributos dos sistemas policiais a partir da estrutura dos Estados, escrito há mais de 25 anos. Bayley (1975:328-379). Muitas das conclusões de David Bayley aplicam-se também para o estágio atual da pesquisa sobre serviços de inteligência.

13. Sobre a evolução das instituições diplomáticas modernas e sua relação com a espionagem, dois trabalhos principais são citados por Herman (1996:3). Para uma história mais convencional sobre as raízes da atividade de inteligência na diplomacia secreta praticada pelos soberanos modernos, ver Thompson & Padover (1965). Um trabalho mais recente, sobre o significado moderno do termo inteligência na experiência diplomática britânica e francesa a partir do século XVI, é o de Derian (1992). Embora tenha elementos interessantes aqui e ali, de modo geral o trabalho de Derian perde-se num cípóal de análises pós-estruturalistas sobre a intertextualidade dos termos inteligência e antidiplomacia, ou sobre o poder discursivo de uma concepção "cronopolítica" e "tecnoestratégica" da guerra. Para quem se interessar por uma aplicação da aparelhagem discursiva do pós-estruturalismo à discussão sobre teoria da atividade de inteligência e vigilância, ver Derian (1993:29-51).

14. A predominância de uma abordagem histórica nos trabalhos britânicos sobre inteligência favorece que se use a Inglaterra como exemplo nessa seção. Sobre as diferentes ênfases e os respectivos problemas nos estudos sobre inteligência nos Estados Unidos e na Grã-Bretanha, ver Godson & Robertson (1987). Sobre a origem, evolução e configuração atual do sistema britânico de inteligência, ver Godson (1988). Ver também os capítulos sobre Inglaterra em Richelson (1988), bem como Richelson & Ball (1985). Para a experiência da inteligência britânica na II Guerra, ver Hinsley (1993). O próprio livro de Herman (1996) traz referências importantes, embora dispersas. Ver ainda os verbetes sobre Inglaterra e agências britânicas em Polmar & Allen (1997:181-191).

15. Sobre a gênese da esfera pública burguesa e a posterior transformação da função política da esfera pública e do princípio da publicidade, ver Habermas (1994a:17-26 e 181-211). Sobre a distinção público/secreto, um comentário adicional pode ser encontrado em Bobbio (1989:176-190).

16. A atividade de decifração é tão antiga quanto o uso da escrita para a comunicação de mensagens importantes e o uso de códigos secretos para sua redação. Segundo David Kahn (1996:93), o manual de criptologia mais antigo preservado até hoje é um trabalho árabe do século IX, descoberto em 1992. Até então, acreditava-se que o documento

criptológico mais antigo fosse um outro manual árabe, escrito em 1492. O que o Estado europeu moderno talvez tenha introduzido originariamente foi a organização de serviços especializados para esse fim, mas a pequena escala das *black chambers* européias dos séculos XVI a XIX poderia perfeitamente ser equivalente ou até menor do que organizações semelhantes existentes na China ou nos califados árabes. Ver Kahn (1996).

17. Ver o capítulo 3 (As finanças, a geografia e a vitória nas guerras: 1660-1815) do livro de Kennedy (1989:79-140).

18. Ver Young (1984).

19. Na Grã-Bretanha, o Intelligence Services Act of 1994 subordinou administrativamente o SIS e o GCHQ, as duas agências de coleta de inteligência externa, ao Ministério das Relações Exteriores, o Foreign and Commonwealth Office (FCO). A subordinação direta dos órgãos de inteligência externa aos responsáveis pela tomada de decisões e implementação de políticas externas reflete a prática britânica de envolver os oficiais de inteligência e os *policymakers* no processo de preparação de *assessments*, o que no contexto norte-americano é considerado um anátema, por implicar risco de politização e enviesamento (*bias*) das análises. Para uma comparação direta entre as práticas britânicas e norte-americanas de produção de análises em inteligência, ver Herman (1994). Para uma utilização dessa variável (“grau de envolvimento da inteligência no processo de produção de políticas”) num modelo comparativo mais amplo, ver o capítulo 5 (The distinctiveness of American intelligence) de Johnson (1996:119-145).

20. O serviço de inteligência exterior (humint) mais efetivo do século XX foi o Primeiro Diretório da KGB soviético. O serviço mais eficiente foi o da Alemanha Oriental, o Hauptverwaltung Aufklärung (HVA). Ambos eram parte de organizações muito maiores, fundamentalmente voltadas à inteligência de segurança e ao policiamento político interno (caso dos diretórios de segurança da KGB e, no caso da Alemanha Oriental, da Stasi). Sobre a inserção específica do HVA e da Stasi no Ministério da Segurança do Estado da RDA, ver a autobiografia de Marcus Wolf, ex-diretor do serviço de inteligência exterior da Alemanha Oriental: Wolf & McElvoy (1997). Sobre as organizações de segurança e de inteligência da União Soviética, ver Richelson (1986) e também Parrish (1991). Sobre as organizações de inteligência e segurança da Rússia após o colapso do regime soviético em 1991, ver Galeotti (1996) e ainda Knight (1996).

21. Há várias referências à espionagem nos cinco livros de Moisés do Velho Testamento, que os judeus chamam de *Torah*, especialmente em Números, capítulo 13, onde Deus ordena a Moisés que envie espiões à terra de Canaã, sendo cada um deles de uma das tribos de Israel, cujas funções os tornam então príncipes. A outra referência direta é no livro de Josué, capítulo 2, em que Josué envia dois espiões para fazer o reconhecimento avançado de Jericó. A estada dos espiões de Josué na casa da prostituta Raabe, tal como aparece na Bíblia, provavelmente foi a origem do tratamento bastante comum da espionagem como a “segunda profissão mais antiga do mundo”. Além da Bíblia, confrontar o verbete *biblical spies* em Polmar & Allen (1997:65-66).

22. No último capítulo (XIII) do *Ping-fa*, Sun Tzu destaca o papel dos diferentes tipos de espiões para o conhecimento avançado dos planos do inimigo, das dificuldades do terreno, das movimentações e do estado de espírito das tropas. “O que possibilita ao soberano inteligente e ao bom general atacar, vencer e conquistar coisas além

do alcance dos homens comuns é a previsão. Ora, essa previsão não pode ser extraída da coragem, nem também por indução decorrente da experiência, nem por qualquer cálculo realizado. O conhecimento das disposições do inimigo só pode ser conseguido de outros homens". Sun Tzu (1985).

23. Creveld (1985:17-57).

24. Para uma análise bastante crítica sobre o significado da expressão "revolução nos assuntos militares" (RMA), ver o capítulo final de Proença Jr., Diniz & Raza (1999). Cf. também Vickers (1997). Sobre a RMA ocorrida com as guerras napoleônicas, ver o já citado Creveld (1985:58-102). Cf. também o capítulo 6 (Tactical and strategical transformation in the era of the French Revolution and Napoleon: 1791-1815) do livro de Jones (1987:320-386). Sobre inteligência e RMA nos dias de hoje, ver Fitzsimonds (1995).

25. Coakley (1991). Ver também, para aspectos mais técnicos do problema, Boyes (1985).

26. Isso não quer dizer que a espionagem militar não fosse uma prioridade dos novos serviços. Casos como o do coronel Redl (espião russo na Áustria) e do barão Schluga (espião alemão em Paris), logo antes da I Guerra Mundial, servem de lembrete contra simplificações acerca da natureza da inteligência militar. Além disso, o uso de redes extensas de fontes humanas para monitorar a mobilização e as linhas de comunicação e abastecimento nos territórios ocupados ("low level assets") também indica que não se tratava simplesmente de escolher entre fontes ostensivas e espionagem. Cf. Richelson (1995).

27. Herman (1996:16-19).

28. Para um relato histórico sobre os usos da inteligência na I Guerra Mundial, ver Richelson (1995:18-46). Para os problemas de avaliação (*assessment*) e as percepções de ameaça, ver May (1984:13-233).

29. Um comentário sobre Pearl Harbor, breve mas atualizado do ponto de vista historiográfico, pode ser encontrado em Richelson (1995:115-123). O tratamento analítico mais interessante sobre o episódio foi feito por Wohlstetter (1962).

30. A tradução mais adequada para *joint* seria conjunto, mas como no jargão militar brasileiro o termo conjunto indica uma articulação fraca ("cooperativa") entre as forças, fazendo com que o próprio Estado-maior conjunto não unifique o comando das forças singulares em operações militares, preferi adotar aqui o termo integrado (seguido da expressão internacional original entre parênteses). Para uma justificativa adicional dessa prática, ver Proença Jr. & Diniz (1998, p. 77-79, nota 6).

31. Países como a Costa Rica, que não têm Forças Armadas, poderiam ser uma exceção, mas isso dependeria de uma análise das capacidades de inteligência presentes em sua diplomacia, forças constabulares e polícia nacional. De todo modo, o problema do componente militar dos sistemas nacionais de inteligência me parece mais afeito aos Estados mais poderosos do sistema internacional, incluindo potências regionais e países relevantes em diferentes "complexos de segurança". Ver Buzan, Wæver & Wilde (1998).

32. Para uma descrição detalhada das organizações militares de inteligência norte-americanas, ver Richelson (1999:55-129).

33. Dandeker (1990:119-133). Ver também Goldstein (1983).
34. Na França, o policiamento organizado sob controle das autoridades centrais remonta à segunda metade do século XVII. Segundo Bayley (1975:343-345), a coleta de informações de segurança foi instituída já durante a Revolução Francesa, mas adquiriu uma expressão organizacional mais definida depois do *18 Brumário*. Para Charles Tilly: “Durante os anos iniciais da Revolução, as forças de polícia do Antigo Regime se dissolveram de forma geral quando os comitês populares, os guardas nacionais e os tribunais revolucionários assumiram suas atividades diárias. Todavia, com o Diretório, o Estado concentrou a fiscalização e a apreensão numa organização isolada e centralizada. Fouché de Nantes tornou-se ministro da polícia em VII/1799 e, daí por diante, passou a existir um ministério cujos poderes se estenderam a toda a França e aos territórios conquistados. Na época de Fouché, a França havia se transformado num dos países mais policiados do mundo”. Tilly (1996:174).
35. Ver Andrew (1986a) e também Fischer (1997).
36. No caso dos Estados Unidos, por exemplo, até o final da II Guerra Mundial o FBI controlava as operações de inteligência na América Latina. Mesmo após o final da Guerra Fria, há considerável pressão para a atuação internacional do órgão em temas como terrorismo, proliferação de armas de destruição maciça, crime organizado, lavagem de dinheiro, crimes eletrônicos e tráfico de drogas. Em todas essas áreas há disputas jurisdicionais com a CIA, a DEA, o Secret Service e o INR. Para uma primeira avaliação das operações do FBI no exterior, ver Holt (1995:20-37).
37. Em nenhuma dessas atividades é fácil delimitar a jurisdição das polícias e dos serviços de inteligência. As culturas organizacionais, os mandatos legais e os objetivos da coleta e análise de informações são muito diferentes nesses dois tipos de organizações estatais. Mesmo levando-se em conta que uma das matrizes organizacionais dos serviços de inteligência contemporâneos foi o policiamento político voltado para a repressão dos dissidentes, há pelo menos duas linhas de separação entre polícia e inteligência que têm sido persistentes ao longo do tempo e em diferentes contextos nacionais: a) tipicamente, enquanto as investigações criminais buscam elucidar a autoria de crimes e contravenções penais específicas, os alvos dos serviços de inteligência são atores e fenômenos mais abrangentes, os quais precisam ser conhecidos para que políticas públicas mais eficazes possam ser desenhadas. O produto final de uma investigação criminal é a instrução de um processo judicial, enquanto o produto de uma operação de inteligência é um relatório sobre o conhecimento adquirido; b) *grosso modo*, polícia cuida de problemas “internos” do país, enquanto inteligência está mais voltada para o “exterior”. Nos Estados Unidos, o National Security Act of 1947 as amended prevê, na seção que trata das atribuições do DCI, que as responsabilidades da CIA (uma organização diretamente subordinada ao DCI) envolvem a coleta de inteligência de fontes humanas e através de outros meios, com a exceção de que a CIA não deve exercer quaisquer funções de polícia, de intimidação judicial, de imposição da lei ou de segurança interna (“*the Agency shall have no police, subpoena, or law enforcement or internal security functions*”). Ver Section 103 (d) (3) [50 US Code 403-1], National Security Act of 1947, em US Congress (1998b:14). Essa restrição legal foi justificada pelos legisladores norte-americanos do imediato pós-II Guerra como necessária para evitar que a CIA se transformasse numa espécie de Gestapo nas mãos de presidentes inescrupulosos. Mas ela também refletia o *lobby* do

FBI contra o que era considerado uma violação de sua jurisdição. Afinal, desde pelo menos 1919, a polícia federal norte-americana também tinha uma divisão especializada em inteligência de segurança (*security intelligence*) contra a espionagem internacional, a sabotagem, a “subversão comunista” e, mais tarde, voltada para a obtenção e análise de informações sobre o crime organizado, terrorismo internacional e doméstico, além de organizações clandestinas utilizando “violência politicamente motivada” (PMV). Na prática, nem a CIA acatou 100% a prescrição legal de não se envolver em operações de inteligência doméstica, nem o FBI absteve-se 100% de ir ao estrangeiro e montar suas próprias redes de informações sobre temas determinados pelo diretor. Além de abusos de poder e extrapolação de mandatos, isso decorreu das dificuldades inerentes a uma separação entre as funções de inteligência externa, inteligência de segurança para fins internos, contra-inteligência (em suas dimensões defensivas e ofensivas) e inteligência policial, mais próxima da investigação criminal propriamente dita. Mesmo nos países que procuraram delimitar legalmente as jurisdições sobre essas áreas, a complexidade atual do fenômeno criminal e o crescimento de ameaças transnacionais à ordem pública e aos ordenamentos legais dos países estão forçando uma significativa revisão de fronteiras. Para um comentário sobre o caso dos Estados Unidos, ver Snider (1995:243-264).

Vale notar o comentário de John Coleman no mesmo volume sobre as dificuldades operacionais no relacionamento entre a CIA e a Drug Enforcement Administration (DEA) em países latino-americanos e, de modo geral, sobre as dificuldades de relacionamento entre as agências policiais e os órgãos de inteligência. Na época em que redigiu o comentário, Coleman era o chefe de operações da DEA em Nova Jersey, mas já exercera a função de conselheiro do diretor da DEA para programas no estrangeiro. Para a dificuldade que os serviços de inteligência têm com suas próprias unidades de contra-inteligência e com a atuação das organizações de “*law enforcement*” na área de contra-inteligência, ver Hulnick (1997:269-286).

38. Nos países que seguiam o modelo soviético (KGB), havia uma organização centralizada de inteligência e segurança, organizada em moldes militares, dividida em diretórios responsáveis por humint, contra-inteligência, inteligência de segurança, operações encobertas, sigint, infosec etc. A manutenção da ordem pública e a repressão política eram realizadas também pelas polícias e pelas tropas do Ministério do Interior (MVD). O modelo de organização do aparato de segurança e inteligência brasileiro durante o regime militar (1964/85), baseado numa agência central (SNI) que vertebrava um sistema nacional (Sisni), foi descrito por analistas como mais próximo do modelo soviético do que dos modelos liberais ocidentais. Cf. Stepan (1988:19-20). Ver também Bruneau (2000:1-36).

39. Sobre as missões do FBI na área de inteligência doméstica (*security intelligence*), contra-inteligência e contraterrorismo, ver Watson (1995). Sobre as funções de inteligência policial e análise criminal, ver Peterson (2000).

40. Sobre as agências de inteligência do Japão, ver Hansen (1996).

41. Isso resulta do fato de as próprias polícias originarem-se em parte das Forças Armadas, a partir de uma bifurcação de missões que, na Europa, ocorreu em épocas muito diferentes em cada país. Na Inglaterra essa divisão é clara desde o surgimento do atual modelo de policiamento civil, entre 1829 e 1889. As linhas militares de organização do trabalho policial predominam ainda hoje em muitos países, como a Itália, a França, a Rússia e o

Brasil. Por outro lado, hoje em dia a maioria das Forças Armadas tem organizações de segurança e contra-inteligência próprias, inclusive em nível ministerial, como é o caso do Defense Security Service (DSS) do Departamento de Defesa dos Estados Unidos. Embora essas organizações tenham como missão a proteção de segredos governamentais, o que as torna bastante próximas dos serviços de inteligência propriamente ditos na medida em que existem trocas de experiência que beneficiam mutuamente as operações informacionais ofensivas e defensivas, elas não são formalmente consideradas parte integrante dos sistemas nacionais de inteligência. Como mencionado, a principal organização departamental de inteligência do Departamento de Defesa dos Estados Unidos é a Defense Intelligence Agency (DIA). Em outros países, a contra-inteligência e a inteligência de segurança são ainda fortemente vinculadas à inteligência militar. Na Inglaterra atual, o serviço de inteligência de segurança é uma organização civil subordinada diretamente ao ministro do Interior.

42. Para um excelente tratamento do caso inglês em perspectiva comparada com os sistemas policiais da França, Alemanha e Itália, ver o texto já citado de Bayley (1975:328-379).

43. Atualmente, o SIS é subordinado ao Foreign Office e o MI-5 é subordinado ao Home Office, que são, respectivamente, os ministérios das Relações Exteriores e do Interior no governo britânico.

44. Ver, por exemplo, o excelente trabalho de Gill (1994).

45. Esses percentuais sobre prioridades e alocações de recursos estão disponíveis em <<http://www.mi5.gov.uk>>.

46. Canadá (1999). Sobre os serviços de inteligência de segurança de Canadá, Inglaterra, Rússia, França e Estados Unidos, ver Richelson (1988).

47. No Brasil, o Decreto nº 3.448, de maio de 2000, criou um Subsistema Brasileiro de Inteligência de Segurança Pública no âmbito do Sistema Brasileiro de Inteligência (Sisbin), que por sua vez fora instituído pela Lei nº 9.883/99, a mesma lei que criou a Agência Brasileira de Inteligência (Abin). Em tese, a criação de um subsistema de inteligência de segurança pública permitiria a coordenação, a integração e o compartilhamento de informações relevantes nas áreas de inteligência de segurança, contra-inteligência e inteligência policial. Integram o subsistema a própria Abin, o Gabinete de Segurança Institucional (GSI) da Presidência da República, o Ministério da Justiça (através da unidade de inteligência da Polícia Federal), o Ministério da Defesa, o Ministério da Integração Regional (através da área de Defesa Civil) e, mediante adesão, os órgãos de inteligência das polícias civis e militares dos 26 estados e do Distrito Federal. Além da forte rivalidade entre a PF e a Abin, a efetivação do decreto terá ainda que superar a precariedade (em termos de agilidade e transparência) das unidades de inteligência das polícias militares e civis, cuja reforma ainda sequer foi iniciada na maioria das unidades da Federação. O Decreto nº 3.448/00 e a Lei nº 9.883/99 estão disponíveis em formato pdf na página da Abin: <[www.abin.gov.br](http://www.abin.gov.br)>.

48. Para um comentário útil sobre inteligência policial, mais especificamente sobre as relações entre investigação criminal e operações de coleta de inteligência, ver Lyman (1999:425-427). Sobre inteligência criminal enquanto produto analítico, ver Peterson (1994). Referências adicionais podem ser encontradas na página da International Association of Law Enforcement Intelligence Analysts: <<http://www.ialeia.org>>.

49. A Marinha foi a única força armada dos Estados Unidos que manteve um comando de primeiro escalão separado para as funções de sigint e infosec/comsec. No Exército (Inscom), Força Aérea (AIA) e Fuzileiros Navais (MCIA) essas funções são exercidas por comandos subordinados de segundo escalão, que também podem ser colocados sob opcon do diretor da NSA. Aliás, o pessoal do Inscom é encarregado da operação das principais estações fixas de interceptação da NSA no exterior. Ver Richelson (1999:55-129).

50. Para uma visão mais detalhada das mudanças organizacionais na inteligência militar nos Estados Unidos, ver o livro já citado de Richelson (1999:55-129). Para uma discussão mais detalhada das linhas de comando e controle em inteligência militar, ver a seção IV (The Defense Department's Intelligence Structure: a review and recommendation for reform) do relatório de Odom (1997:51-68). Sobre a integração vertical da área de sigint no *establishment* de defesa daquele país, ver a seção V (The signals intelligence discipline: structure and management) do mesmo relatório: Odom (1997:69-78). Sobre doutrina de operações integradas em inteligência, ver três documentos principais: a) Joint Intelligence Support to Military Operations. DoD Joint Publication # 2-01. November, 1996. 175pp. b) Joint Intelligence Doctrine. DoD Joint Publication # 2-0. May, 1995. 189pp. c) Intell XXI: A Concept for Force XXI Intelligence Operations. Tradoc Pamphlet 525-XX. January, 1996. 80pp. Esses documentos estão acessíveis na página do Pentágono na internet: <<http://www.defenselink.mil/pubs>>.

51. Em Israel, por exemplo, a principal instância de coordenação ainda é o comitê dos dirigentes das agências de inteligência, segurança e polícia, o Va'adat Rashei Hasherutim (Vaadat), que é coordenado pelo chefe do Mossad. Mas o gabinete do primeiro-ministro tem agora uma unidade própria de supervisão e definição de prioridades de coleta de informações (*requirements*) que coordena suas atividades com o Vaadat. No Brasil, a Agência Brasileira de Inteligência (Abin) é o órgão central e, do ponto de vista legal, coordena o Sistema Brasileiro de Inteligência (Sisbin). Embora a agência devesse ser ligada diretamente ao presidente da República segundo os termos de sua lei de criação, na prática a Abin encontra-se subordinada ao Gabinete de Segurança Institucional (GSI) da presidência da República. A supervisão externa será feita, segundo a legislação em vigor em julho de 2000, pela Câmara de Relações Exteriores e Defesa Nacional (Creden) do Conselho de Governo, no Poder Executivo, e por comissão mista da Câmara dos Deputados e do Senado Federal. Ver Antunes (2000).

52. Os quatro sistemas nacionais de polícia analisados por David Bayley foram diferenciados em 13 atributos: 1. Maior ou menor extensão das tarefas formais, tais como a prevenção do crime e a fiscalização da cobrança de impostos. 2. Maior ou menor extensão das tarefas informais, tais como a mediação de conflitos entre as partes. 3. A presença ou não de tarefas políticas, tais como a segurança do regime político, do governo ou mesmo a coleta de inteligência. 4. O grau de agregação da autoridade sobre as unidades do sistema (local ou nacional, descentralizada ou centralizada). 5. O número de forças policiais especializadas. 6. A esfera de controle político, se local ou nacional, e se a prestação de contas é feita para um corpo político representativo ou burocrático. 7. A esfera de controle legal, se a polícia submete-se a um sistema legal unificado ou a cortes administrativas especiais. 8. Se a carreira é unitária ou se é diferente para oficiais e para policiais/práças. 9. Se o treinamento é predominantemente militar ou civil. 10. Se a especialização funcional é alta ou baixa, por exemplo, em relação a patrulhamento, investigação criminal, periciamento técnico, guarda de fron-

teiras, polícia fiscal etc. 11. Como a polícia é percebida pelo público em relação a temas como confiabilidade, autoritarismo, corrupção, eficiência etc. 12. Se o modo de intervenção policial é mais ou menos individualizado, mais ou menos formal. 13. Dinâmicas do uso da força e de armamento. Embora os quatro casos sejam significativamente diferentes entre si, se fosse para tratar esses indicadores tipológicos como parte de um *continuum*, a Inglaterra de 1975 estaria num extremo e a Itália em outro. Tomando como ponto de partida essa diferença, Bayley estuda por que as características decisivas dos sistemas de cada país formam-se em diferentes períodos do processo moderno de desenvolvimento nacional e quais as variáveis independentes mais importantes na explicação dos atributos de cada caso nacional. Ver Bayley (1975).

53. Um conjunto adicional de interações entre variáveis é utilizado pelo autor para explicar as diferenças entre os quatro casos. Em especial, Bayley destaca que as práticas de organização do poder anteriores ao momento de surgimento e amadurecimento dos sistemas nacionais de polícia influenciaram diretamente a abrangência das tarefas e o grau de centralização do sistema. A natureza da violência social existente, a presença ou não de uma forte resistência popular ao governo, a mudança nas demandas sociais por lei e ordem como resultado da composição interna da população, a existência ou não de ortodoxias religiosas ou políticas, as reações das elites à incorporação e, finalmente, a própria posição internacional do país, de maior ou menor segurança internacional. Ao final do ensaio, Bayley levanta uma hipótese interessante sobre a tendência a uma maior convergência internacional dos padrões nacionais de organização, procedimentos e *accountability* no trabalho policial. Essa convergência seria muito mais clara em relação ao desempenho operacional, onde existem medidas e padrões relativamente internacionalizados. Ver Bayley (1975:328-379).

54. Um trabalho clássico sobre a expansão do governo central nos Estados Unidos é Löwi (1979). Os dados mencionados aqui são retirados de Stanley & Niemi (1995), e também do Banco Mundial (1997). Para dados comparativos sobre gastos governamentais que invalidam o núcleo da teoria da escolha pública sobre os “gastos excessivos”, ver Przeworski (1985:85).

55. Ver Zegart (1999).

56. Para uma síntese das premissas neo-institucionalistas e de sua aplicação ao estudo das burocracias domésticas de serviços e de regulação, ver Moe (1990).

57. No capítulo 1 (*Towards a theory of national security agencies*), além do tema principal sobre a necessidade de reformular o modelo neo-institucionalista para dar conta das diferenças entre agências domésticas de políticas públicas e agências de segurança nacional, Zegart também faz comentários úteis, embora incidentais, sobre as diferenças entre o novo institucionalismo e a abordagem da política burocrática (Graham Allison). O esquema analítico de Zegart é ousado e de modo geral bastante consistente, mas três aspectos me pareceram muito problemáticos. Primeiro, seu ponto de partida para propor um modelo de agências de segurança nacional é uma crítica superficial e absolutamente equivocada ao “realismo” na área de relações internacionais. Além de errada, sua crítica é fútil, pois não tem nenhuma função posterior na construção do modelo. Em segundo lugar, é problemática sua suposição de que os presidentes, ao contrário dos legisladores e dos burocratas, são mais protegidos do assédio dos grupos de interesses e têm mais incentivos para concentrarem-se em grandes temas nacionais.

Afinal, esses incentivos não surtiram muitos efeitos em alguns dos presidentes norte-americanos que mais influenciaram o desenho organizacional das agências de segurança nacional (ex.: Truman, Reagan e Clinton). A própria caracterização dos presidentes como agentes perfeitos do público e vítimas indefesas do poder dos burocratas é claramente demasiada. Finalmente, a excessiva preocupação de Zegart em não parecer “funcionalista” e concentrar sua explicação nas preferências e constrangimentos institucionais dos agentes fez com que seu modelo subestimasse a um ponto inaceitável o conhecimento sobre o que as agências realmente “fazem”, ignorando as funções exercidas e os requisitos tecnológicos como fatores explicativos sobre o desenho organizacional das agências de segurança nacional. Além desses três problemas mais sérios, o critério de diferenciação entre agências domésticas e agências de segurança nacional baseado no grau de interdependência burocrática (“degree of bureaucratic interconnectedness”) me parece exigir maior especificação, pois a falta de delimitação clara de jurisdição entre agências ocorre também – e talvez em graus mais elevados – em setores da burocracia no ambiente interno (ex.: atividades urbanas ou planejamento governamental). O último ponto é que sua pretensão (explicitada na Conclusão do livro) de estar fundando as bases para uma “teoria geral da burocracia” parece esbarrar nos problemas mencionados e também na necessidade de muitos estudos comparativos em escala internacional. Ver Zegart (1999:12-53 e 223-236).

58. Os dados sobre grupos de interesse utilizados por Amy Zegart são resultados de pesquisas sobre associativismo civil, *lobbies* no Congresso e fontes de financiamento de campanhas de deputados. Os grupos de interesse na área de segurança nacional são mais recentes: enquanto 75% dos *Think Tanks* de política internacional e dos escritórios de *lobby* na área de defesa sediados em Washington, DC, começaram a operar na década de 1970, organizações ambientalistas como o Sierra Club (1892), associações empresariais como a National Association of Manufacturers (1892) e grupos de pressão temáticos como a National Education Association (1857) são muito mais consolidados. Os grupos de interesse na área de segurança nacional são menos numerosos: em 1990, de um total de 9.138 grupos de pressão atuando sobre o Congresso dos Estados Unidos, 922 eram de alguma forma relacionados com assuntos internacionais. Os grupos da área de saúde sozinhos eram mais numerosos (1.054) do que os de política externa. Em terceiro lugar, grupos de interesse na área de segurança nacional investem menos nas campanhas dos congressistas membros dos comitês de sua área. Segundo Zegart, enquanto um membro do Senate Committee on Banking recebia em média 29% dos recursos para campanha de doadores de fundos relacionados ao setor bancário, um membro do Senate Committee on Armed Services recebia apenas 6% dos fundos de sua campanha de doadores com interesses no setor. Ver Zegart (1999:22-27 e 239-240).

59. Ver, por exemplo, o projeto internacional de pesquisa comparada Intelligence and Democracy in the Americas: Challenges for the 21st Century, no qual os pesquisadores estão trabalhando com uma versão modificada do modelo neo-institucionalista para analisar as recentes reformas nos serviços de inteligência na Argentina, Brasil, Chile, Equador e Guatemala: <<http://www3.ndu.edu/chds>>.

60. As diferenças existentes entre as próprias burocracias de segurança nacional (NSC, JCS e CIA) desdobram-se na diversidade interna dos próprios sistemas de inteligência (CIA, FBI, DIA etc.). Os padrões de desenvolvimento dos sistemas nacionais de inte-

ligrências refletem também essas diferenças entre os vários tipos de organizações de inteligência, bem como suas diferenças em relação às Forças Armadas, polícias, serviço diplomático ou instâncias de formulação de políticas (tais como os *staffs* dos conselhos nacionais de segurança). Entre os dois tipos extremos de organizações governamentais, Zegart aponta a necessidade de incorporar a uma teoria geral da burocracia uma vasta quantidade de agências que ficariam a meio caminho no *spectrum* burocrático. Em particular, seria interessante ver como ficariam posicionadas no modelo as organizações de política econômica que atravessam a dicotomia externo/interno (bancos centrais, comércio exterior, conselhos de política econômica etc.). Ver Zegart (1999:233).

61. Para uma escala comparativa (muito limitada) entre (poucos) casos nacionais que situa as posições de cada país ao longo de um *continuum* e não de forma polar, ver Johnson (1996:119-145).

62. Para uma descrição sumária dos sistemas de inteligência de países selecionados, ver <[www.fas.org/irp](http://www.fas.org/irp)>.

63. A comparação direta entre Estados Unidos e Grã-Bretanha é feita com base em Herman (1996:29-38).

64. Cf. a seção 3 do National Security Act of 1947 as amended. Os itens G e J do § 4º da seção 3 desse ato deixam em aberto a inclusão de quaisquer outros departamentos ou escritórios como parte da IC, conforme o DCI e o presidente julgarem adequado. Deriva dessa abertura legal a confusão sobre a inclusão ou não de importantes agências governamentais norte-americanas como parte das capacidades de inteligência daquele país. Para uma abordagem mais detalhada sobre o sistema norte-americano, ver Richelson (1999:16-149), especialmente os capítulos 2 a 6.

65. Ver <[www.fas.org/irp/budget.html](http://www.fas.org/irp/budget.html)>. Sobre a dinâmica de preparação do orçamento de inteligência nos Estados Unidos, ver Lowenthal (2000:34-38) e, principalmente, Elkins (1997).

66. Atualmente o governo britânico publica na internet alguns dados básicos sobre as agências civis de inteligência, mas quase nada sobre as capacidades de inteligência das Forças Armadas, por motivos que podem ser considerados óbvios por enquanto: <[www.cabinet-office.gov.uk/cabsec/1998/cim](http://www.cabinet-office.gov.uk/cabsec/1998/cim)>.

67. A decisão de tornar público o agregado orçamentário das três agências britânicas principais de inteligência foi tomada pelo governo trabalhista do primeiro-ministro Tony Blair em 1998. Ver <[www.cabinet-office.gov.uk/cabsec/1998/cim](http://www.cabinet-office.gov.uk/cabsec/1998/cim)>.

68. Ver Herman (1996:341-361).

69. A formulação de James Q. Wilson é uma resposta direta às abordagens predominantes sobre o comportamento dos burocratas, derivadas da teoria da escolha pública (*public choice theory*). Cada autor define a autonomia das agências governamentais de acordo com sua premissa sobre o que quer que sejam as preferências fundamentais dos burocratas: maximização de orçamentos, de recursos organizacionais, de prestígio, de remuneração pessoal, de estabilidade funcional, “*bureau shaping*”, jurisdição indisputada etc. De todas essas, a mais plausível me parece ser essa de Wilson (autonomia), na medida em que consiste em uma suposição substantiva sobre as preferências dos burocratas (atendendo assim à exigência metodológica da economia neoclássica

sobre o confinamento dessas suposições ao lado da oferta), ao mesmo tempo em que essa suposição consiste em afirmar a busca de autonomia como uma precondição para outras preferências endogenamente formadas nas próprias interações conflitivas. Sobre autonomia e a racionalidade desses “*bureaucratic turfs*”, ver Wilson (1989). A posição de Wilson sobre a autonomia burocrática é, nesse aspecto, compatível com as posições de Adam Przeworski (“o Estado é ‘autônomo’ quando ele formula suas próprias metas e as realiza em face da oposição”) e do próprio Samuel Huntington (“institucionalização política, no sentido de autonomia, significa o desenvolvimento de organizações e procedimentos políticos que não sejam apenas expressões dos interesses de grupos sociais determinados”). Para a “explicação” do crescimento institucional baseada na postulação de que burocratas maximizam orçamentos e ofertam níveis excessivos de serviço (subótimos para o público) porque são precariamente supervisados, ver dois textos seminais da *public choice*: Niskanen (1977) e também Buchanan (1977). Para uma exposição didática das diversas ramificações dessa literatura, ver o texto já citado de Wayne Parsons (1995:306-323). Para uma crítica da explicação da autonomia estatal feita pela corrente principal da *public choice*, ver Przeworski (1985:77-85). Para uma crítica do modelo “maximizador de orçamentos” e a formulação alternativa de um modelo explicativo do “crescimento institucional” baseado nas alternativas estratégicas e nos dilemas de ação coletiva dos burocratas (“*bureau-shaping model*”), ver Dunleavy (1991:147-259).

70. Se as agências governamentais conseguem garantir razoavelmente sua autonomia, então elas provavelmente vão tentar obter mais recursos ou ampliar sua jurisdição. O problema, segundo James Wilson, é que isso envolve um enorme “se” condicional: “*Turf problems were not major problems when the only important federal agencies were the Post Office, the Pension Bureau, the Army, and the Customs Service. Turf problems are large, and largely insoluble, when the government has within it dozens of agencies that make foreign policy, scores that make or affect economic policy, an countless ones that regulate business activity and enforce criminal laws*” Wilson (1989:195). Disputas interburocráticas não são insanáveis e tampouco são irracionais, apenas são difíceis porque envolvem aspectos vitais da identidade e das preferências de atores políticos organizados.



## Capítulo 3

### Segurança nacional, segredo e controle

*Since we have argued that there are some values and institutions embodied in the state which genuinely merit being ‘secured’, we cannot dismiss the problem by contending that ‘national security’ is simply a sham, a dishonest slogan designed to favour ‘sinister interests’ and to legitimate various forms of repression. Rather, the state is simultaneously protector and threat to vital personal and political values, and we must all live with the inescapable contradiction as best we can.*

Lustgarten & Leigh (1994:22).

O tema da transparéncia dos atos governamentais é cada vez mais recorrente na discussão atual sobre a democracia. Um dos aspectos mais difíceis dessa discussão é o da relação entre segurança nacional, segredo governamental e controle das atividades de inteligência, pois esse tema revela o quanto a busca por transparéncia no Estado contemporâneo constitui um dilema do processo de institucionalização. Os governantes tendem a justificar institucionalmente e a delimitar as funções dos serviços de inteligência em termos de sua necessidade para a segurança nacional. As prioridades, recursos, estruturas organizacionais, missões e alvos das operações de inteligência e de contra-inteligência são definidos e hierarquizados, na melhor das hipóteses, segundo a escala de preferências dos responsáveis pela segurança nacional. Entretanto, a própria noção de segurança nacional é problemática, pois tanto o seu significado quanto as consequências práticas de seu uso estão longe de ser auto-evidentes.

Daí ser inconsistente pretender resolver o debate sobre a justificação pública do valor da atividade de inteligência apenas referindo-se genericamente às necessidades da segurança nacional. Em particular, a recorrente utilização da noção de segurança nacional como um princípio de justificação de práticas políticas repressivas e autoritárias torna questionável a compatibilidade entre tal noção e uma concepção democrática de governo e de resolução de conflitos nas sociedades contemporâneas. Por outro lado, dada a irredutibilidade da segurança coletiva à segurança individual, não é possível simplesmente abandonar o conceito de segurança nacional.

Considerando essa dupla dificuldade, pretendo argumentar que a tensão entre segurança estatal e segurança individual é ineliminável no contexto atual, e que isso tem repercussões decisivas para se pensar o papel das organizações de inteligência e de segurança no Estado contemporâneo, particularmente o problema da transparência dos atos governamentais nesse tipo de atividade.

Parece adequado começar sistematizando as justificativas políticas e os principais riscos e tensões associados à noção de segurança nacional. Isso será feito através da análise crítica de duas tentativas recentes de superação dos impasses da noção convencional de segurança nacional: 1. o fracasso da rentativa liberal de delimitar juridicamente as situações em que os governantes poderiam mobilizar as razões da segurança nacional para justificar práticas políticas; 2. as possíveis consequências não antecipadas pelas propostas de substituição do conceito de segurança nacional pelo conceito de segurança humana como base para as políticas públicas nas áreas de defesa e inteligência.

Em seguida discute-se o segredo governamental como um dos pilares da segurança nacional, analisando-se também o papel do segredo nas operações de inteligência, bem como o papel das agências de inteligência na formação de um sistema de segredo governamental, além dos custos do segredo em termos de eficiência e controle público. Realizados esses dois exercícios, é possível avaliar criticamente os limites e os desafios dos mecanismos de supervisão e prestação de contas (*accountability*) que garantiriam o controle externo sobre os serviços de inteligência.

## Segurança nacional

Como ponto de partida para a discussão, serão apresentadas algumas definições mínimas sobre segurança, segurança nacional e ameaças. Essas definições mínimas serão posteriormente contrastadas com a concepção liberal de segurança nacional e com a abordagem da segurança humana. Ao final desta seção serão oferecidas algumas indicações provisórias sobre a abordagem dos problemas de segurança nacional realizada a partir da chamada “teoria dos complexos de segurança”.<sup>1</sup>

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.

As medidas de proteção devem guardar certa proporcionalidade em relação às ameaças percebidas contra a existência, a efetividade e a autonomia de quem – ou do que – está sendo protegido. Na ausência de proporcionalidade,

a busca de segurança torna-se ela própria uma ameaça à efetividade, à autonomia e, no limite, à própria existência do “objeto” da proteção. O requisito de proporcionalidade serve principalmente para problematizar a noção de segurança enquanto uma condição absoluta de ausência de ameaça ou mesmo de incerteza.<sup>2</sup> A proteção total de tudo e/ou de todos, contra tudo e/ou todos, é algo não apenas impossível do ponto de vista material e psicológico, mas indesejável enquanto pretensão totalitária. Ter isso claro é crucial para iniciar qualquer discussão sobre segurança nacional.<sup>3</sup>

Por segurança nacional entende-se aqui uma condição relativa de proteção coletiva e individual dos membros de uma sociedade contra ameaças à sua sobrevivência e autonomia. Nesse sentido, o termo refere-se a uma dimensão vital da existência individual e coletiva no contexto moderno de sociedades complexas, delimitadas por Estados nacionais de base territorial.<sup>4</sup> No limite, estar seguro nesse contexto significa viver num Estado que é razoavelmente capaz de neutralizar ameaças vitais através da negociação, da obtenção de informações sobre capacidades e intenções, através do uso de medidas extraordinárias e do leque de opções relativas ao emprego de meios de força. A dupla face dessas ameaças, interna e externa, implica algum grau de complementaridade e de integração entre as políticas externa, de defesa e de provimento da ordem pública.<sup>5</sup> A segurança nacional, como uma condição relativamente desejável a ser obtida através dessas políticas públicas, fornece a principal justificativa para o exercício da soberania e o monopólio estatal do uso legítimo de meios de força.<sup>6</sup>

A grande maioria dos ordenamentos constitucionais contemporâneos reconhece a agressão militar, a espionagem, as operações encobertas, a invasão territorial e o bloqueio econômico como ameaças externas vitais, capazes de engendrar respostas dissuasórias proporcionais por parte dos Estados ameaçados. Ameaças internas seriam, caracteristicamente, os apoios internos àquelas ameaças externas, acrescidas da problemática noção de “subversão” (uso sistemático da violência para forçar mudanças sociais, políticas e legais).<sup>7</sup> Nas últimas décadas, foi acrescentada uma nova categoria de ameaças transnacionais ou transestatais à segurança nacional, tais como o crime organizado, o narcotráfico e o terrorismo.<sup>8</sup>

Apesar da definição de segurança nacional e da delimitação jurídica das ameaças, apresentadas nos dois parágrafos anteriores, é importante insistir que o significado do termo e as consequências práticas de sua utilização variam enormemente em diferentes contextos políticos e institucionais.

Longe de resolver os problemas, qualquer definição constitui apenas um ponto de partida muito precário para a reflexão. Na verdade, a própria insistência em um conceito abstrato e atemporal de segurança nacional, aplicável a quaisquer contextos e circunstâncias, torna-se parte do problema,

pois tende a separar arbitrariamente a chamada “baixa” política dos conflitos de opinião e de interesses daquilo que seria a “alta” política relativa aos problemas de segurança e de uso da força nas relações entre Estados (e também nas relações sociais dentro dos Estados). Em geral, essa insistência num conceito absoluto de segurança nacional tende a “despoliticizar” de forma autoritária o conceito, desautorizando a própria discussão sobre o tema.

Em se tratando de regimes democráticos, é preciso um esforço na direção contrária, trazendo os temas de segurança, defesa, inteligência e policiamento para a agenda regular dos debates políticos sobre políticas públicas.<sup>9</sup> Certamente há restrições para isso, especialmente aquelas relacionadas ao segredo governamental (que serão discutidas na próxima seção), mas não há motivo para se pensar que tais temas sejam dotados de qualquer tipo de sacralidade que impeça a pesquisa teórica ou empírica nessa área importante de atuação do Estado.

Um passo importante para avançar a discussão sobre segurança pode ser dado através da avaliação de duas tentativas recentes de superação dos impasses da segurança nacional.

Primeiro, a tentativa frustrada de resolver a tensão entre segurança estatal e segurança individual pela via estritamente jurídica e normativa. Essa tem sido a posição liberal típica no debate internacional, e embora ela contribua para uma avaliação dos riscos inevitáveis para a democracia, ocasionados pela operação de organizações de força e de inteligência responsáveis pela segurança nacional, tem sido incapaz de ir além da delimitação jurídica das ameaças consideradas legalmente válidas para que um governo possa alegar razões de “segurança nacional” para seus atos.

Segundo, os riscos de se tentar resolver a ambigüidade moral do conceito de segurança nacional através do recurso ao conceito de segurança humana (*human security*). A crítica dessa tentativa permitirá que se tenha uma avaliação mais precisa dos riscos de perda de eficiência na operação das Forças Armadas e dos serviços de inteligência, principalmente em função da expansão excessiva do leque de requerimentos defensivos e informacionais resultantes da adoção do conceito de segurança humana como um parâmetro para o planejamento de políticas de segurança. Além de resultar em perda de eficiência, uma eventual ancoragem das missões das Forças Armadas e dos serviços de inteligência no conceito de segurança humana traz riscos adicionais para a política democrática ao “securitizar” temas e problemas não relacionados ao uso potencial da força (educação, meio ambiente, saúde etc.).

Em relação ao primeiro tema, é preciso começar notando, junto com autores como Barry Buzan (1991:35-56) e Charles Tilly (1996:397-412), que as relações de segurança são inextrincáveis entre os diferentes níveis de

análise (sistêmico, estatal e individual) das relações internacionais. O sistema internacional como um todo, subsistemas regionais e funcionais, atores unitários, tais como Estados ou organizações intergovernamentais, subunidades, como agências governamentais e grupos sociais, ou mesmo indivíduos, afetam uns a segurança dos outros de maneiras variadas. Mudanças políticas internas em um país, por exemplo, alteram as intenções e a capacidade diplomática e militar daquele país no ambiente internacional, alterando assim a distribuição de poder no sistema internacional. Por sua vez, um traço estrutural do sistema internacional (a ausência de governo mundial, ou anarquia) produz consequências para o comportamento das unidades do sistema (mecanismo de *self-help*, ou autodefesa) que, por sua vez, afeta os grupos e indivíduos nos Estados.

Entretanto, a relevância do conceito de segurança varia bastante ao longo dos níveis de análise. Isso acontece porque problemas de segurança referem-se mais diretamente às relações políticas de amizade e inimizade (ameaças) que acompanham a escala dos “objetos referentes” ao longo dos diferentes níveis de análises.

Argumentando em termos pragmáticos, Buzan, Wæver e Wilde (1998:35-42) sustentam que os objetos referentes de uma ameaça precisam ser de uma escala intermediária entre o indivíduo e a humanidade para que consigam obter atenção e legitimar seus clamores de segurança, mobilizando a ação de outros atores nas relações internacionais. Indivíduos e pequenos grupos sociais raramente têm conseguido obter atenção pública para suas necessidades de segurança, assim como têm fracassado as tentativas de afirmar a humanidade inteira como um referente adequado para problemas de segurança (não obstante o temor do holocausto nuclear durante a Guerra Fria ou a percepção de ameaça sobre a degradação ambiental à escala global nas últimas décadas). Note-se que esses autores reconhecem a primazia analítica dos Estados em relação aos problemas de segurança, mas não a consideram exclusiva, inevitável ou perene.

Por sua vez, Lustgarten e Leigh (1994:3-35) reconhecem que, embora em termos axiomáticos apenas a segurança dos indivíduos conte do ponto de vista moral, em termos empíricos o fator singular mais importante e abrangente no condicionamento das “chances de vida” de um indivíduo ainda é o seu “pertencimento” a um Estado nacional (cidadania). A inserção dos indivíduos na família, mercado, classe social, etnia, gênero ou faixa etária não teria impactos similares em termos de segurança para a sua existência pessoal. Embora essa seja uma posição disputável pelo menos em relação à classe social, ela tem a vantagem de tornar evidente por que as preocupações com a segurança do Estado não são meras derivações ou extensões das preocupações com a segurança dos indivíduos.<sup>10</sup>

Estados têm primazia como objetos de segurança porque sua existência é uma condição necessária para a realização de qualquer valor individual ou coletivo num sistema internacional caracterizado pela anarquia.<sup>11</sup> Daí que o direito internacional público identifique a segurança nacional com a segurança estatal. Independentemente das suas diferenças em relação a qualquer um dos quatro componentes que definem os Estados enquanto uma “classe de objetos” (a base física formada por uma população e território, as instituições de governo, alguma idéia justificadora que torna aquelas instituições legítimas aos olhos da população e a soberania, que se desdobra em exercício exclusivo da autoridade interna e controle de fluxos diversos de interações com outras unidades soberanas), todos os Estados têm como preocupações fundamentais a continuidade de sua existência organizacional, a manutenção de sua integridade territorial, a sobrevivência de sua população e a independência em relação a outros governos.<sup>12</sup> O desempenho relativo de um Estado no provimento de ordem pública e na defesa nacional constitui o elemento mínimo a partir do qual se pode julgar suas pretensões de obter lealdade e obediência por parte dos cidadãos.

Entretanto, os fatores que determinam se a vida das pessoas será ou não *“solitária, pobre, sordida, embrutecida e curta”* são muito mais complexos e diversificados do que a condição necessária, porém insuficiente, de segurança decorrente do cumprimento eficaz das tarefas “hobbesianas” de provimento de ordem pública e de defesa nacional. O mecanismo de reciprocidade entre proteção estatal e consentimento dos indivíduos se mantém no mundo contemporâneo, embora os recursos de poder, as demandas, opiniões e direitos dos cidadãos também sejam muito mais complexos e diversificados do que eram os dos súditos.<sup>13</sup>

No mínimo, isso significa que os meios e os métodos através dos quais o Estado garante as condições elementares de segurança são relevantes para a segurança individual e coletiva (“nacional”) dos habitantes de uma unidade política qualquer. Ou seja, o mesmo Estado que obtém legitimidade do fato de ser o principal responsável pela segurança nacional, freqüentemente torna-se ele próprio uma fonte de ameaça mais ou menos direta para a segurança dos indivíduos, de grupos e da própria nação.<sup>14</sup>

Ameaça direta quando o governo mobiliza os meios de força sob seu controle contra alvos individuais ou grupos que fazem parte da população que supostamente deveria estar sendo protegida, os quais não infringiram nenhuma lei ou ameaçaram violentamente a ordem pública. A aplicação intensa de coerção fez parte da trajetória típica da construção estatal moderna na maioria dos países e, ainda hoje, quando os interesses do Estado se chocam com os de algum grupo ou indivíduo, os governantes e suas burocracias têm recursos de poder para tentar impor, mais ou menos coercitiva-

mente, sua vontade em nome da ordem pública, da moralidade ou da segurança nacional.<sup>15</sup>

Além da violência direta em escalas variadas (da prisão ilegal, tortura e assassinato de dissidentes do regime até o genocídio de vastos contingentes populacionais), o Estado também ameaça a segurança dos indivíduos sempre que o sistema de justiça criminal e o policiamento são ineficientes ou arbitrários, e crimes contra a vida e o patrimônio das pessoas podem ser cometidos impunemente, ou quando os governantes implementam políticas externas e de defesa que aumentam enormemente o divórcio entre a segurança individual e a segurança do Estado (por exemplo, no caso da dissuasão nuclear baseada na destruição mútua assegurada, em que parte da população é entregue como refém para estabilizar a interação estratégica). De forma mais indireta ainda, a luta entre diferentes grupos pelo controle dos recursos estatais que permitem governar uma população e um território (guerra civil, revolução ou qualquer outro tipo de “soberania múltipla”) ameaça a segurança de indivíduos e setores da população que não estão diretamente envolvidos no confronto.<sup>16</sup>

Essa tensão entre segurança individual e segurança estatal é um traço imanente da ordem política moderna e manifesta-se com maior ou menor intensidade dependendo da natureza do regime político e da inserção conjuntural de cada país no sistema internacional. Quando são levadas em conta as diferenças entre os Estados (tamanho da população e do território, diferentes ideologias justificadoras, instituições de governo e graus de desempenho em relação aos atributos da soberania), a tradução prática da noção de segurança nacional torna-se potencialmente tão diversa quanto a diversidade dos Estados existentes e suas respectivas relações com suas populações e com os outros Estados.

No caso dos países cujas instituições de governo são as da democracia representativa e a ideologia justificadora da Constituição é liberal e democrática (poliarquias), embora seja razoável esperar que a tensão entre segurança individual e segurança estatal seja menor do que nas ditaduras, permanece como um problema empírico analisar suas manifestações específicas.<sup>17</sup>

Constatando essa dupla face do Estado, protetora e ameaçadora da vida e da liberdade individual a um só tempo, Lustgarten e Leigh (1994:8-10) tentam religar o conceito de segurança nacional com a democracia propondo que se considere a proteção dos direitos humanos como uma dimensão central da própria segurança estatal. Afinal, as ações tomadas pelas instituições governamentais para tentar garantir a segurança nacional precisam levar em conta a natureza mesma das instituições que se pretende proteger e de suas bases de legitimização. É comum que atos governamentais tomados em nome da segurança nacional sejam considerados válidos ou não em si

mesmos, embora gerem preocupações secundárias por suas implicações para a democracia e os direitos humanos.

Porém, dizem Lustgarten e Leigh, ao invés de um jogo de soma zero no qual os ganhos de segurança estatal impliquem perdas de segurança individual e vice-versa, essa contradição poderia ser resolvida se as instituições evitassem medidas de segurança que limitam ou sacrificam liberdades civis e políticas, considerando que elas atingem não apenas os indivíduos e grupos que são os alvos diretos dessas medidas, mas trazem também perdas para as liberdades de todos e afetam negativamente a segurança nacional na medida em que enfraquecem as bases da legitimidade de um Estado fundamentado em instituições democráticas representativas e valores correspondentes.

Isso não quer dizer que as democracias não sejam capazes, não devam ou jamais tenham adotado medidas de segurança que acarretam limitações a certos direitos civis e políticos individuais, tais como o direito de reunião, a garantia de inviolabilidade de correspondências e comunicações, o direito de viajar e movimentar-se livremente em áreas públicas, o direito à informação governamental, a liberdade de imprensa, a inviolabilidade doméstica contra buscas e apreensões sem mandato judicial etc. Mas, para pretender obter o consentimento do público para essas medidas repressivas o governo que as propõe e implementa, alegando ameaças à segurança nacional, precisaria justificá-las em termos da gravidade real e da proximidade da ameaça, da eficácia das medidas propostas para neutralizar a ameaça percebida, do número de pessoas e interesses atingidos pelas medidas repressivas e da razão por que a operação regular dos meios estatais de coerção não é suficiente.<sup>18</sup>

Tipicamente, nas democracias tais medidas deveriam ser consideradas apenas excepcionalmente (vide os institutos do estado de defesa e do estado de sítio no caso da Constituição brasileira<sup>19</sup>), deveriam ser temporárias, não poderiam implicar qualquer autorização para a violação do direito à vida e à integridade física dos atingidos, precisariam ser autorizadas pelo Poder Legislativo nacional e as responsabilidades legais das autoridades envolvidas não seriam suspensas durante sua vigência.<sup>20</sup>

Embora o ponto dos dois autores britânicos seja consistente com os fundamentos liberais do direito positivo, encontrando ainda uma razoável tradução na prática política das poliarquias institucionalizadas, sua tentativa de solucionar o *trade-off* entre segurança individual e segurança estatal a partir da proposição normativa de se “pesar” os direitos humanos nos dois lados da balança encontra sérios obstáculos.

Primeiro, porque mesmo nos casos excepcionais previstos pelas constituições democráticas o dispositivo constitucional sobre as medidas de segurança não faz mais do que fixar alguns parâmetros bastante genéricos e frouxos para o processamento de uma disputa essencialmente política sobre a

gravidade das ameaças, sobre a gravidade das medidas propostas e sobre o exercício efetivo de coerção. Ou seja, a tensão entre segurança estatal e individual se mantém – pois está baseada numa contradição inerente ao exercício da autoridade num mundo complexo e burocratizado –, e sua natureza política impede que a mera proposição normativa da subsunção das medidas de segurança à proteção aos direitos humanos possa resolvê-la.<sup>21</sup>

Segundo, a relação entre segurança estatal e democracia não é direta, especialmente no caso da capacidade de neutralizar ameaças externas. No longo prazo, e em termos muito agregados, o desenvolvimento econômico e a democracia – que em grande parte decorre da ultrapassagem de certo limiar de desenvolvimento econômico – têm impactos positivos sobre a capacidade defensiva de um país. Mesmo assim, é importante destacar que o binômio desenvolvimento e segurança, característico dos regimes autoritários na América Latina nas décadas de 1960 e 1970, implicava, na verdade, a construção de “capacidades” nacionais e desempenhos específicos em duas áreas muito diferenciadas e nem sempre intercambiáveis. Os ganhos em desenvolvimento não se traduzem automaticamente em ganhos de capacidade defensiva e segurança, como se isso pudesse ocorrer independentemente das escolhas políticas concretamente encaminhadas pelos governantes no que diz respeito às políticas externa e de defesa.<sup>22</sup>

Da mesma forma, a natureza democrática ou não de um regime político não resolve por si mesma todos os problemas associados à segurança estatal. Basta dizer que a afirmação segundo a qual o Canadá não é apenas diferente da China, mas muito mais democrático do que ela, não equivale à afirmação, bem mais disputável, de que o Estado canadense considerado isoladamente é mais capaz do que o Estado chinês para respaldar seus valores e interesses ou para neutralizar ameaças vitais através do uso de meios de força.<sup>23</sup>

Nesse sentido, a posição de Barry Buzan sobre a irredutibilidade da segurança estatal à segurança individual e vice-versa é mais realista que a posição de Laurence Lustgarten e Ian Leigh. Isso pode ser observado mesmo considerando-se o lado inverso da questão, sobre como a diminuição relativa da capacidade defensiva externa de um Estado não se traduz automaticamente em perda de autoridade do Estado em relação aos cidadãos. Segundo Buzan (1991:51), dificilmente o declínio na capacidade defensiva de um Estado no sistema internacional – por exemplo, decorrente do advento das armas nucleares e do bombardeio estratégico – faz declinar igualmente a autoridade do Estado sobre seus cidadãos. Infelizmente, o contrário também é verdadeiro, pois dificilmente variações nos níveis de segurança individual dos membros de uma população chegam a comprometer por si mesmos a estabilidade e a capacidade defensiva do Estado como um todo.<sup>24</sup>

Em resumo, a abordagem liberal do conceito de segurança nacional tende a afirmar precipitadamente que os Estados são inseguros porque – e

apenas na medida em que – suas instituições governamentais são autoritárias ou quando Estados autocráticos ameaçam Estados democráticos. Por sua vez, os autores que recorrem à noção de segurança humana (*human security*) tendem a sustentar equivocadamente que os Estados são inseguros porque – e apenas na medida em que – suas populações são pobres e excluídas ou quando Estados ricos ameaçam Estados pobres.

Formulado em sua máxima abrangência no Relatório sobre o desenvolvimento humano do Programa das Nações Unidas para o Desenvolvimento (Pnud) publicado em 1994, o conceito de segurança humana procurou articular uma série de tentativas anteriores de alargar e substituir a noção de segurança nacional vigente durante a Guerra Fria. Desde os anos 1970 e 1980, muitos autores e comissões internacionais vinham falando dos problemas associados à segurança social, à segurança ambiental, à segurança global (ameaça de holocausto nuclear), à segurança alimentar e à segurança individual (fosse ela ameaçada pela doença, pelo crime ou pela repressão estatal). Com o final da Guerra Fria e a intensificação dos debates sobre desenvolvimento sustentável no começo da década de 1990, a inclusão de novos temas na agenda de segurança foi reivindicada a partir desse conceito sintético de segurança humana. Em relação à noção anterior de segurança nacional, o novo conceito teria algumas diferenças fundamentais, segundo seus proponentes.

Do ponto de vista dos “objetos” da segurança, há uma postulação explícita para que se abandone o Estado como o referente empírico mais importante para a consideração de problemas de segurança, colocando em seu lugar as demandas de segurança dos indivíduos, dos grupos sociais destituídos (minorias étnicas, pobres, outros segmentos excluídos na população), da humanidade como um todo e até mesmo da biosfera.

A própria definição do que seriam os problemas “reais” de segurança deveria deslocar-se, segundo a abordagem da *human security*, da capacidade de neutralizar ameaças de tipo predominantemente militar para a neutralização das ameaças à vida humana que são resultantes da degradação ambiental, da instabilidade econômica e da desintegração de laços sociais. Modificando-se a percepção do que seriam as ameaças “reais” à segurança das pessoas, os instrumentos e instituições capazes de prover segurança também deixariam de depender principalmente dos meios de força controlados pelos Estados soberanos de base territorial e suas alianças militares tradicionais, tais como a organização do Pacto de Varsóvia e a Organização do Tratado do Atlântico Norte (Otan). Na nova abordagem, principalmente em função do novo perfil das ameaças percebidas, seriam centrais as agências especializadas do sistema das Nações Unidas (ONU), bem como outras organizações integradoras multiestatais ou multinacionais, além das organizações não-governamentais (ONGs) operando em bases transnacionais ou subnacionais.<sup>25</sup>

Segundo a síntese de Jean Daudelin (1999:17), os componentes centrais dessa redefinição do conceito de segurança seriam a individualização, a desmilitarização, a globalização e a democratização dos problemas e soluções de segurança humana.<sup>26</sup>

Nesse caso, as objeções que tenho dizem respeito à produtividade analítica do conceito de segurança humana *vis-à-vis* o conceito de segurança nacional, mas também à própria validade da prescrição subjacente a essa mudança de ênfase. As objeções analíticas dirigem-se para a perda de coerência intelectual de um programa de pesquisas que pretendesse partir da noção de que existem “problemas de segurança sempre que a vida dos indivíduos estiver ameaçada”, o que ocorreria na proporção direta em que tudo aquilo que de alguma forma determina se a vida dos indivíduos será ou não “*solitária, pobre, sórdida, embrutecida e curta*” fosse transformado em objeto da alçada dos estudos e políticas de segurança.

Em artigo sobre o renascimento dos estudos de segurança publicado há alguns anos, Stephen Walt (1991:213) já havia alertado que a inclusão de tópicos como fome, Aids, poluição, abuso infantil ou recessão econômica no âmbito do programa de pesquisas sobre “segurança” serviria apenas para dificultar a investigação especializada desses importantes problemas e não acrescentaria nada ao necessário estudo dos problemas específicos relacionados ao uso da força na dinâmica política das relações interestatais, subnacionais e transnacionais.

Certos temas de relações internacionais, não diretamente ligados à dinâmica do combate ou aos aspectos logísticos e estratégicos, tais como a economia da proliferação de armamentos – desde minas antipessoais e armas ligeiras até armas químicas, biológicas e nucleares (WMD) – ou a aplicação de justiça em casos de crimes contra a humanidade, são claramente uma parte integrante dos estudos estratégicos. De modo geral, temas econômicos, médicos ou ambientais tendem a fazer parte da agenda de pesquisa dos estudos estratégicos quando estão relacionados, ainda que indiretamente, ao uso da força. Mas é preciso ter claro que o estudo da segurança, na medida em que se afasta dos estudos estratégicos, tende a disputar agendas de pesquisa e a tentar mesmo substituir a disciplina de relações internacionais como um todo. De qualquer modo, a função primária do conceito de *human security* tem sido menos a de estruturar um programa de pesquisas e mais a de orientar a política externa de alguns países, organizações não-governamentais e agências multilaterais.<sup>27</sup>

Mesmo como opinião no debate político (*policy advocacy*), a abordagem da segurança humana enfrenta problemas de legitimação e dilemas morais semelhantes aos já enfrentados pelo conceito de segurança nacional. Em primeiro lugar, ela assume acriticamente que segurança é sempre uma

boa coisa, um estado desejável para quaisquer relacionamentos. Em segundo lugar, a ampliação excessiva do conceito de segurança permite que novas regras estabelecidas no âmbito de organizações intergovernamentais (ONU, Otan etc.), em que predominam os interesses dos países-membros mais poderosos, autorizem uma intervenção dos países mais poderosos nos países mais fracos por uma variedade crescente de motivos.

Ora, ainda que, em geral, a segurança seja um estado melhor do que a insegurança (quando não há contramedidas eficazes disponíveis contra as ameaças vitais), não se deve perder de vista que o que se chama de segurança no sistema de relações interestatais é um tipo de estabilização relativamente precária de relações conflitivas e ameaçadoras. No caso das relações interestatais, essa estabilização só é obtida à custa da mobilização de recursos coercitivos e medidas excepcionais que aumentam as tensões entre segurança individual e segurança estatal. Ao reivindicar a “securitização” de temas como o combate à pobreza, o controle epidemiológico de doenças, a melhoria da educação e a luta contra a degradação ambiental, a abordagem da *human security* pretende trazer esses temas para o centro da agenda, obtendo o mesmo tipo de prioridade e tratamento especial dos temas tradicionais de segurança, especialmente a defesa militar externa e o provimento de ordem pública dentro dos países. Mas os riscos associados a esse procedimento parecem não despertar preocupação nos primeiros formuladores dessa abordagem.

Um exemplo contemporâneo dos problemas advindos da securitização indiscriminada de quaisquer temas socialmente relevantes seria o caso da espionagem econômica, que ainda encontra dificuldades para se justificar nos países democráticos em função do imperativo da separação entre interesses públicos e privados, mas que poderia legitimar-se com base no conceito de *human security*, aprofundando a securitização do desempenho econômico num mundo crescentemente interdependente e competitivo. Portanto, ignorar que a “securitização” de temas como a preservação ambiental e a competitividade econômica traz consigo os riscos de utilização desproporcional de medidas repressivas e de limitações das liberdades individuais é por demais ingênuo ou politicamente interessado, principalmente considerando-se as diversas racionalizações do uso de mecanismos repressivos por diversos tipos de regimes políticos ao longo do último século.<sup>28</sup>

Na verdade, se se trata de ter algum horizonte normativo em torno desse tipo de problema, este deveria ser algo mais próximo da *desecuritization* mencionada por Ole Wæver (1998), um deslocamento dos problemas relevantes para fora do “modo de emergência e exceção” associado às medidas de segurança e para dentro do processo considerado normal de argumentação e disputa política democrática.

A melhor forma para evitar o terreno minado da definição *a priori* e arbitrária do que seriam as “reais” ameaças contra a segurança dos indivíduos e

Estados seria analisar os próprios processos políticos de securitização de certos temas e problemas. Nos termos propostos por Buzan, Wæver e Wilde (1998: 21-47), isso significaria compreender como interagem em cada caso concreto três pólos do processo: os objetos referentes (que são vistos como ameaçados em sua existência e/ou autonomia e reivindicam seu direito à sobrevivência), os atores securitizadores (os quais declararam que um objeto referente está sendo ameaçado e requisitam contramedidas) e os atores funcionais (que legitimam ou não a percepção de ameaça e as contramedidas de segurança requisitadas).<sup>29</sup>

O mesmo esquema analítico permite diferenciar processos *ad hoc* de securitização e processos relativamente institucionalizados de securitização. Se um dado tipo de ameaça é persistente, recorrente ou emergencial, a escolha de respostas políticas adequadas e a definição de prioridades e graus de urgência podem ser institucionalizadas através de procedimentos tipificados e agências governamentais especializadas.

Assim, por exemplo, riscos potenciais de ameaças militares externas em ambientes internacionais cambiantes, bem como a avaliação sobre o grau adequado de preparação para a eventual necessidade de sustentação externa dos interesses e valores governamentais através da força, justificam e explicam a centralidade das Forças Armadas em qualquer arranjo nacional defensivo. Embora os diversos componentes e os diferentes aspectos de uma política de defesa devam estar em constante debate e reavaliação nas democracias, refletindo a instrumentalidade das Forças Armadas em relação à política, a dinâmica temporal e de recursos envolvida nas decisões sobre defesa implica a superioridade relativa dos procedimentos institucionalizados de deliberação e gestão governamental dos assuntos de defesa e segurança. Em outras palavras, não se constroem Forças Armadas após a identificação de uma ameaça iminente à segurança nacional.

Porém, de modo algum tal institucionalização deveria significar que o processo político possa ser substituído por decisões meramente “técnicas” relativas às possibilidades de emprego da força em situações concretas. Como já destacava Barry Buzan (1991:140), a ambigüidade e a complexidade da maioria das ameaças tornam inherentemente difícil manter a proporcionalidade das respostas governamentais, o que repõe constantemente a segurança como um problema político. Ao invés de compor um “pacote de legitimação” que resolveria de uma vez por todas questões de prioridade e recursos, é justamente o risco de constituição de “caixas-pretas” de segurança no processo político (*black security boxes*) que torna importantes os procedimentos institucionalizados de securitização.<sup>30</sup>

Prescritivamente, Lustgarten e Leigh (1994:23-26) sustentam a necessidade de se reaprender a linguagem mais clara e precisa da defesa nacional, abandonando a vaguezza da “segurança nacional” e sua tendência a hipertrofiar as

“ameaças” em função dos interesses setoriais das burocracias especializadas em garantir a segurança estatal. Isso é certamente necessário e compatível com o esforço feito aqui de desmitificação do conceito de segurança nacional. Porém, mesmo sem se falar em segurança nacional restaria a tarefa de situar criticamente o papel das organizações de força e de inteligência na confluência das políticas públicas de defesa externa, provimento de ordem pública e afirmação diplomática dos interesses e opiniões governamentais no plano internacional.

Por isso – e também pela disseminação do uso desse conceito no debate público internacional – foi preferível destacar aqui as contradições internas insanáveis da noção de segurança, reconhecendo que por segurança nacional quase sempre se está falando, na verdade, de segurança estatal e, ainda assim, tentar mostrar por que essa segurança nacional ou estatal não pode ser reduzida ao bem-estar dos indivíduos que compõem qualquer uma dessas coletividades a que chamamos de países.

Saber quando uma ameaça vital efetivamente se torna uma questão de segurança nacional depende não apenas do tipo de ameaça (militar, econômica etc.), mas também da percepção que os atores políticos têm dela e da intensidade e da extensão das consequências estimadas. Conhecer essas dinâmicas e informar os resultados das análises de forma ágil para os governantes e comandantes militares é a função primordial dos serviços de inteligência. Em síntese, outras coisas sendo iguais, quanto mais intensa for uma ameaça e quanto mais universais forem as consequências para os membros de uma dada unidade política, maior tende a ser a legitimidade das medidas de segurança adotadas pelo governo.

Esse é um bom critério, mas o problema é que ameaças costumam envolver grande complexidade de fatores causais, diversidade de fontes ou outras ambigüidades.<sup>31</sup> Como diz Barry Buzan (1991:142), mesmo que as informações fossem perfeitas – ilimitadas e não-distorcidas – a complexidade inerente das ameaças e das consequências das respostas escolhidas desafiaria a capacidade de discernimento dos atores. Desafio ainda maior no caso de interações conflitivas, nas quais não apenas as informações disponíveis são escassas, mas as assimetrias e negações mútuas de informação (*denial and deception*) são uma componente fundamental da própria interação. Tudo isso torna difícil a deliberação política sobre medidas de segurança e os processos de justificação dessas práticas por parte dos atores “securitizadores”.

É justamente para reduzir a incerteza e aumentar a capacidade de preservar a segurança nacional que existem as Forças Armadas, polícias e serviços de inteligência. Tais organizações são parte do necessário esforço governamental para a solução de problemas de segurança, mas, na medida em que a própria busca de segurança é problemática, tais organizações de força e inteligência são também parte do problema.

Na sua dupla função, informacional e coercitiva, os serviços de inteligência têm seus traços definidos pelos dilemas e desafios de segurança nacional discutidos até aqui. Um aspecto particularmente significativo desses dilemas manifesta-se na questão do segredo governamental, tema da próxima seção.

## Segredo governamental

De acordo com a conhecida definição do sociólogo Edward Shils (1996:26), um segredo é uma retenção compulsória de conhecimento, reforçada pela perspectiva de punição em caso de revelação. Essa definição apenas em parte é equivalente a outras definições correntes na literatura especializada, tais como a de Sissela Bok (1989), que afirma ser um segredo qualquer coisa mantida intencionalmente escondida.<sup>32</sup>

Enfatizando esse aspecto intencional do segredo como uma propriedade da informação que é escondida do conhecimento de outrem, Kim Lane Scheppele utiliza uma formulação bastante concisa e abrangente: “*A secret is a piece of information that is intentionally withheld by one or more social actor(s) from one or more other social actor(s)*”.<sup>33</sup> O problema da definição de Scheppele (que é basicamente a mesma de Bok) é que ela é abrangente demais para os propósitos da discussão a ser feita sobre inteligência e segredo. Scheppele reconhece que a retenção intencional de informações na relação entre dois ou mais atores sociais varia segundo os contextos da interação, mas sua definição não nos permite diferenciar segredos privados de segredos públicos.

A abordagem de Shils é preferível, pois ela mantém a idéia de intencionalidade e acrescenta um elemento regulador externo para a retenção da informação: a punição legalmente estatuída no caso de revelação. O segredo público é assim distinto de uma informação qualquer que é mantida privadamente em segredo, a qual não passa de uma retenção voluntária de conhecimento reforçada pela indiferença alheia.<sup>34</sup>

Nesse sentido um tanto paradoxal, segredos são uma forma de regulação pública de fluxos de informação. Há pelo menos cinco categorias de informações reguladas pelo sigilo de tipo público: defesa nacional; política externa; processos judiciais; propriedade intelectual e patentes; privacidade dos cidadãos. A justificação pública para a necessidade de sigilo varia muito em cada categoria.<sup>35</sup> Das cinco categorias, as duas primeiras contêm a maioria das informações mantidas em segredo com base em considerações de segurança nacional. Esse é o tipo de segredo público de que se ocupará esta seção. Vale notar que a justificação do segredo baseada no risco potencial para a segurança nacional não é facultada aos atores privados, mas apenas ao Estado e seus representantes e, mesmo assim, em situações especiais.

Os segredos governamentais são compatíveis com o princípio de transparência dos atos governamentais somente quando a justificação de sua ne-

cessidade pode ser feita, ela própria, em público. Isso é o que David Luban (1996:154-198) chama de máximas de primeira ordem e de máximas de segunda ordem relativas ao princípio da transparência. Uma defesa não-apriorística desse princípio envolve admitir o segredo governamental a respeito de normas, procedimentos e políticas (máximas de primeira ordem) desde que as razões para a regulação secreta dessas informações (máximas de segunda ordem) possam ser expostas e justificadas publicamente.<sup>36</sup>

Nada impede, entretanto, que máximas de terceira ou quarta ordem sejam adotadas por governos ou serviços de inteligência para justificar (freqüentemente de forma apodíctica) uma decisão de manter em segredo as próprias razões pelas quais eles mantêm em segredo certas políticas.<sup>37</sup> Ou seja, assim como no caso da segurança nacional, não há antídotos definitivos contra o abuso do recurso ao segredo governamental. No limite, é preciso admitir que esse é um tipo de regulação poderosa que se baseia em confiança (*trust*). Entretanto, justamente porque o uso excessivo de máximas de terceira ordem conduz à deslegitimização e ao cinismo em relação às próprias instituições que se pretende proteger através do segredo, um regime democrático precisa tentar traduzir o princípio moral da transparência em proposições de desenho institucional.

Ao cabo, o segredo governamental pode ser compatível com o princípio de transparência somente quando decisões sobre a aplicação desse tipo de regulação a determinados fluxos informacionais são tomadas através de mecanismos institucionais publicamente estabelecidos no contexto de regras do jogo democráticas.

Nas áreas de atuação governamental relacionadas com a defesa nacional e a política externa, a principal justificativa para a restrição da circulação de informações produzidas ou mantidas pelo governo é o dano potencial que sua apropriação por uma terceira parte (ex.: um governo estrangeiro) poderia causar para a segurança estatal e, por decorrência, para a segurança individual dos membros da coletividade. Por exemplo, sistemas de armas, planos de contingência e mobilização, pesquisa científica e tecnológica de aplicação militar, intenções em negociações de acordos internacionais, desempenho de capacidades defensivas e outras coisas semelhantes, uma vez conhecidas por um adversário ou inimigo, aumentam nossas vulnerabilidades e fornecem uma vantagem comparativa crucial para os adversários nas interações conflitivas.

Além de ser necessário por questões puramente defensivas, o segredo muitas vezes também é decisivo para que os governos possam planejar, implementar e concluir missões militares e diplomáticas. Um exemplo óbvio do papel crucial do segredo é a tentativa de obtenção de surpresa em ataques militares, mas também se pode argumentar na mesma direção em

relação ao sucesso de negociações diplomáticas sensíveis (por exemplo, as negociações secretas entre China e Estados Unidos que precederam a visita de Nixon a Pequim em 1972, ou as negociações secretas entre representantes palestinos e israelenses que precederam os chamados Acordos de Oslo em 1993). Nesses casos, a justificação do segredo baseia-se mais na necessidade de impedir que os objetivos governamentais sejam frustrados pela publicização precoce da informação do que nos danos potenciais à segurança nacional.

A necessidade de sigilo também é reivindicada em processos de deliberação intragovernamental sobre os temas domésticos considerados relevantes para a segurança nacional (energia, transportes, policiamento etc.), processos decisórios durante os quais a revelação prematura das divergências de opinião dentro do governo poderia ser danosa para a segurança das operações e para a possibilidade de sucesso de qualquer das metas e planos eventualmente escolhidos. Nesses casos, a aplicação de restrições de sigilo é muito mais problemática em termos legais e, principalmente, políticos. O risco envolvido, do ponto de vista da democracia, é que o recurso ao sigilo impeça a necessária transparência dos atos governamentais, tanto pela impossibilidade de verificação de responsabilidades individuais na história administrativa das decisões, quanto pela restrição pura e simples dos direitos políticos dos cidadãos.<sup>38</sup>

Uma última justificativa genérica para o segredo estatal é a necessidade de proteger as identidades e relacionamentos confidenciais de agências governamentais com certos indivíduos, grupos e governos. A necessidade de sigilo nesses relacionamentos emerge de uma variedade de contextos e toma formas diversas, embora o caso mais evidente seja justamente o da proteção de fontes e métodos na área de inteligência. Além do risco de vida para os próprios indivíduos e suas famílias, a exposição (“*blow*”) desse tipo de relacionamento através do fracasso de uma das partes em manter segredo tem efeitos em cadeia sobre a disposição de cooperação futura, o que é considerado prejudicial para a segurança nacional e para a perspectiva de viabilização dos interesses e políticas governamentais na arena internacional.

Para além da justificação pública sobre sua necessidade prática e validade moral, os segredos de Estado não se manteriam secretos se contassem apenas com a discrição dos indivíduos que partilham a informação sigilosa ou com a indiferença alheia. A proteção dos segredos de Estado depende de três processos complementares: 1. procedimentos de classificação; 2. controles de acesso; e 3. punições em caso de revelação não autorizada.

No primeiro caso, autoridades legalmente competentes identificam conjuntos informacionais sensíveis para a segurança nacional e aplicam regras de classificação que definem o grau de sigilo necessário e a intensidade das medidas de restrição física de acesso para cada informação.

As classificações de segurança são feitas através da atribuição de marcadores externos que definem a importância de cada informação para a segurança nacional (tipicamente, são utilizadas as categorias de confidencial, secreto e ultra-secreto).<sup>39</sup> A atribuição de um marcador específico para um documento ou conjunto informacional é feita – em tese – por um funcionário ou órgão legalmente autorizado. No caso de informações consideradas extremamente vitais para a segurança nacional, por exemplo, a atribuição da categoria de ultra-secreto só pode ser feita pela autoridade mais alta do país ou por sua expressa delegação.<sup>40</sup> As categorias de sigilo também prevêem tempos de duração para a restrição de acesso correspondentes ao grau de sigilo atribuído, ou seja, quanto mais secreta uma informação maior o tempo que transcorrerá até sua completa publicização.

No segundo bloco de medidas (controles de acesso), as medidas de restrição física de acesso a essas informações implicam sistemas de vigilância, manejo, armazenamento e transmissão, não importa em que mídia específica as informações estejam. A disciplina de segurança de sistemas de informações (infosec) preocupa-se não apenas com a criptografia das mensagens e dos acervos informacionais, mas cada vez mais com a redução das vulnerabilidades sistêmicas das redes de produção, armazenamento e comunicação de informações. No caso, trata-se de evitar que as informações sigilosas de categorias diversas sejam interceptadas por usuários não-autorizados (espionagem) ou que possam ser alteradas ou destruídas (sabotagem).<sup>41</sup>

Garantias adicionais de preservação dos segredos governamentais são obtidas através de sistemas de veto de acesso para pessoas não-autorizadas, bem como através de restrições adicionais de circulação das informações sigilosas através da aplicação do princípio conhecido como “necessidade de conhecer” (*need-to-know*).

Sistemas de veto envolvem a aplicação de procedimentos de checagem de segurança para todas as pessoas que se candidatam a um emprego em agências governamentais na área de defesa, inteligência e segurança. Nas áreas consideradas críticas para a segurança nacional, controles de segurança são aplicados tanto para funcionários civis e militares quanto para empregados de empresas privadas que mantenham contratos com agências governamentais. No caso das agências de inteligência, além das checagens padronizadas sobre antecedentes criminais e fichas de crédito e saúde, são realizadas entrevistas mais detalhadas com parentes, vizinhos e conhecidos sobre o passado individual, além da aplicação de testes especiais com “detectores de mentiras” (*polygraph tests*).

Depois de passar satisfatoriamente pelos sistemas de veto e investigação, para ter acesso às informações classificadas (sigilosas) os ocupantes de cargos públicos precisam obter credenciais correspondentes à classe da informação (reservada, confidencial, secreta e ultra-secreta). Em geral, o nível de acesso depende do grau de senioridade do funcionário e/ou da importâ-

cia do cargo ocupado. Vale observar que, uma vez concedida a credencial de acesso, a mesma não acompanha o funcionário ou a autoridade eleita independentemente dos cargos que ele ocupar ou do período transcorrido. Checagens de segurança periódicas são, ao menos em tese, necessárias para a renovação das credenciais de acesso.<sup>42</sup>

Porém, por mais drásticos que sejam os procedimentos de segurança para a concessão de credenciais, o acesso aos segredos governamentais depende ainda da aplicação do princípio de segmentação das informações mais sensíveis (“*need-to-know*”). Basicamente, esse princípio diz que cada documento ou conjunto informacional pode ser acessado apenas pelos funcionários que efetivamente precisam ficar sabendo do seu conteúdo, e não por qualquer um que possua uma credencial de acesso com nível de classificação compatível. Isso gera novos marcadores externos e restrições adicionais para o acesso aos segredos governamentais. No caso do sistema de classificação dos Estados Unidos, por exemplo, além das três categorias ascendentes de segurança (*confidential*, *secret* e *top secret*), são utilizados cerca de 50 marcadores adicionais que, embora não tenham o mesmo estatuto legal, muitas vezes estabelecem regulação mais intensa do que o sistema formal. Programas, informações e documentos com acesso especial (SCI – *special compartmented information*) podem ser estabelecidos com base no princípio da “necessidade de conhecer”.<sup>43</sup>

No terceiro bloco de medidas, se falham os procedimentos de segurança, entram em cena os elementos dissuasórios que diferenciam a definição de segredo público de Edward Shils: sanções administrativas e penalidades legais. Nesse caso, é importante diferenciar a obtenção de segredos através da espionagem do mero vazamento de informações sigilosas para o público.

Segundo Lustgarten e Leigh (1994:221-248), por se tratar de uma ação discreta e/ou furtiva, a espionagem bem-sucedida abre uma cunha na segurança de informações que o governo demora a perceber ou sequer toma consciência. Um espião operando em favor de um governo estrangeiro, independentemente de suas motivações (ideologia, dinheiro, chantagem, vingança etc.), não pode alegar o bem comum da nação que ele está espionando e tampouco da humanidade como um todo para justificar sua ação. Quer se trate de um agente recrutado (cidadão ou residente permanente) ou de seu controlador estrangeiro (que pode ter cobertura diplomática ou não), o ato de espionar é uma ação que altera a distribuição de poder internacional e trai a confiança horizontal na qual se baseia a própria cidadania. Em um mundo de Estados que precisam se defender, a espionagem é uma conduta criminalizada na maioria dos ordenamentos legais.

Nos Estados Unidos, por exemplo, dependendo da gravidade do caso, a espionagem pode ser punida pelo júri com a prisão perpétua ou mesmo com

a pena de morte.<sup>44</sup> Mesmo que muitos espiões não cheguem sequer a ser processados, o que ocorre inclusive por questões intrínsecas à própria lógica das operações de contra-inteligência, o ponto a ser destacado é que a gravidade com que a espionagem é encarada contrasta com a relativa banalização dos vazamentos de informações sigilosas nas democracias.<sup>45</sup>

A causa desse fenômeno reside no entendimento da jurisprudência de que a divulgação não-autorizada de informações sigilosas causa relativamente menos dano do que a espionagem, porque a própria publicização da informação alerta imediatamente o governo e desencadeia contramedidas e tentativas de controle de danos. Também pode ser que a divulgação não-autorizada de informações sigilosas tenha sido acidental, ou que tenha sido intencionalmente motivada pela decisão de expor alguma corrupção, arbítrio ou incompetência governamental que vinha sendo ocultada através das regras formais do segredo público. Nesses casos, mesmo que a motivação do agente que torna pública a informação faça diferença para a avaliação de sua credibilidade, os danos para a segurança nacional devem ser contrastados com o eventual benefício público resultante da transgressão. Obviamente, isso é sempre controverso, e as tentativas de regulação legal do fenômeno esbarram em sua complexidade política.<sup>46</sup>

Na maioria dos casos que aparecem corriqueiramente na mídia, na verdade o vazamento de informações sigilosas (*leakage*) é um recurso de poder utilizado por membros do próprio governo para lançar balões-de-ensaio sobre políticas e projetos, para torpedear uma política da qual discordam ou meramente para avançar seus próprios interesses na disputa interburocrática. Nos Estados Unidos, o vazamento de informações sigilosas é penalizado com medidas administrativas (desde a censura até a perda do cargo ou emprego), multas em dinheiro e até 10 anos de prisão.<sup>47</sup> Porém, naquele país a relativa impunidade dos vazamentos de informações sigilosas por membros do alto escalão do governo central tende a gerar, por um lado, descrédito público para a necessidade de operar sistemas de classificação e, por outro, uma reação defensiva da parte dos órgãos de segurança que pode ser descrita como hiperclassificação. Aliás, pode-se dizer que falhas em qualquer um dos três processos descritos nos parágrafos anteriores tendem a gerar uma expansão excessiva nos outros dois, como uma espécie de “compensação” perversa.

Seja como for, o segredo governamental é uma forma de regulação de fluxos de informação bastante utilizada no Estado contemporâneo. Como em quase tudo na área de estudos de inteligência, os dados empíricos disponíveis referem-se ao caso dos Estados Unidos, de confiabilidade não testada e sabidamente de difícil comparação em função da escala. No relatório final da comissão criada pelo Congresso para analisar a “Proteção e Redução do

Segredo Governamental” (1997), consta que apenas os documentos classificados com mais de 25 anos somavam naquele ano mais de 1,5 bilhão de páginas. O montante total de documentos classificados não é conhecido. Estima-se que num único ano (1992) o governo dos Estados Unidos tenha gerado 6,2 milhões de páginas de documentos classificados como sigilosos.<sup>48</sup> Cerca de 99% das classificações originais são feitas em cinco órgãos do governo federal (53% no Departamento de Defesa, 30% na CIA, 10% no Departamento de Justiça, 3% no Departamento de Estado e 3% no Departamento de Energia). É muito claro o peso dos órgãos de inteligência na formação do sistema de segredo governamental dos Estados Unidos, o que pode ser extrapolado para os demais Estados contemporâneos como hipótese de trabalho.

Como lembra Michael Herman (1996), a relação entre segredo e inteligência começa pelo fato de as operações de coleta de informações em inteligência visarem justamente a obtenção de informações que não podem ser obtidas (ou são de difícil acesso) através de meios corriqueiros de pesquisa. Para dizer isso nos termos mais enfáticos e algo exagerados de Kenneth Robertson (1987), a atividade de inteligência consiste antes de mais nada na tentativa de descobrir os segredos de outros através da utilização de meios secretos. Na verdade, Michael Herman é mais preciso ao considerar que a *rationale* do segredo na área de inteligência assenta-se em três diferentes tipos de consideração a respeito de fontes, informações, operações, métodos e tecnologias empregadas.

Em primeiro lugar, utiliza-se o segredo como forma de regulação quando o valor da inteligência obtida depende de o alvo não ficar sabendo o que efetivamente se sabe sobre ele. Por exemplo, o conhecimento prévio de um plano inimigo para um ataque surpresa abre a possibilidade de se preparar uma emboscada. Mas isso só é possível se o inimigo não souber que a vítima do ataque sabe que será atacada.

Em segundo lugar, o segredo deriva também da precária situação legal dos métodos empregados para coletar inteligência. Principalmente em tempo de paz, espionagem, vigilância eletrônica e invasão de redes de computadores (*computer hacking*) contrariam as leis dos países-alvos e mesmo as leis internacionais que garantem a inviolabilidade do território, do espaço aéreo e das águas territoriais. Os custos políticos dessas violações podem ser minimizados através do segredo, que também permite um manejo diplomático mais eficaz das crises eventuais.

Em terceiro lugar, a razão mais forte para o segredo é a vulnerabilidade das fontes às contramedidas de segurança que o alvo tomaria, caso soubesse do esforço adversário em obter inteligência. De qualquer modo, o que se pretende proteger através do segredo não é qualquer informação em parti-

cular que uma fonte já tenha fornecido, mas sim a continuidade dos fluxos de inteligência.<sup>49</sup>

Na guerra e na paz, segredos marcam profundamente o *modus operandi* e a cultura organizacional do serviço de inteligência, mesmo quando o trabalho de análise se baseia principalmente em fontes ostensivas, não-secretas. Note-se que não existe relação direta e unívoca entre a natureza secreta das fontes ou meios de coleta e a qualidade das análises produzidas em inteligência. Há, sim, no entanto, associações negativas entre a intensidade/quantidade de segredos governamentais e a possibilidade de controle dos cidadãos sobre o governo.

Portanto, do ponto de vista dos arranjos institucionais democráticos a aplicação desse tipo de regulação a um específico fluxo informacional teria um duplo ônus da prova: o da necessidade do segredo para a eficácia da missão e o da garantia de controle público, ainda que indireto. Os problemas relativos ao controle externo das atividades de inteligência constituem o objeto da próxima seção deste capítulo.

## Controle externo

O acesso dos cidadãos às informações sobre o que os governantes fazem e sobre o que eles sabem é uma condição necessária para se manter os governos contemporâneos minimamente representativos em relação aos governados. Um dos principais dilemas enfrentados pela teoria democrática é como compatibilizar a necessária autonomia que os governantes precisam ter para defender os interesses e a segurança dos governados com o pleno funcionamento de mecanismos capazes de assegurar que as ações dos governantes serão conduzidas respeitando-se a vontade dos governados. Esse respeito é tanto relativo à vontade manifestada expressamente pelos governados (responsividade) quanto é relativo à avaliação posterior das ações dos governantes pelos governados (*accountability*). Do ponto de vista de uma teoria da democracia, portanto, a representatividade se estabelece através de eleições (chamadas de mecanismos verticais de prestação de contas) e também da fiscalização mútua entre órgãos e poderes (chamados de mecanismos horizontais de prestação de contas).<sup>50</sup>

Esse dilema é particularmente difícil quando se trata de discutir o controle público sobre a segurança nacional, o segredo governamental e os serviços de inteligência. Isso ocorre porque, nesses casos, as tensões entre segurança estatal e segurança individual, assim como as tensões entre segredo governamental e o direito dos cidadãos à informação, são estruturalmente determinadas pela natureza anárquica da autoridade no sistema internacional e são mais ou menos agudas dependendo da natureza dos regimes políticos, das formas de governo e de outras características institucionais e esco-

lhas políticas dos sujeitos relevantes em cada país. Embora possam e devam ser reduzidas através da ação política consciente e da construção institucional cuidadosa, tais tensões são inelimináveis nos marcos do atual sistema de Estados, o qual representa a forma moderna predominante de resolução do problema do acomodamento institucional do convívio social em sociedades complexas marcadas por conflitos de interesses e de opiniões.

Em se tratando da existência e da operação de serviços estatais de inteligência e segurança, a dupla tensão discutida nas seções anteriores implica dois tipos de riscos principais: 1. o risco de manipulação dos serviços por parte de governantes procurando maximizar poder; 2. o risco de autonomização dos próprios serviços, que se transformariam num tipo de poder paralelo dentro do Estado. Mesmo que não existam garantias definitivas contra esses riscos, nesta seção serão discutidos alguns dos mecanismos encontrados nos regimes poliárquicos (as democracias “realmente existentes”) que permitem certo grau de controle dos cidadãos sobre os serviços e os usos que os governantes fazem das capacidades estatais de inteligência e segurança.

Existem sete tipos principais de mecanismos de controle público sobre as atividades de inteligência e segurança:

- as próprias eleições;
- a opinião pública informada pela mídia;
- mandatos legais delimitando as funções e missões das diferentes agências e áreas funcionais;
- procedimentos judiciais de autorização de certas operações e de resolução de disputas de interpretação sobre os mandatos legais;
- inspetorias e corregedorias nos próprios órgãos de inteligência;
- outros mecanismos de coordenação e supervisão no Poder Executivo;
- mecanismos de supervisão e prestação de contas no Poder Legislativo.<sup>51</sup>

Do ponto de vista da participação individual dos cidadãos, esses mecanismos variam desde formas mais diretas de expressão de preferências, tais como a sinalização de mandatos através de eleições e a avaliação pessoal *a posteriori* também através de eleições, as manifestações de rua e pesquisas de opinião pública, até os mecanismos mais indiretos, tais como os organismos de supervisão no Poder Executivo e no Poder Legislativo.

De modo geral, na área de inteligência e segurança os mecanismos de controle público são bastante frágeis e incertos, sendo que os mais indiretos e horizontais tendem a ser relativamente mais efetivos. Diante dessa relativa fragilidade, é comum encontrar exortações sobre a necessidade de programas de treinamento e processos de socialização dos funcionários das agê-

cias de inteligência que incorporem elevados valores cívicos e alto grau de profissionalismo e respeito à Constituição. Esse é um tema complexo e, embora me pareça inegável a necessidade de um código de conduta em qualquer profissão (deontologia), preferi destacar aqui as instituições externas de controle e não as normas internas que regulam o comportamento considerado adequado para os serviços de inteligência numa democracia.<sup>52</sup>

No restante desta seção serão discutidos brevemente os instrumentos legais e políticos, os recursos, a dinâmica interna e os déficits institucionais de cada tipo de mecanismo de controle.

### *Eleições*

Como destacam Przeworski, Stokes e Manin (1999:29-51), as eleições são os principais mecanismos de garantia da representatividade em regimes democráticos porque elas têm uma dupla função: selecionar programas de governo, sinalizando assim parâmetros bastante gerais de um “mandato” para os políticos eleitos e, em segundo lugar, por ocorrerem periodicamente, permitirem também avaliar as ações realizadas e decidir sobre a continuidade ou não desses mandatos. Governos são representativos quando são responsivos às preferências dos eleitores e/ou quando eles prestam contas dos seus atos diante dos eleitores.

Todavia, a eficácia institucional das eleições como mecanismo que garante a responsividade (eleições como seleção de mandatos) ou mesmo a *accountability* (eleições como avaliação de mandatos) é severamente constrangida por uma série de fatores. Do lado dos políticos, esses constrangimentos vão desde a necessidade que os candidatos têm de ofertar programas para atrair o eleitor mediano, ao mesmo tempo que precisam acertar compromissos com indivíduos e grupos dotados de recursos de poder capazes de garantir sua eleição, passando pela modificação radical das políticas oferecidas durante a eleição porque as condições de governo são distintas e chegando até os constrangimentos resultantes do fato de que a coalizão no governo e outros fatores externos permitem aos políticos diluir responsabilidades em relação aos resultados das políticas implementadas, o que termina por enfraquecer decisivamente as eleições como mecanismos de avaliação de *performance*. Do lado dos eleitores, os constrangimentos vão desde a complexidade da relação entre políticas governamentais e situações concretas de bem-estar e segurança até o fato de os programas ofertados precisarem ser selecionados com base em consequências antecipadas no curto e no médio prazos, passando pelo obstáculo quase intransponível de que eleições são momentos episódicos nos quais avalia-se o desempenho dos governantes em dezenas de áreas distintas, relacionadas com milhares de decisões toma-

das ao longo de mandatos multianuais, o que dificulta enormemente qualquer avaliação retrospectiva e qualquer sinalização detalhada de preferências. Esses e outros fatores (principalmente a disponibilidade e o custo das informações) tornam muito difícil atribuir responsabilidades claras aos governantes e aos diferentes candidatos e seus programas.<sup>53</sup>

Junta-se a isso o impacto de diferentes arranjos institucionais sobre os resultados eleitorais e as eleições revelam-se, no final das contas, mecanismos muito imperfeitos para os cidadãos controlarem os governantes em quaisquer áreas temáticas ou aspectos políticos mais específicos.<sup>54</sup> Nesse contexto institucional, e a não ser eventualmente em situações de conflito internacional ou quando emergem grandes escândalos políticos, as atividades de inteligência e segurança estatal têm baixíssima probabilidade de aparecerem numa disputa eleitoral qualquer como um *issue* destacado. Por tudo isso, o controle externo de políticas de inteligência através do processo eleitoral tende a ser muito esporádico e fragmentado. Embora a eleição envolva a participação individual dos cidadãos, particularmente no caso dos temas de segurança e inteligência esse é um mecanismo de controle excessivamente indireto, que depende quase completamente do que acontece no âmbito dos mecanismos mais diretos de supervisão para que questões relacionadas com segurança e inteligência cheguem à atenção do público e, eventualmente, entrem na agenda eleitoral.

### *Mídia*

Um dos papéis fundamentais da mídia seria justamente levar à atenção do público temas relevantes e polêmicos. Porém, de forma semelhante ao que acontece no caso das eleições, os déficits institucionais mais gerais associados à função fiscalizadora da mídia sobre as ações governamentais são agravados quando se trata das atividades de inteligência e de segurança. Dois tipos principais de dificuldades podem ser destacados: 1. Os limites da isenção jornalística em contextos nos quais as grandes empresas de comunicação e os governos mantêm relações simbióticas e ao mesmo tempo conflitivas. 2. Os limites impostos pelo segredo governamental e as difíceis decisões sobre tornar público ou não um segredo obtido pelos meios de comunicação.<sup>55</sup>

O primeiro tipo de dificuldade existe na medida em que as empresas de comunicação precisam manter níveis de audiência lucrativos, o que pode chegar a ponto de o veículo relatar notícias com o viés que melhor atenda a esse imperativo. Por seu turno, governos precisam comunicar ao público suas ações com um viés capaz de contribuir para a manutenção de taxas de aprovação popular viáveis politicamente. Como o governo depende da mídia como um canal incomparável de comunicação com o público e a mídia depende do governo como uma fonte inesgotável de notícias mais ou menos

impactantes sobre a audiência, a relação tende a oscilar permanentemente entre cooperação e antagonismo.

Como os temas de inteligência e segurança são particularmente sensíveis a ambos os tipos de pressão (manipulação da informação pelo governo e “espetacularização” da notícia pela mídia), isso limita bastante a capacidade de a mídia comportar-se como um agente do público na fiscalização e no controle das políticas e agências de inteligência e de segurança. Limitação não quer dizer impossibilidade. Há exemplos de cobertura jornalística que contribuem para esclarecer o público, mas as limitações para isso são realmente muito grandes.<sup>56</sup>

A função fiscalizadora da mídia na cobertura das áreas de inteligência e segurança é ainda mais prejudicada naqueles contextos em que as práticas profissionais de investigação e de isenção jornalística são fracas, onde há grande dependência de fontes oficiais não verificadas independentemente ou, ainda, nas situações em que a própria fusão corporativa da indústria de entretenimento e de notícias produz incentivos adicionais para a “ficcionalização” dos fatos narrados. Como se sabe, desde o século XVIII existe um gênero literário sobre espionagem, o qual foi decisivo para formar as imagens e a aura de mistério e aventura que cerca as atividades de inteligência para a maioria das pessoas. As versões contemporâneas desse gênero na literatura, no cinema e nos jogos eletrônicos possuem tal grau de penetração na cultura de massas que se torna tentador para os veículos de comunicação “preencherem” os vácuos informativos com um suprimento de imagens, efeitos especiais e trilhas sonoras de seus bancos de dados corporativos. Normalmente isso não é uma decisão dos jornalistas, mas sim uma pressão empresarial que pode ou não prejudicar o conteúdo informacional e crítico das matérias.<sup>57</sup>

Além desses aspectos mais estruturais da relação entre empresas de comunicação e agências governamentais de inteligência, a isenção da mídia pode ser comprometida também no nível micro, especialmente quando os serviços de inteligência recrutam ou manipulam jornalistas empregados por veículos de comunicação, seja como fontes de informação, seja como intermediários entre o serviço e uma fonte, ou mesmo utilizando identidades jornalísticas para oficiais de inteligência operando no exterior sem cobertura diplomática.<sup>58</sup> Embora a abordagem dos órgãos de inteligência possa ocorrer com qualquer outra profissão que tenha acesso ao exterior (acadêmicos, técnicos especializados, diplomatas, membros do clero, empresários etc.), no caso do jornalismo, ao concretizar-se o recrutamento, ele diminui evidentemente a capacidade de a mídia atuar como um mecanismo de fiscalização.

Como a eventual exposição do vínculo de um jornalista com os serviços de inteligência de seu próprio país afeta a credibilidade da mídia e a

confiança do público no governo, a comparação entre custos e benefícios pode estar por trás do anúncio feito em 1976 pelo então DCI, George Bush, de que a CIA encerrara naquele ano todos os contratos remunerados com funcionários de empresas de comunicação anteriormente empregados pela agência. Seja qual for a razão para essa decisão no caso norte-americano, quando assumiu a direção da KGB, em 1991, Yevgueny Primakov anunciou também o fim da utilização de veículos de comunicação soviéticos (rusos) como cobertura para a atuação de oficiais de inteligência no exterior, especialmente o *Izvestia*.<sup>59</sup>

Ainda que a mídia esteja longe de ser um agente perfeito do público e tenha severas limitações endógenas e exógenas para fiscalizar o governo, a existência de diversos veículos e mídias independentes pode, no mínimo, exercer alguma pressão competitiva sobre as agências governamentais responsáveis pela obtenção de inteligência a partir de fontes ostensivas (*open sources intelligence*) e pela produção de inteligência sobre temas correntes (*current intelligence*). Afinal, o mero alcance global das agências de notícias e o impacto do uso comercial das novas tecnologias de informação e comunicação (TICs) posicionam as empresas privadas de comunicação para competirem com os produtores governamentais de inteligência pela atenção dos governantes, *policymakers*, comandantes militares e chefes de polícia. No entanto, os eventuais impactos positivos dessa competição são mais claros em relação à agilidade do que em relação à transparência.<sup>60</sup>

Sobre o segundo tipo de dificuldade que a mídia enfrenta para exercer uma função fiscalizadora (segredo governamental como um tipo de regulação pública sobre fluxos de informação), nos contextos em que vigora efetivamente a liberdade de imprensa a decisão sobre publicar ou transmitir uma matéria que envolva a revelação de informações reguladas por classificações de segurança (segredos) tende a ser uma responsabilidade da própria empresa, ponderados os argumentos governamentais sobre as necessidades de segurança nacional. Embora a revelação de segredos de Estado seja um crime tipificado na maioria dos ordenamentos jurídicos contemporâneos, uma vez revelados por uma fonte “oficial” é difícil caracterizar como crime a publicação ou a ampla divulgação da informação. Esta passa a ser, portanto, uma decisão principalmente política. A responsabilização legal sobre a divulgação de segredos governamentais por parte de agentes privados tende a acontecer apenas em situações extremas, que envolvam acusações de espionagem ou traição.<sup>61</sup>

Como regra geral, em se tratando de pensar a mídia como um mecanismo de fiscalização a serviço dos cidadãos, a decisão jornalística a favor da publicização de segredos governamentais somente seria aceitável quando o próprio governo falhasse em justificar publicamente a necessidade do segredo do ponto de vista da segurança nacional, ou seja, quando a informação

classificada estiver servindo apenas para ocultar uma incompetência, um crime ou um capricho dos governantes e não para proteger os cidadãos de ameaças contra a sua segurança. Certamente uma recomendação tão genérica apenas reforça a convicção de que se trata, em última análise, de um tipo de decisão política inevitavelmente polêmica, a qual sempre envolve riscos morais e incertezas que apenas em parte são minimizados pelos parâmetros fornecidos pelo mandato legal das agências de inteligência e segurança.

### *Mandatos legais*

A própria idéia de que os serviços de inteligência deveriam ter uma regulamentação legal mais detalhada de suas funções, mandatos e missões é relativamente recente. Como lembra corretamente Peter Gill (1996:313-333), no caso britânico passaram-se mais de 80 anos entre a criação dos serviços de inteligência exterior e de segurança (originariamente uma única organização fundada em 1909) e a promulgação das duas leis (Security Service Act, 1989, e Intelligence Services Act, 1994) que atualmente regulam o funcionamento, as missões e os mecanismos de prestação de contas das três principais agências de inteligência daquele país.

A importância central da delimitação desses mandatos, do ponto de vista dos mecanismos de controle público, é que eles fixam expectativas normativas associadas ao desempenho de papéis sociais até então desconhecidos para o público. Quando uma lei ou uma diretriz executiva pública delimita os objetivos, os meios, as responsabilidades e as condutas esperadas de cada agência de um sistema nacional de inteligência, isso fornece uma base mínima a partir da qual se pode avaliar os desempenhos desses sistemas do ponto de vista da agilidade e da transparência.

Porém, uma limitação óbvia para que essa avaliação seja feita pelos cidadãos individualmente é que muitas das diretrizes e regulações mais importantes (sobre requerimentos informacionais, alocações de recursos, operações específicas e produtos de inteligência, por exemplo) são necessariamente secretas.<sup>62</sup> Ainda assim, os contornos mais gerais das atividades de inteligência e segurança podem e devem ser fixados em leis e diretrizes executivas públicas. As diretrizes executivas tendem a ser mais detalhadas do que as legislações aprovadas pelo Parlamento.

Apenas para citar um exemplo, note-se que o National Security Act of 1947 norte-americano estabelece genericamente que inteligência significa o conjunto de “informações relativas às capacidades, intenções e atividades de governos, organizações ou indivíduos estrangeiros”, fixando então como mandato da CIA a coleta de inteligência a partir de “fontes humanas e outros meios apropriados, sendo que a agência não terá poderes de polícia, subpoena

(intimação sob sanção) ou de imposição da lei, assim como não deverá exercer funções de segurança dentro do país". Apenas depois de 1981, como resultado de longas disputas sobre o significado e a abrangência desse mandato, a Executive Order 12.333 estabeleceu os tipos de informações que a CIA deveria coletar, analisar e disseminar sobre alvos estrangeiros, além de explicitar pela primeira vez que a agência também era encarregada das operações de contra-inteligência no exterior e das operações encobertas (chamadas nessa *executive order* de *special activities*). Além de detalhar os objetivos, tipos de informações e técnicas de coleta passíveis de serem utilizadas pela CIA, a Executive Order 12.333 também explicita as funções e alvos que são vedados à atuação da agência. Mais importante do que esse detalhamento, no entanto, foi o fato de que essa *executive order* pela primeira vez especificou publicamente as missões e áreas de atuação de uma série de outras agências de inteligência norte-americanas que não haviam sido criadas por lei, mas por decisão administrativa secreta do Poder Executivo.<sup>63</sup>

Os mandatos legais são necessários tanto para estabelecer parâmetros para os governantes controlarem o grau de eficiência e efetividade dos serviços de inteligência e de segurança (agilidade), quanto para auxiliar os cidadãos a controlarem o grau de compatibilidade entre a atuação desses mesmos serviços e as regras institucionais democráticas (transparência). Um aspecto pouco notado a respeito dos mandatos é que, do ponto de vista dos serviços de inteligência, estes funcionam também como uma forma de proteção das próprias agências contra eventuais pressões políticas de ministros ou chefes de governo e de Estado para a realização de missões impróprias e que, diante da existência de mandatos codificados legalmente, seriam também ilegais e passíveis de responsabilização.

Em nenhuma outra área de atuação dos serviços de inteligência contemporâneos os mandatos legais são mais necessários do que na área de inteligência interna ou de segurança.<sup>64</sup> Como salientam Lustgarten e Leigh (1994: 374-411), a maioria dos serviços de inteligência de segurança forjou sua cultura organizacional e seus hábitos operacionais no contexto da repressão aos movimentos de esquerda ou, de modo mais geral, combatendo a dissidência política e os críticos dos governos. A forte orientação ideológica anticomunista dos serviços de segurança dos países capitalistas e a forte orientação repressiva contra os dissidentes nos países do chamado Socialismo Real tornaram-se substitutos de uma delimitação mais precisa, politicamente deliberada e legalmente consistente dos conteúdos de termos como "subversão", "terrorismo" e "sabotagem".

Analizando os mandatos legais atualmente em vigor para os serviços de inteligência de segurança da Grã-Bretanha, Canadá e Austrália, Lustgarten e Leigh observaram que as missões de contra-espionagem e as medidas defensivas de segurança (operacional e informacional) tendem a ser menos ambíguas e

implicam menos riscos para as liberdades civis dos cidadãos dos países democráticos.<sup>65</sup> Já no caso da obtenção de inteligência sobre ameaças terroristas, sabotagem e subversão há denúncias recorrentes sobre a falta de proporcionalidade entre as ameaças e as medidas de segurança com as quais os governos tendem a responder, bem como denúncias sobre a caracterização arbitrária de dissidentes políticos como “terroristas”. No contexto pós-Guerra Fria, há uma tendência moderada nesses três países (mais acentuada no caso australiano) para uma definição legal mais estrita de subversão, apontada como a “utilização organizada e continuada de meios violentos para fins de transformação da ordem política constitucionalmente estabelecida”. Isso exclui do mandato legal dos serviços de segurança (*security intelligence*) a vigilância física e eletrônica de ativistas, manifestantes ou participantes de organizações de oposição ao governo, mesmo nos casos em que os cidadãos se engajam em atos de desobediência civil. Por outro lado, essa tentativa de definição legal mais neutra do ponto de vista ideológico resulta também do crescimento da violência politicamente motivada e do terrorismo perpetrados por organizações de extrema direita, tais como as milícias norte-americanas ou os grupos racistas e xenófobos existentes em quase todos os países mais industrializados e de renda *per capita* mais elevada.

Claro está que os mandatos legais não resolvem os problemas políticos resultantes da interpretação sobre as áreas, os métodos e a intensidade da atuação das agências de inteligência. Tampouco as definições contemporâneas dos termos “subversão, terrorismo e sabotagem” estão isentas de viés político ou ideológico conservador, mesmo nas poliarquias institucionalizadas.<sup>66</sup> Entretanto, considerando-se que existem realmente ameaças que exigem a manutenção de organizações de *security intelligence*, os mandatos legais tornam-se imprescindíveis para ao menos estabelecer parâmetros a partir dos quais se possa julgar as ações e prioridades desses órgãos.

Além disso, os mandatos legais tornam-se mais importantes diante dos resultados recentes de estudos institucionais como o de Amy Zegart (1999:1-53), que concluiu que o fator mais importante na determinação da trajetória das agências de segurança nacional (entre as quais incluem-se os serviços de inteligência) são as escolhas estruturais feitas no momento da criação dessas agências. Essas escolhas estruturais envolvem não apenas o desenho organizacional, mas principalmente o conjunto de regras formais e costumes quase-legais que delimitam suas missões e métodos de atuação.

Ao avaliar os desafios relacionados ao controle do público sobre as atividades de inteligência em contextos de transição e consolidação democrática, Thomas Bruneau (2000:1-36) destacou três tipos de escolhas que seriam decisivas e que deveriam constar do mandato legal do setor: 1. A primeira escolha envolveria determinar em quais áreas de especialização da atividade de inteligência o governo deveria investir (humint, sigint, imint, aná-

lise, contra-inteligência, operações encobertas etc.), quantas organizações deveriam ser criadas para as diferentes missões e qual o volume de recursos que o país deveria dedicar para a montagem de um sistema nacional de inteligência. 2. A segunda escolha estaria relacionada ao peso relativo (nas esferas de produção e de consumo) das organizações militares e das organizações civis de inteligência, bem como ao grau de controle ou autoridade formal que os militares terão sobre os recursos humanos, tecnológicos e orçamentários do setor. 3. O terceiro tipo de escolha refere-se à relação considerada desejável entre inteligência e políticas governamentais (*policymaking*). Há grande variação no modo como as poliarquias lidam com essa relação, mesmo no caso dos países anglo-saxões. Enquanto nos Estados Unidos o processo de análise e produção de inteligência estratégica é coordenado por um diretor central de inteligência, formalmente separado do processo de *policymaking*, na Inglaterra a inteligência coletada por diferentes agências (MI-5, SIS, CGHQ, Jarc etc.) é analisada e integrada ao processo decisório por times mistos de analistas de inteligência e pessoal dos ministérios “consumidores” de inteligência, times coordenados pelo Ministério das Relações Exteriores ou pelo Ministério do Interior, conforme o caso.<sup>67</sup>

Enfim, os três tipos de escolhas têm consequências para o controle externo das atividades de inteligência e, uma vez traduzidos em ordenamentos legais e mandatos, tendem a durar no tempo, ainda que sejam sujeitos a interpretações políticas ou até mesmo judiciais.

### *Judiciário*

Embora o Judiciário possa ser acionado para resolver disputas entre os cidadãos e o governo a respeito dos mandatos legais e da conduta dos serviços de inteligência e de segurança, isso não acontece facilmente. Recorrendo mais uma vez ao estudo de Lawrence Lustgarten e Ian Leigh (1994:320-359 e 468-492), pode-se afirmar que existem grandes dificuldades jurídicas e políticas para que o Judiciário exerça um papel revisor independente das decisões do Poder Executivo nas áreas relacionadas com a segurança nacional.

Do ponto de vista jurídico, caberia mencionar a percepção do próprio Poder Judiciário sobre sua incapacidade constitucional para julgar as práticas do Poder Executivo em matérias de segurança nacional. Esse tipo de auto-refreamento expressa uma visão da divisão dos poderes altamente formalista, mas de grande apelo. Mesmo em países como a Grã-Bretanha, onde a doutrina da divisão dos poderes não é tão formal, o entendimento do Judiciário é que a sanção dos atos do Poder Executivo nessas áreas de política de defesa nacional, segurança, política externa e inteligência deve ser feita, quando for o caso, pelo Parlamento.

Influenciam nessa percepção os próprios princípios processuais, pois na área de segurança nacional seria mais difícil tomar decisões judiciais baseadas no estabelecimento de provas “além de qualquer dúvida razoável”. Principalmente quando se está falando de revisar judicialmente decisões referentes, por exemplo, ao emprego de meios diplomáticos ou militares para dissuadir um governo estrangeiro de tomar uma decisão qualquer que poderá prejudicar os interesses nacionais e a segurança nacional no médio prazo. Considerando a diferença proposta por Ronald Dworkin (1978:22) entre decisões políticas e decisões baseadas em princípios, as ações governamentais na área de segurança e inteligência seriam protótipos de decisões políticas, enquanto o ato de julgar seria inerentemente um tipo de processo decisório baseado em princípios abstratos e regras gerais. Na medida em que decisões de segurança nacional dificilmente podem ser revistas com base em questões factuais, pois envolvem antes de mais nada escolhas “difícies” baseadas em tendências e probabilidades, a orientação do Judiciário rumo a decisões baseadas no esclarecimento dos fatos e na busca de justiça para as partes em processos de adjudicação de conflitos tende a afastá-lo de litígios com o Poder Executivo sempre que as razões de segurança nacional são utilizadas para justificar as práticas do governo.

A capacidade de assegurar justiça para o tratamento das partes em adjudicações de conflitos entre indivíduos e o Estado que envolvam temas de segurança nacional é prejudicada ainda pelo segredo governamental, que limita o exercício do próprio princípio do contraditório. Ora, esse princípio diz basicamente que se deve escutar a outra parte (*audi alteram partem*). O problema é que quando uma das partes é o governo do país e a outra parte é um indivíduo e o governo pode impedir legalmente que informações ou provas sequer apresentadas ao tribunal por questões de segurança nacional, há um esgarçamento quase irreparável do próprio princípio: uma das partes não será adequadamente ouvida porque apenas o governo tem acesso às informações que poderiam provar o ponto do litigante.<sup>68</sup>

Do ponto de vista político, valeria destacar que esse auto-refreamento do Poder Judiciário tende a ser um arranjo funcional tanto para o próprio Judiciário quanto para o Poder Executivo. Mesmo sem admitir formalmente que sua capacidade de desempenhar um papel de árbitro entre decisões do governo e a interpretação divergente de algum indivíduo afetado por aquela decisão é baixa, há uma série de procedimentos e manobras através dos quais o Judiciário tende a aceitar as justificativas oficiais sem maiores questionamentos. Para dizerê-lo nos termos de Ronald Dworkin (1988), isso compromete a idéia de que a função judicial é baseada na prioridade da lei sobre as razões de Estado. Como já foi visto em relação ao próprio conceito de segurança nacional, diante de uma decisão que afete concreta e imediatamente

mente um indivíduo ou a população inteira de forma negativa, as alegações do Poder Executivo de que esse custo é aceitável tendo-se em vista os interesses mais gerais e de longo prazo do público, relacionados à sua segurança ou bem-estar, deveriam ser cuidadosamente pesadas por alguma autoridade externa. Entretanto, na esmagadora maioria dos processos judiciais envolvendo problemas de segurança nacional analisados por Lustgarten e Leigh (1994), a decisão final dos tribunais foi favorável ao Poder Executivo.<sup>69</sup>

Por outro lado, um papel mais ativo do Judiciário no controle da legalidade e da razoabilidade das ações executivas em áreas de segurança e inteligência pode acontecer quando a própria legislação em vigor exige uma aprovação judicial *ex ante* de certas operações. Ou então *a posteriori*, quando juízes são encarregados (ainda que de forma *ad hoc*) da coordenação de comissões de inquérito sobre operações ou atividades sobre as quais pesem suspeitas de conduta imprópria ou ilegal.

Um exemplo da primeira situação pode ser encontrado nas disposições legais do Foreign Intelligence Surveillance Act of 1978 norte-americano (Fisa). Basicamente, essa lei determina que quaisquer operações de vigilância eletrônica e buscas físicas contra alvos estrangeiros para fins de obtenção de inteligência externa, que ocorram dentro do território dos Estados Unidos, precisam ser autorizadas por escrito pelo Attorney General (ministro da Justiça/advogado-geral) e confirmadas por uma corte especial de Justiça. Por vigilância eletrônica entende-se a interceptação clandestina de comunicações telefônicas, mensagens de e-mail, fax ou a utilização de microfones escondidos, sensores de movimento, localizadores etc. Por buscas físicas, entende-se a invasão sub-reptícia de locais privados para obtenção de documentos, instalação de escutas eletrônicas, vigilância de movimentos do alvo etc. A corte especial do Fisa é formada por sete juízes membros de cortes distritais de diferentes circuitos e pode autorizar operações por até um ano quando o alvo é um governo estrangeiro, ou por até 90 dias em todos os outros casos sob a jurisdição dessa lei. Uma corte de apelação é formada por três juízes de cortes distritais ou cortes de apelação de diferentes circuitos, e, caso uma solicitação de vigilância física ou eletrônica seja recusada também pela corte especial de apelação, o governo pode levar cada solicitação operacional até a Suprema Corte. Embora as requisições de autorização precisem fornecer detalhes sobre os alvos, os tipos de informações e as justificativas para a necessidade de uso de técnicas intrusivas especiais, uma avaliação do Comitê de Inteligência do Senado sobre os relatórios classificados enviados anualmente pelo attorney general ao Congresso indicou que nos primeiros cinco anos de vigência do Fisa nenhuma solicitação de vigilância havia sido recusada sequer em primeira instância.<sup>70</sup>

No caso da participação de juízes em comissões extrajudiciais (um traço característico do sistema de supervisão britânico), as preocupações levantadas

por Lustgarten e Leigh (1994:487-491) dizem respeito à compatibilidade entre a orientação factual que tendem a ter os juízes e o trabalho de formulação de recomendações de política que resulta do trabalho de comissões *ad hoc* para revisão de temas polêmicos na área de segurança nacional. Na verdade, dizem respeito mais ainda aos casos em que juízes participando de comissões revisoras extrajudiciais desenvolvem posições partidárias sobre determinadas escolhas de política governamental nessas áreas e, posteriormente, precisam arbitrar diferenças de interpretação e conflitos de interesses nas mesmas áreas em que atuaram *pro tempore*. Como muitas dessas comissões são criadas após um escândalo ou no contexto de fortes críticas à atuação dos serviços de inteligência, um risco maior ainda seria o governo utilizar as próprias comissões especiais dirigidas por juízes como um expediente para ganhar tempo e acalmar os críticos sem realmente fazer alguma coisa.

Esse tipo de desconfiança ocorre também em relação à capacidade de os corregedores e inspetores dos próprios órgãos de inteligência e segurança agirem de forma efetiva, com isenção e autonomia. Mas esse já é o tema do próximo item.

### *Inspetorias e corregedorias*

Nos países que seguem o modelo anglo-saxão de organização dos sistemas nacionais de inteligência, a instituição de corregedorias e escritórios de inspetoria geral tem conformado um padrão consistente de resposta governamental às denúncias de violação do mandato legal das agências, autonomização administrativa e escândalos políticos associados ao setor. Além disso, como destaca Geoffrey Weller (1997:383-406) em artigo onde compara o desempenho institucional dos inspetores gerais dos serviços de inteligência dos Estados Unidos, Inglaterra, Canadá e Austrália, as demandas por *accountability* e maior responsividade dos serviços às autoridades eleitas aumentaram nesses países ao longo das últimas décadas também em função da crescente complexidade operacional e organizacional da área de inteligência.

Diante desses dois fatores (esforços das autoridades responsáveis para evitar escândalos e necessidade de uma resposta institucional à complexificação crescente do setor), um dos mecanismos encontrados foi a instituição de escritórios de inspetoria geral e corregedorias independentes dos dirigentes das agências de inteligência. Nos quatro países analisados por Weller, a figura de um corregedor/inspetor nomeado pelos próprios dirigentes das agências existia desde a época da criação dos sistemas nacionais de inteligência e segurança, mas a partir de meados da década de 1970 surgiram críticas mais ou menos severas sobre a capacidade de esses corregedores administrativos fiscaliza-

rem efetivamente a compatibilidade das práticas dos serviços de inteligência com os mandatos legais e as diretrizes políticas dos governantes.

De modo geral, pode-se dizer que a efetividade de qualquer um desses mecanismos de supervisão e *accountability* nas áreas de segurança e inteligência depende do grau de autonomia do órgão fiscalizador em relação ao órgão fiscalizado, da vontade política/capacidade pessoal dos procuradores e fiscais para exercerem seu mandato, dos recursos disponíveis e do acesso efetivo às informações, documentos e pessoas relevantes da organização. Em relação a essas condições necessárias, mesmo entre Estados Unidos, Grã-Bretanha, Canadá e Austrália existem variações significativas que deveriam ser levadas em conta em estudos comparativos posteriores com um número maior de casos nacionais.

A autonomia dos inspetores tende a ser um pouco maior no caso do sistema presidencialista norte-americano, pois os nomes dos inspetores-gerais de inteligência da CIA e dos departamentos de Estado, Justiça, Tesouro, Energia e Defesa precisam ser sabatinados e confirmados pelo Senado, não podem ser demitidos pelos dirigentes das agências e devem reportar-se pelo menos anualmente aos comitês de inteligência do Senado e da Câmara dos Representantes. Nos sistemas parlamentaristas de Canadá, Austrália e Grã-Bretanha, o Legislativo não participa diretamente da nomeação e os inspetores-gerais reportam-se somente aos ministros responsáveis pelas agências de inteligência ou a outros órgãos de supervisão do próprio Poder Executivo. Esse é o caso do Canadá, onde o inspetor-geral do Canadian Security Intelligence Service (CSIS) é nomeado pelo gabinete ministerial e envia seus relatórios para o Solicitor General e para o Security Intelligence Review Committee (Sirc), que eventualmente os repassa para o Parlamento.. Na Austrália, o inspetor-geral é nomeado pelo governador-geral, com base numa indicação feita pelo primeiro-ministro após consulta ao líder da oposição.<sup>71</sup>

A vontade política e a capacidade de exercer um papel investigador e controlador obviamente variam não apenas de país para país, mas também de indivíduo para indivíduo. De modo geral, em seu artigo, Weller tem uma avaliação positiva sobre os inspetores-gerais estatutários, mas uma opinião menos favorável sobre o desempenho dos inspetores e corregedores administrativamente nomeados.

Por outro lado, esse desempenho diferencial está ligado à própria amplitude dos mandatos e aos incentivos que cada inspetoria tem para cumprir aquele mandato. Os mandatos podem incluir desde o controle da legalidade das operações de inteligência até a realização de auditorias financeiras, passando pela verificação do grau de aderência das ações dos dirigentes das agências de inteligência às diretrizes das autoridades responsáveis e à lei, pela revisão dos métodos e procedimentos operacionais para fins de reco-

mendação de melhorias ou, ainda, pela condução de investigações específicas em caso de denúncias internas e externas. Dos casos analisados por Weller, apenas o inspetor-geral da Austrália e, no caso dos Estados Unidos, o inspetor-geral da CIA podem receber diretamente denúncias externas dos cidadãos e iniciar investigações sobre essas denúncias autonomamente. Nos demais casos, qualquer denúncia deve ser encaminhada à autoridade ministerial responsável, que encarrega então os escritórios de corregedoria e inspeção da sua apuração. No caso da auditoria financeira, apenas o escritório do inspetor-geral da CIA tem essa função, que em todos os demais casos é delegada para comissões especiais dos próprios órgãos centrais de auditagem de contas públicas.<sup>72</sup>

Em termos de recursos disponíveis, é preciso levar em conta a abrangência dos mandatos e do número de agências sob a jurisdição de cada inspetor-geral. Considerando apenas os casos da Austrália e dos Estados Unidos, onde os mandatos dos inspetores-gerais são mais abrangentes, pode-se afirmar que os recursos atuais são escassos. Na Austrália, o inspetor-geral é responsável por fiscalizar cinco agências que somam juntas cerca de 15 mil funcionários civis e militares. São elas a Australian Security Intelligence Organisation (Asio), a Defence Intelligence Organisation (DIO), o Australian Secret Intelligence Service (Asis), o Defence Signals Directorate (DSD) e o Office of National Assessments (ONA). Para supervisionar essas cinco agências, considerando que sua missão envolve a apuração de reclamações internas e denúncias externas, o escritório do inspetor-geral conta com sete funcionários.<sup>73</sup> Nos Estados Unidos, o escritório do inspetor-geral da CIA (uma organização com cerca de 16 mil funcionários) contava em 1997 com 121 funcionários, sendo que pelo menos 30 eram contadores trabalhando na divisão de auditoria financeira do escritório. No Departamento de Defesa, onde o escritório do inspetor-geral para a área de inteligência supervisiona quatro agências (NSA, NRO, Nima e DIA) que, somadas, têm cerca de 40 mil funcionários, os recursos são ainda menores do que na CIA.<sup>74</sup>

Finalmente, a capacidade de acesso aos documentos, pessoas e locais é garantida aos inspetores-gerais em todos os ordenamentos legais mais recentes, embora existam exceções no caso da Inglaterra e do Canadá. Entretanto, problema maior do que as exceções é a decisão sobre o que fazer com o material obtido diante da falta de pessoal de apoio para avaliar adequadamente as informações. Os corregedores e inspetores-gerais produzem relatórios regulares e também relatórios especiais. Em alguns casos, como o do relatório do inspetor-geral da CIA sobre o caso Aldrich Ames (ex-chefe da seção russa da contra-inteligência na CIA que espionava para os soviéticos e depois para os russos), esses relatórios são “megaprojetos” que envolvem a cooperação de várias instâncias de supervisão e meses de trabalho.<sup>75</sup>

Segundo Weller (1997:396-398), de modo geral o papel dos inspetores-gerais estatutários tem sido positivo e seus relatórios têm contribuído para aumentar o grau de agilidade e transparência dos sistemas de inteligência nos quatro países onde o autor conduziu entrevistas. Mas permanece o fato de que a maioria das recomendações surgidas a partir desses mecanismos de controle é feita *a posteriori*, na esteira de escândalos ou de problemas gerenciais internos às próprias organizações.

Assim, mesmo que os inspetores-gerais e corregedores na área de inteligência não sejam necessariamente os “tigres sem dentes” que alguns parlamentares temiam inicialmente, seu trabalho é por definição muito dependente dos demais mecanismos de supervisão e *accountability* do Poder Executivo e do Poder Legislativo.

### *Poder Executivo*

Além das inspetorias gerais e corregedorias localizadas nas agências de inteligência e nos ministérios responsáveis, o Poder Executivo supervisiona seus serviços de inteligência através de vários outros tipos de ferramentas institucionais. Serão mencionadas aqui apenas as instâncias de controle voltadas mais direta e exclusivamente para os serviços de inteligência. Antes, porém, duas observações preliminares precisam ser feitas.

O controle da legalidade dos atos das agências de inteligência e segurança é decisivo para manter a confiança pública e, do ponto de vista dos governantes, para evitar escândalos políticos. Além do controle da legalidade, os comitês executivos de supervisão e coordenação também são encarregados de garantir a adequação entre as prioridades operacionais das agências de inteligência e as necessidades informacionais dos tomadores de decisão, sejam eles os chefes de governo, seus ministros, os comandantes militares e os chefes de polícia. Esses tomadores de decisão são ao mesmo tempo os “*principals*” das agências (seus “gerentes”) e os consumidores de seus produtos. Dada a complexidade organizacional e funcional dos atuais sistemas nacionais de inteligência e segurança, os comitês do Poder Executivo encarregados de supervisão e controle externo tendem a ser também algo especializados no controle da legalidade, no controle das prioridades, dos arranjos organizacionais, dos processos internos e/ou na qualidade dos produtos de inteligência. Portanto, para avaliar o desempenho de qualquer instituição de controle externo das atividades de inteligência é preciso ter clara sua *expertise* institucional no campo geral da supervisão executiva.

Uma segunda observação preliminar diz respeito à influência do tipo de governo sobre o desenho organizacional das instâncias de controle externo e supervisão. Não é demais destacar, como o fazem José Cheibub e Adam Przeworski (1999:223), que, embora as diferenças entre democracia e ditadura sejam cruciais

para explicar as relações mais gerais do Estado com os diversos grupos sociais, em se tratando de mecanismos de *accountability*: a diferença relevante se dá internamente à democracia, entre regimes parlamentaristas e regimes presidencialistas. Em parte por isso, no restante desta seção serão utilizados principalmente exemplos retirados da experiência federativa e presidencialista dos Estados Unidos, pois apesar da diferença gigantesca de escala operacional é a mais próxima do marco constitucional adotado no Brasil, e isso facilita a compreensão das funções dos diferentes mecanismos de supervisão.<sup>76</sup>

Naturalmente, casos nacionais como o do Canadá, com sua ênfase na área de inteligência de segurança (*security intelligence*), um desempenho institucional muito bom dos mecanismos de controle externo e uma escala de operações do sistema nacional de inteligência compatível com a dos principais países latino-americanos, seriam igualmente interessantes e merecedores de análise. Mas o modelo parlamentarista adotado naquele país neutraliza boa parte da divisão adotada aqui entre mecanismos de supervisão do Poder Executivo e do Poder Legislativo. No Canadá, o principal mecanismo de supervisão existente é o Security Intelligence Review Committee (Sirc), uma comissão não-parlamentar formada por conselheiros do primeiro-ministro (*privy councillors*). De modo geral, o envolvimento direto do Parlamento no controle dos órgãos de inteligência canadense é baixo, e é no Privy Council Office (PCO) que se localizam as principais instâncias de supervisão externa das agências de inteligência daquele país. Existe um sub-comitê de segurança nacional no Standing Committee on Justice and Legal Affairs do Parlamento, mas como o governo já depende inteiramente da manutenção de uma maioria na Câmara Baixa do Parlamento, a tendência é que os assuntos de inteligência e segurança sejam deixados exclusivamente para os ministros responsáveis.<sup>77</sup>

No caso dos Estados Unidos, a divisão de poderes e os mecanismos de *checks and balances* entre o Congresso e a Presidência induzem uma diferenciação mais clara entre os mecanismos de supervisão e controle existentes no âmbito do Poder Executivo e do Poder Legislativo. No Poder Executivo, as diversas instâncias de supervisão, gerenciamento e coordenação das políticas de inteligência acompanham a complexidade do próprio sistema e visam a manter essas funções no âmbito do Poder Executivo.<sup>78</sup>

Na Presidência da República, existe desde a década de 1950 uma comissão de notáveis, o President's Foreign Intelligence Advisory Board (Pfiab), que tem poderes para solicitar relatórios aos inspetores-gerais e conduzir estudos independentes, fornecendo aconselhamento direto ao presidente da República sobre a política de inteligência, a qualidade do trabalho das agências e inclusive sobre a legalidade de certas ações. Os membros do *board* são nomeados e servem à disposição do presidente. Segundo autores como Pat

Holt (1995:202-205) e Mark Lowenthal (2000:134), essa proximidade do órgão supervisor independente em relação ao presidente tem sido tanto um fator positivo quanto um risco. Na época de seu primeiro *chairman* (dr. James Killian, presidente do Massachusetts Institute of Technology – MIT), o Pfiab trabalhou principalmente sobre temas técnicos e sobre falhas nos procedimentos operacionais das agências, tendo obtido significativo impacto com suas recomendações. A partir dos anos 1980, as nomeações para o *board* passaram a ser crescentemente pautadas por necessidades políticas, e a relevância do órgão teria declinado. Através de uma subcomissão do Pfiab chamada Intelligence Oversight Board (IOB), o escritório da Presidência conta também com um ponto focal para o recebimento de informações sobre eventuais ilegalidades cometidas pelos serviços de inteligência, encaminhadas pelos inspetores-gerais, por funcionários das agências ou diretamente pelo público. De modo geral, o pequeno número de funcionários de apoio e o funcionamento excessivamente *ad hoc* do Pfiab são restrições importantes ao exercício de seu papel supervisor.<sup>79</sup>

De forma mais orgânica e permanente, a Presidência exerce controle sobre as atividades de inteligência através do *staff* do National Security Council (NSC). O diretor de programas de inteligência no *staff* do NSC teria, ao menos em certo grau, condições para direcionar as ações das agências. A própria legislação estabelece que o DCI se reporta ao presidente e ao NSC e, além disso, o fato de a burocracia altamente especializada do conselho ser nomeada pelo presidente para ajudá-lo a formular e a defender a visão presidencial sobre os temas de segurança nacional tende a garantir-lhe autoridade para demandar os serviços de inteligência através de vários mecanismos institucionais (inclusive a *situation room*, na Casa Branca, para monitoramento de crises). Segundo Amy Zegart (1999:76-108), uma das principais características da atual estrutura do NSC é que o crescimento do papel do assessor de Segurança Nacional como diretor de uma grande equipe de formulação de políticas de segurança foi acompanhado pelo esvaziamento relativo do papel do conselho, entendido enquanto a reunião formal de seus membros estatutários (o presidente, o secretário de Defesa e o secretário de Estado). Isso faz do NSC quase exclusivamente um órgão assessor da Presidência. Por isso mesmo, o desempenho do *staff* do NSC dedicado à supervisão das atividades de inteligência é profundamente dependente do interesse do próprio presidente por esses temas. Como lembra Jeffrey Richelson (1999:384-386), a atual estrutura de apoio para o diretor de programas de inteligência do NSC é simplesmente a última de uma série histórica de comitês que tiveram suas prioridades e composição alteradas a cada nova eleição presidencial.<sup>80</sup>

Além dessas duas instâncias, o sistema de supervisão do Poder Executivo nos Estados Unidos abrange ainda as instâncias existentes no âmbito do escri-

tório do diretor central de inteligência e do Departamento de Defesa, para mencionar apenas os mais importantes naquele contexto.<sup>81</sup>

Como o DCI é simultaneamente o coordenador de todo o sistema de inteligência dos Estados Unidos e também o diretor da CIA, parte das reformas introduzidas na década de 1990 visaram a aumentar a capacidade gerencial do DCI sobre o sistema e a separar as instâncias de coordenação geral da direção imediata da CIA. Assim, existem hoje inúmeras instâncias no escritório do DCI voltadas para a supervisão das atividades de inteligência daquele país, algumas colegiadas e outras executivas. Entre os fóruns colegiados mais importantes deve-se mencionar o Executive Committee (IC/Excom) e o National Foreign Intelligence Board (NFIB). Ambos são compostos pelos dirigentes das principais agências de inteligência e pelos responsáveis pela supervisão nos ministérios. O IC/Excom auxilia o DCI a revisar a política nacional de inteligência, o planejamento e as prioridades de alocação de recursos e de obtenção de informações. Também estabelece padrões de avaliação gerencial e indicadores de desempenho. Com uma composição um pouco mais ampla, o NFIB tem como tarefa principal revisar e aprovar as estimativas nacionais de inteligência (NIEs), o principal documento analítico produzido pelos serviços de inteligência norte-americanos. Em tese, esse *board* também é responsável por revisar e coordenar os esforços das várias agências em relação à inteligência externa (*foreign intelligence*), definir procedimentos para o compartilhamento das informações obtidas por diferentes agências e aprovar acordos internacionais com agências de inteligência de outros países. Entre os órgãos executivos que auxiliam diretamente o DCI, deve-se mencionar o Community Management Staff (CMS) e o National Intelligence Council (NIC). Basicamente, a função do CMS é elaborar, avaliar, justificar e monitorar o orçamento de inteligência externa dos Estados Unidos, o National Foreign Intelligence Program (NFIP). Para isso, equipes gerenciais formam grupos de trabalho especializados em diferentes áreas de planejamento estratégico, tradução das necessidades dos usuários em prioridades de coleta, integração de recursos entre diferentes disciplinas de coleta e avaliação de desempenho. Enquanto a função do CMS é gerencial (funcionando como o braço executivo do IC/Excom), o NIC é basicamente um órgão analítico (que elabora as análises de longo prazo que são enviadas para a aprovação do NFIB).<sup>82</sup> Dividido em 12 áreas geográficas e funcionais, cada uma dirigida pelo analista mais veterano da Intelligence Community, o NIC é responsável pela elaboração anual de estimativas de inteligência (NIEs) e também por conduzir avaliações estratégicas com recursos integrados de todas as agências de inteligência do país.<sup>83</sup>

Em todos os ministérios onde existem órgãos de inteligência ou de segurança há também instâncias de supervisão e gerenciamento. Para men-

cionar apenas um exemplo, no Departamento de Defesa (DoD) três autoridades principais exercem funções de supervisão e coordenação das atividades de inteligência nas organizações subordinadas ao Pentágono. Além do inspetor-geral, existe um Assistant to the Secretary of Defense for Intelligence Oversight (ATSD-IO) responsável por garantir que as atividades de inteligência sejam conduzidas em conformidade com as leis e as diretrizes executivas. No âmbito do escritório do Assistant Secretary of Defense for Command, Control, Communications and Intelligence (ASD-C<sup>3</sup>I) concentra-se a maioria das funções executivas de controle e revisão na área de inteligência militar, desde o gerenciamento da formação de recursos humanos até a revisão das arquiteturas de sistemas de suporte para a coleta de inteligência tática, passando por um leque de temas relevantes para essas agências de suporte ao combate. No caso do Under Secretary of Defense for Acquisitions, Technology and Logistics (USD-AT&L), são significativas as atividades de controle e supervisão sobre os programas de pesquisa, desenvolvimento e aquisição de sistemas e plataformas de coleta de inteligência desenvolvidos por agências militares que lidam com grandes orçamentos, tais como NRO, Daro, Darpa e DTRA.<sup>84</sup>

Por mais complexas que sejam essas instituições de controle, é preciso lembrar que as organizações que elas devem controlar tendem a ser ainda mais complexas e diferenciadas funcionalmente. Não há estudos sistemáticos sobre o desempenho dos órgãos de supervisão do Poder Executivo, mesmo nos Estados Unidos.<sup>85</sup> No entanto, é possível pelo menos identificar três tipos de dificuldades que os órgãos de controle devem enfrentar.

Do ponto de vista gerencial, trata-se da dificuldade de se estabelecer uma relação clara entre os *inputs* (orçamentários, tecnológicos e de pessoal) e os *outputs* (produtos finais) em muitos dos sistemas e áreas de atuação das agências de inteligência.<sup>86</sup> Do ponto de vista político, trata-se da dificuldade de avaliar o relacionamento adequado entre os analistas de inteligência e os responsáveis pelo processo de tomada de decisões em diversos contextos de formulação e execução de políticas de segurança, defesa e relações exteriores. Como salienta Michael Herman (1996:298-304), é extremamente difícil medir o valor e o impacto do conteúdo informacional dos produtos de inteligência na qualidade das políticas públicas, o que torna ainda mais exigente o monitoramento da satisfação dos usuários com os produtos e serviços fornecidos pelos órgãos de inteligência.<sup>87</sup> Finalmente, do ponto de vista do controle da legalidade dos atos dos serviços de inteligência, trata-se menos de alguma dificuldade intransponível para o exercício de uma supervisão efetiva e mais da dificuldade de se manter a confiança do público e a legitimidade das ações do Poder Executivo em situações de risco potencial, nas quais um poder se propõe a fiscalizar a si próprio.

Como a maioria dos instrumentos de controle existentes no Poder Executivo surgiu em contextos em que o governo pretendia antecipar um envolvimento maior do Congresso, isso sugere que, apesar de o Poder Executivo dispor dos mecanismos mais efetivos de controle e gerenciamento das atividades de inteligência, dada a natureza dessas atividades, a confiança do público só poderia ser mantida com a presença de mecanismos efetivos de supervisão e *accountability* no âmbito do Poder Legislativo.

### *Supervisão congressual*

Considerando a fragilidade relativa dos demais mecanismos de controle externo sobre as atividades de inteligência discutidas até aqui, o papel do Congresso como instituição fiscalizadora do Poder Executivo adquire centralidade justamente porque o Legislativo é considerado o poder mais representativo nas democracias. Assim, antes de concluir esta seção é preciso discutir o grau de controle efetivo que o Congresso tem sobre as atividades de inteligência, além de problematizar a premissa segundo a qual os parlamentares são melhores agentes dos cidadãos do que os burocratas, os presidentes, os juízes ou a mídia, em se tratando dessas áreas de políticas públicas.

Segundo Adam Przeworski (1985:80-86), o imperativo da renovação periódica dos mandatos e a proximidade maior com os eleitores influenciam fortemente os parlamentares a agirem como agentes dos representados. Por outro lado, é preciso lembrar que os resultados das eleições dependem ainda dos sistemas eleitorais e partidários, da organização interna do processo legislativo e da dinâmica política que tende a neutralizar parcialmente as eleições como mecanismos representativos (como vimos no item *Eleições*). Além disso, as preferências dos parlamentares estão longe de se esgotar na preferência intermediária e decisiva da renovação do mandato. Pelo contrário, existe um amplo leque de situações nas quais os parlamentares agem segundo suas próprias preferências e não segundo as preferências dos eleitores. Em especial, não existe nenhuma relação necessária e direta entre o interesse geral dos cidadãos num governo ágil e transparente e uma atuação específica dos parlamentares na supervisão de qualquer agência executiva que não esteja sob os holofotes de uma crise política ou administrativa imediata. Finalmente, mesmo que a supervisão sistemática dos órgãos do Poder Executivo seja do interesse dos cidadãos e os parlamentares ajam como agentes perfeitos do público em relação a essa preferência, resta saber se o Congresso como instituição é capaz de realizar tal supervisão satisfatoriamente.

Ao contrário da hipótese adotada por autores como William Niskanen (1977) e outros expoentes da teoria da escolha pública (*public choice*)

sobre o excessivo insulamento burocrático das agências governamentais e a precária supervisão congressual como causas do crescimento ineficiente do gasto público e da conseqüente oferta de um nível subótimo (excessivo) de serviços governamentais, trabalhos neo-institucionalistas como os de Terry Moe (1990) e outros já demonstraram que os poderes legislativos são capazes, especialmente através de suas comissões, de exigir informações das agências do Poder Executivo e formular suas próprias preferências sobre gastos e níveis de *output*. Quando as burocracias governamentais são forçadas a revelar seus custos reais ou qualquer escala de oferta de serviços, o Congresso pode garantir que o nível de atividade governamental seja mais próximo das suas preferências do que supunham os modelos anteriores.<sup>88</sup>

Mesmo concordando com isso, Amy Zegart (1999:1-53) demonstrou a necessidade de uma especificação mais precisa das condições institucionais e contextuais que afetam as interações entre o Congresso e diferentes tipos de burocracias. No caso das chamadas agências governamentais de segurança nacional (ministérios de relações exteriores, Forças Armadas, serviços de inteligência e de segurança etc.), as mesmas premissas neo-institucionalistas conduziram a autora a conclusões bastante distintas sobre a capacidade de o Congresso efetivamente controlar os órgãos governamentais.

Para Zegart, os parlamentares tendem a evitar o envolvimento em atividades de supervisão das agências de segurança nacional porque tais atividades envolvem altos custos transacionais para a obtenção de informações e muitos conflitos para construir a autoridade necessária ao exercício efetivo da supervisão. Devido ao segredo governamental e à baixa densidade de grupos de interesse atuando nessa área na sociedade civil, o tempo de construção de laços de confiança e do conhecimento especializado necessários para uma atuação relevante é simplesmente demais para parlamentares que precisam “mostrar serviço para seus eleitores”, tendo em vista o imperativo intermediário da renovação do mandato ou da progressão na carreira política. Além dos custos serem elevados, o retorno esperado é baixo, pois a segurança nacional é um bem público (*public good*), e isso reduz as oportunidades de ganho político individual associadas à lógica distributiva de funcionamento do Congresso (*logrolling e pork-barrel*). Afinal, como se trata de áreas de políticas públicas sob domínio constitucional e historicamente reafirmado do Poder Executivo, qualquer ação dos congressistas para reduzir dotações orçamentárias, criar ou eliminar órgãos, modificar seu desenho organizacional ou limitar a liberdade de manobra dos governantes envolve o risco de acusações de que o Legislativo está enfraquecendo a capacidade de defesa militar e política dos interesses e da segurança da nação.

Portanto, os parlamentares que tendem a se envolver de forma duradoura e especializada com temas de política externa e segurança nacional

são aqueles que pretendem um dia concorrer a cargos no governo ou que têm vínculos com grupos de interesse que são relevantes em sua região eleitoral (ex.: os empregados de uma fábrica de satélites em sua *constituency*), ou ainda aqueles que têm preocupações normativas e preferências associadas à segurança enquanto um bem público. Mesmo que esses parlamentares tenham incentivos eleitorais para fazer da supervisão sobre as agências de inteligência uma alta prioridade dos seus mandatos, eles são poucos e em qualquer legislatura e dificilmente utilizarão seu capital político para tentar mobilizar o Congresso ou os demais parlamentares que não compartilham a mesma agenda temática. O argumento geral de Zegart é plausível, mas não elimina a necessidade de um comentário específico sobre a dinâmica de trabalho dos comitês de inteligência do Congresso.

No contexto institucional dos Estados Unidos, a supervisão congressual sobre as atividades de inteligência (e sobre a área de segurança nacional, de modo geral) baseia-se em algumas capacidades constitucionais e políticas bastante específicas.<sup>89</sup> Dada a centralidade das comissões temáticas na organização do processo legislativo no Congresso, a maioria dos exemplos será retirada diretamente da experiência dos comitês de inteligência do Senado (Senate Select Committee on Intelligence – SSCI) e da Câmara de Representantes (House Permanent Select Committee on Intelligence – HPSCI), instituídos respectivamente em 1976 e 1977.<sup>90</sup>

As principais bases da supervisão congressual incluem: 1. A autoridade legislativa propriamente dita e a autorização anual do orçamento. 2. A autoridade para aprovar tratados internacionais e requerer relatórios e informações ao Poder Executivo. 3. O poder para confirmar a nomeação de indivíduos indicados pelo presidente para certos cargos. 4. A autoridade para convocar audiências e testemunhos (*hearings*) e iniciar investigações sobre temas considerados relevantes.<sup>91</sup>

Com exceção do National Security Act of 1947 e suas sucessivas emendas, a maior parte das regulações sobre a atividade de inteligência nos Estados Unidos é feita através de Executive Orders e outras diretrizes administrativas. Entretanto, em ocasiões diversas ao longo da segunda metade do século XX o Congresso aprovou legislação adicional sobre pontos mais específicos (*miscellaneous legislation*).<sup>92</sup> O Congresso controla a aprovação (*authorization*) do orçamento anual e, num estágio subsequente, a definição dos recursos que serão alocados para cada programa específico (*appropriation*). A cada ano fiscal, uma lei de autorização deve ser aprovada antes que as agências governamentais possam gastar qualquer dinheiro.<sup>93</sup> Para a área de inteligência, os dois atos legislativos mais importantes são o Intelligence Authorization Act e o Defense Authorization Act, no qual uma boa parte dos recursos é inserida sem identificação (verbas secretas). Ao ana-

lisar e modificar a proposta orçamentária enviada pelo presidente todos os anos, o Congresso pode controlar o tamanho das agências, os detalhes de cada programa e os planos de desembolso. Uma prática comum também é a introdução de mudanças políticas e organizacionais no funcionamento do sistema norte-americano de inteligência utilizando-se como veículo legislativo as leis anuais de autorização de fundos.<sup>94</sup> Como no caso de qualquer outra lei, uma vez aprovadas ao final de um tortuoso processo de tramitação, as leis de autorização orçamentária para o ano fiscal podem ser vetadas pelo presidente, mas isso só ocorre excepcionalmente, em função dos altos custos políticos implicados.<sup>95</sup>

A Constituição dos Estados Unidos prevê que a ratificação de tratados internacionais assinados pelo governo depende da sua aprovação por dois terços dos membros do Senado. Embora a análise dos tratados seja normalmente encaminhada ao Senate Committee on Foreign Relations, o SSCI é rotineiramente envolvido na avaliação de tratados sobre controles de armas e no monitoramento dos mecanismos de verificação (*compliance*). Relatórios secretos e declarações públicas foram emitidos pelo comitê de inteligência do Senado em relação ao Salt II (1979), INF (1988), CFE (1991), Start I (1992) e Open Skies (1993), entre outros. O Judiciário norte-americano também tem interpretado o Poder Legislativo do Congresso, tal como definido pela Constituição (art. I, seção 8), como um poder que envolve a autoridade para requerer acesso a quaisquer informações que o Poder Executivo tenha sob sua guarda. No caso das atividades de inteligência, essa interpretação tem sido motivo de polêmicas recorrentes entre o Congresso e o presidente. Foi o chamado Case Act of 1972 que estabeleceu que cópias do texto completo de todos os acordos internacionais assinados pelo governo (além dos tratados, que requerem constitucionalmente a aprovação do Senado) deveriam ser enviadas ao Congresso. A partir dali, muitas outras requisições sistemáticas de informações e relatórios foram sendo introduzidas nos Estados Unidos. Em especial, o chamado Hughes-Ryan Amendment (1974) estabeleceu pela primeira vez a obrigatoriedade de um relatório formal e por escrito (*presidential finding*) sobre todas as operações encobertas a ser enviado para os comitês de inteligência, Forças Armadas e relações exteriores das duas casas do Congresso. Ainda que disposições posteriores tenham determinado que os *findings* sobre operações encobertas deveriam ser entregues apenas aos comitês de inteligência, de modo geral os requerimentos de relatórios não apenas se tornaram uma praxe do sistema de supervisão congressual das atividades de inteligência como vêm sendo ampliados nos últimos 15 anos.<sup>96</sup>

A terceira fonte de autoridade dos comitês congressuais sobre a *intelligence community* é a exigência legal de que o nome do DCI seja investigado, sabatinado e aprovado pelo Senado. Além do DCI, também é

necessária a aprovação senatorial para uma série de outros cargos, entre os quais destacam-se os cargos de deputy director of Central Intelligence (DDCI), CIA inspector general (IG), deputy director of Central Intelligence for Community Management (DDCI/CM) e assistant director of Central Intelligence for Administration (ADCI/A).

Até 1977, o processo de nomeação tendeu a ser burocrático e sem maiores controvérsias, mas desde então alguns ex-futuros DCIs indicados pelo presidente retiraram seus nomes como resultado das audiências congressuais ou por antecipação a um veto resultante do processo de argüição e investigação da vida pregressa. Apenas para mencionar alguns exemplos, em 1977 Theodore Sorenson retirou sua indicação quando senadores do SSCI levantaram críticas quanto ao fato de Sorenson ser um objetor de consciência e também por alegações de utilização imprópria de material classificado em suas memórias. Em 1987, durante sua primeira indicação para ser DCI, Robert Gates retirou a indicação depois de ter sido questionado sobre seu envolvimento no escândalo Irã-Contras. Mesmo tendo sido confirmado pelo Senado em sua segunda indicação em 1991, Gates enfrentou uma investigação sobre as alegações de que teria “politicizado” as análises de inteligência quando foi diretor de análise da CIA durante as administrações Reagan e Bush. Mais recentemente, em 1997 o ex-assessor de Segurança Nacional de Bill Clinton, Anthony Lake, foi forçado a retirar sua indicação para ser DCI antes mesmo de iniciar o processo de argüição no Congresso. Crescentemente partidário e relacionado com aspectos da vida dos indicados que não têm relação direta com o cargo a ser ocupado, o processo de confirmação senatorial é um recurso de poder significativo para o comitê de inteligência do Senado.<sup>97</sup>

Finalmente, os comitês de inteligência do Senado e da Câmara (House of Representatives) podem convocar audiências públicas e secretas, iniciar investigações parlamentares sobre temas controversos e elaborar relatórios próprios de avaliação sobre aspectos estruturais e políticos das atividades de inteligência do governo. Algumas dessas audiências são realizadas para discutir as opiniões dos parlamentares, do governo e de especialistas sobre aspectos da política de inteligência (ex.: as audiências realizadas em 1994 no comitê de inteligência da Câmara para tratar da pertinência ou não da divulgação pública do agregado orçamentário de inteligência), enquanto outras são destinadas à discussão de temas internacionais considerados relevantes para a segurança nacional (ex.: as audiências anuais promovidas pelo comitê de inteligência do Senado para que os diretores da CIA, DIA, FBI e de outras agências exponham sua visão sobre as ameaças internacionais contra os interesses e a segurança dos Estados Unidos). As investigações e relatórios especiais fazem parte da própria gênese dos comitês de inteligência do Congresso, à época das comissões Church (Senado) e Pike (Câmara)

para investigar as operações do governo na área de inteligência. Apenas para mencionar um exemplo mais recente, em 1998 o comitê de inteligência do Senado realizou duas investigações sobre a China, uma sobre as alegações de que o governo chinês realizou operações de influência durante a eleição presidencial de 1996 e a outra investigação sobre os possíveis impactos sobre a segurança dos Estados Unidos resultantes da transferência de tecnologia de satélites para a China. Essas audiências e investigações representam parte considerável do controle externo das atividades de inteligência por parte do Congresso dos Estados Unidos. Em 1997/98, somente o SSCI realizou 95 desses *hearings* formais, principalmente secretos, mas também alguns abertos ao público.<sup>98</sup>

Apesar dessas capacidades formais e de um desempenho que vem sendo aperfeiçoado nos últimos 15 anos desde o escândalo Irã-Contras, autores como Pat Holt (1995), Mark Lowenthal (2000) e Loch Johnson (1996) destacam algumas limitações importantes e desafios recorrentes no funcionamento dos mecanismos congressuais de supervisão (*oversight*) e prestação de contas (*accountability*). Entre os desafios mais relevantes e que não se restringem necessariamente ao caso norte-americano, deve-se destacar:

1. Os limites impostos pelo segredo governamental e os problemas de segurança.
2. O risco de cooptação dos parlamentares.
3. O chamado microgerenciamento das atividades de inteligência.
4. A avaliação da qualidade do trabalho parlamentar.

A instituição do segredo público e as necessidades de segurança operacional e informacional da atividade de inteligência impõem custos transacionais à supervisão congressual. Essa premissa geral, já discutida por Amy Zegart (1999), é verificável até mesmo na legislação que estabelece a obrigatoriedade do fornecimento de informações ao Poder Legislativo. No caso norte-americano, enquanto uma seção da lei afirma que nenhuma informação deve ser retida sob a alegação de que constituiria uma publicização indevida de informações classificadas, a seção seguinte diz que os comitês de inteligência do Congresso devem ser mantidos completamente informados das atividades, organizações, sistemas e recursos de inteligência do Poder Executivo “na extensão em que isso seja consistente com a proteção contra a divulgação indevida de fontes e métodos ou outros materiais excepcionalmente sensíveis”.<sup>99</sup> Na prática, esse requisito de consistência obriga a existência de procedimentos de checagem de *background* para os parlamentares e assessores dos comitês para a concessão de credenciais de acesso (*security clearances*), a construção de instalações físicas e procedimentos para a armazenagem e trato de informações classificadas e severas limitações sobre a disseminação de inteligência para os demais membros do Congresso, o que coloca um peso adicional sobre os parlamentares que atuam nas

comissões. Com tudo isso, o Congresso é visto ainda como uma fonte de vazamentos indevidos de informações, embora isso seja fortemente disputado no caso dos Estados Unidos, onde a maioria dos vazamentos se dá no Poder Executivo. Em muitos casos, certas atividades de inteligência são relatadas apenas oralmente para os presidentes de cada comitê (*chairmen*) e eles devem então decidir pelo Congresso como um todo se alguma ação de controle é ou não necessária.

Além dos limites impostos pelo segredo e por pesados procedimentos de segurança, a efetividade da supervisão congressual pode ser comprometida também pela cooptação dos parlamentares para uma visão acrítica e condescendente em relação às práticas e justificações das agências de inteligência do Poder Executivo. Na medida em que os custos de obtenção de informações e de construção da especialização necessária para um trabalho efetivo de supervisão são muito altos, o risco que se coloca é o do parlamentar ou do assessor ser ostensivamente cooptado ou, mais simplesmente, adotar uma posição excessivamente compreensiva (no sentido de se colocar no lugar do outro, num ato de *verstehen* peculiar). Ainda mais quando as restrições de segurança e a relação intensa de trabalho com os dirigentes dos órgãos governamentais de inteligência (o tipo de camaradagem que os britânicos chamam de “*ring of secrecy*”) tendem a ser utilizadas pelos últimos para avançar suas relações públicas com o Congresso. As medidas para minimizar o risco de cooptação envolvem a fixação de limites temporais para que um parlamentar possa ser membro de uma comissão supervisora de inteligência e um desenho institucional multipartidário e que aumente a responsabilidade dos membros em relação às prerrogativas do presidente da comissão.

Na verdade, o nível apropriado de supervisão congressual que interessa aos cidadãos é difícil de ser estabelecido, se este não é um tema proeminente na agenda eleitoral, nas campanhas de rua ou nas pesquisas de opinião. Um terceiro tipo de risco é o chamado microgerenciamento, uma tendência a focar o trabalho investigativo dos comitês parlamentares em detalhes operacionais de uma área ou em casos específicos e desconsiderar os temas mais gerais e substantivos do desempenho do sistema nacional de inteligência como um todo. Mas isso é controverso, pois, como lembra Pat Holt (1995:231), o que para uns é microgerenciamento para outros é o zelo necessário a um trabalho de supervisão do qual depende a *accountability* de uma área problemática de atuação do Estado contemporâneo.<sup>100</sup>

Finalmente, qualquer comentário sobre a efetividade dos comitês parlamentares de supervisão precisa levar em conta a intensidade e a qualidade das questões levantadas pelos parlamentares durante suas interações com os dirigentes das agências de inteligência. Ou seja, é preciso avaliar aquilo que Frank Smist (1991) chamou um tanto enviesadamente de atitudes institu-

cionais *versus* atitudes investigativas na supervisão congressual. Tomando os *hearings* públicos sobre a CIA como uma medida formal de *accountability* na área de inteligência, Loch Johnson (1996:89-118) estudou a participação dos parlamentares membros dos comitês de inteligência da Câmara e do Senado nessas audiências. Entre 1976 e 1990, a freqüência média de realização dessas audiências públicas foi de 1,6 por ano, somando-se os dois comitês. Em menos de um terço das audiências a maioria dos membros do comitê esteve presente. Das mais de 10 mil perguntas feitas pelos membros dos comitês nessas audiências, apenas 39% das questões levantadas pelos senadores e 36% das questões dos representantes foram perguntas consideradas por Loch Johnson como interrogativas, adversariais ou que demandavam evidências e argumentos mais elaborados (*hardballs*). As demais foram perguntas marcadas por deferência e/ou irrelevância (*softballs*). Mesmo reconhecendo a insuficiência desse estudo para uma avaliação mais integral da experiência norte-americana de supervisão congressual, as conclusões de Loch Jonhson parecem reforçar a idéia de que um dos principais problemas com os mecanismos horizontais de *accountability* democrática na área de segurança nacional é a própria disposição dos parlamentares de se informarem e atuarem mais decisivamente.<sup>101</sup>

Muito mais do que uma peculiaridade dos comitês norte-americanos, esses problemas são gerais e tendem a ser relatados em diferentes trabalhos sobre supervisão congressual e *accountability* horizontal das atividades de inteligência e que focam casos como o do Canadá, Grã-Bretanha, Austrália, Escandinávia, África do Sul e Argentina. Embora isso seja insuficiente para conferir solidez comparativa à tese de Amy Zegart (1999), inclusive porque se observa um desenvolvimento institucional importante ao longo da última década através da formação de comitês conjuntos de inteligência e segurança em muitos legislativos bicamerais, os problemas identificados aqui mostram como ainda se está longe de contar com um sistema de supervisão congressual efetivo sobre as atividades de inteligência e de segurança nacional nas democracias.

Em síntese, dos sete mecanismos de supervisão e controle externo discutidos nesta seção, os mais efetivos são os mecanismos internos ao próprio Poder Executivo (mandatos legais, inspetorias e mecanismos de coordenação) e os comitês parlamentares especializados em temas de inteligência, defesa e política externa. Mesmo sendo desejável um investimento institucional específico na melhoria do desempenho dos sete tipos de controle externo, os comitês parlamentares são mais decisivos especialmente quando têm capacidade de aprovar legislação mandatória, decidir sobre os orçamentos e verificar com independência quaisquer documentos e informações solicitadas.

## A transparência como um desafio

A habilidade de controlar fluxos e acervos informacionais é decisiva para a maximização de poder. No caso da atividade de inteligência, as informações relevantes sobre a atividade das agências não estão disponíveis diretamente para o público, e sua disseminação é regulada pelo segredo governamental. Essas informações militares, econômicas e outras informações sobre ameaças podem ser decisivas para a segurança nacional. E tudo isso confere poder para quem dirige o sistema. Como já disse alguém, se for verdade que o poder corrompe e o poder absoluto corrompe absolutamente, então o poder secreto corrompe secretamente, e deve por isso ser cuidadosamente limitado e supervisionado.<sup>102</sup>

Em *polities* democráticas, os serviços de inteligência e segurança recebem poderes extraordinários para proteger as liberdades, os valores e os interesses dos cidadãos. Precisamente por causa desses poderes, tais serviços podem causar danos a essas mesmas liberdades e às instituições democráticas. Por controlar um importante corpo de informações, por ter especialização em técnicas de vigilância e interceptação de comunicações e por operar uma grande quantidade de recursos sob um manto de segredo, um aparato de inteligência pode se transformar numa ameaça para o governo a que serve e para os cidadãos do próprio país. Num extremo da curva de risco está a instrumentalização dos serviços de inteligência por parte de um governo ou de um dirigente, que poderia utilizá-lo contra seus oponentes políticos internos ou segmentos mais ou menos vastos da população, enquanto no outro extremo da curva está o risco de autonomização dos serviços e sua transformação em centros de poder independentes no sistema político.

De modo geral, as leituras realizadas sugerem que os serviços de inteligência são razoavelmente responsivos aos governantes. Ou seja, que muitos dos abusos e escândalos associados à área de inteligência têm origem nas próprias diretrizes operacionais emanadas dos governantes e comandantes. Além disso, como a doutrina da “negação plausível” diz basicamente que as ações na área de inteligência devem ser conduzidas de modo a permitir ao governo negar seu envolvimento, aprovação ou mesmo o conhecimento das operações para evitar desgastes diplomáticos e crises internacionais, a operação desse mecanismo tende a reforçar a convicção de que os governantes controlam mais efetivamente os serviços de inteligência e segurança do que eles dizem ou parecem controlar. Daí que o risco maior se encontra na ameaça às liberdades dos cidadãos em função da instrumentalização dos serviços por governantes, e não na autonomização dos serviços. Mesmo assim, devido aos recursos tecnológicos e à escala em que operam tais sistemas de inteligência nos países mais industrializados, aos problemas do segredo compartimentado juntou-se progressivamente o peso da tecnocracia, desta-

cado em particular por John K. Galbraith em *O novo estado industrial* (1979). Juntos, o segredo e a tecnologia tendem a constituir um grande desafio para o controle público das atividades de inteligência, mesmo nas poliarquias mais institucionalizadas.<sup>103</sup>

Essas duas dimensões – o segredo e a tecnologia de controle dos eventos políticos – compõem aquilo que Norberto Bobbio (1989:399-415) chama de “poder invisível”, que corromperia a idéia democrática a ponto de impedir, no limite, que se possa dizer que a democracia existe onde existem serviços de inteligência.<sup>104</sup> Mesmo deixando de lado aqui a discussão mais geral sobre o grau de afastamento entre as poliarquias “realmente existentes” e os ideais democráticos, o fato de países norte-americanos e europeus ocidentais – considerados entre os mais democráticos do mundo segundo quaisquer padrões – contarem com serviços de inteligência mais ou menos poderosos indica duas coisas diferentes: por um lado, que a mera presença de serviços de inteligência não viola as condições institucionais de existência da poliarquia.<sup>105</sup> Por outro lado, que isso está longe de significar que o recurso a essas atividades seja isento de problemas, dilemas, tensões e situações de perda de controle mesmo naqueles países.<sup>106</sup>

Por tudo isso, o tema do controle externo sobre as atividades de inteligência é inescapável e central. Nos regimes democráticos atualmente existentes, como foi visto neste capítulo, esse controle é exercido não pelos cidadãos individualmente ou mesmo pelo conjunto de representantes parlamentares, mas por comissões especiais, corregedorias e comitês com regras de funcionamento especiais. No caso do Poder Executivo, trata-se mais da supervisão dos mandatos legais das agências e do controle administrativo sobre a eficiência no cumprimento de missões e prioridades. No caso da supervisão congressual ou parlamentar, são as próprias missões e prioridades das agências de inteligência que precisam ser questionadas, supervisionadas e legitimadas.

Embora as noções de interesse nacional e de segurança nacional (que justificam em última análise as atividades de inteligência) não possam ser concebidas por governantes democráticos nos mesmos termos que a *Raison d'etat* do Antigo Regime, existem novas razões práticas e morais para a tensão entre segurança estatal e segurança individual. Algo semelhante ocorre com os segredos, que já não correspondem aos *arcana imperii* dos reis absolutistas, uma vez que se trata agora de uma forma relativamente excepcional de regulação governamental de fluxos de informações. Entretanto, como essa excepcionalidade é parcialmente neutralizada pela escala em que essa forma de regulação é empregada, surgem novas tensões entre segredo governamental e direito à informação.<sup>107</sup>

Assim, mesmo reconhecendo a validade e até a vitalidade para as justificativas associadas à segurança estatal e ao segredo governamental no mundo pós-

Guerra Fria, o ponto central deste capítulo é a necessidade de uma maior efetividade dos mecanismos externos de controle sobre o Poder Executivo nessa área problemática de atuação governamental. Infelizmente, tanto do ponto de vista dos modelos institucionais e dos procedimentos mais adequados e efetivos para a supervisão externa das atividades de inteligência quanto do ponto de vista da reflexão sobre os problemas éticos associados à segurança nacional, à espionagem internacional, ao segredo governamental, ao uso de operações encobertas e aos acordos secretos entre governos para compartilhamento de inteligência, a discussão sobre o impacto das atividades de inteligência tendeu a ser subestimada até aqui na teoria democrática.<sup>108</sup>

Trata-se de uma lacuna significativa, pois, como foi discutido na terceira seção deste capítulo, mesmo nos países mais democráticos os mecanismos de supervisão congressual são muito recentes e têm evidentes problemas de desempenho institucional. Na medida em que a institucionalização dos serviços de inteligência envolveria não apenas a obtenção de “estabilidade” organizacional, mas também um longo processo através do qual eles se tornam (ou não) organizações “valiosas” para o público, esse é um processo que está fortemente relacionado à transparência, ou seja, à capacidade de o público ver e julgar por si mesmo os atos dos governantes na área de inteligência. Mesmo que os serviços de inteligência contemporâneos se tornem suficientemente ágeis para se estabilizarem organizacionalmente no novo contexto internacional, sua eventual institucionalização dependerá ainda da difícil resolução do dilema da transparência.

## Notas

1. Para um primeiro aprofundamento sobre temas de segurança nacional, ver Buzan (1991). Ver também Buzan, Wæver & Wilde (1998). E ainda Adler & Barnett (1998, especialmente os ensaios de Ole Wæver, Charles Tilly e Andrew Hurrell). No contexto brasileiro, ver Proença Jr., Diniz & Raza (1999). E também Proença Jr. & Diniz (1998).
2. A estrutura geral do argumento a respeito da democracia como resultado contingente de conflitos aparece formulada em Przeworski (1984).
3. Ou bem essa busca de segurança absoluta é irrelevante do ponto de vista prático, ou bem ela implica uma pretensão autoritária de controle sobre variáveis contextuais e sobre a atuação dos atores. De qualquer modo, a seguinte passagem no documento oficial de doutrina da Escola Superior de Guerra do Brasil me parece exemplarmente equívocada: “Os assuntos de Segurança abrangem tanto o chamado universo antagônico (antagonismos), aquele onde ocorrem atitudes dolosamente contrárias aos esforços orientados para o alcance e preservação dos Objetivos Nacionais Permanentes, como o não-antagônico (fatores adversos). Tudo o que pode ameaçar a tranquilidade do homem, dificultar ou impedir a proteção que julga ser um direito seu, causar temores, e o que é capaz de gerar conflitos, constituem as chamadas

razões de insegurança.” Brasil, Escola Superior de Guerra (1999:155). Na verdade, insegurança, no contexto dos Estudos Estratégicos, diz respeito apenas às ameaças e percepções de ameaça contra a existência do “objeto”, sua sobrevivência física, sua identidade simbólica ou sua autonomia. O problema de se saber quando uma ameaça é séria o suficiente para configurar uma ameaça existencial será discutido ao final deste texto.

4. Sobre a natureza multiétnica do Estado nacional moderno, ver Gellner (1993). Ver também Buzan (1991:57-111) e, principalmente, o capítulo 4 (Os Estados e seus cidadãos), do livro já citado de Charles Tilly (1996:157-193).

5. Integração aqui significa coerência (entre fins e meios) e congruência (entre o todo e as partes) nas políticas públicas setoriais. Mas, principalmente, integração não supõe a criação de qualquer tipo de “superministério da segurança nacional” que subordine hierarquicamente as organizações de inteligência, as forças policiais e as Forças Armadas sob um único comando, pois tal concentração de poder é claramente incompatível com qualquer arranjo democrático. Ver Proença Jr. & Diniz (1998:55-56).

6. A referência obrigatória aqui é a conhecida definição de Max Weber sobre o Estado como a agência humana que detém o monopólio do uso legítimo da força. Cf. Weber (1992 e 1993a).

7. Sobre os diversos usos da noção de subversão na Grã-Bretanha, Canadá e Austrália, ver Lustgarten & Leigh (1994:395-410).

8. Um autor bastante orientado para a justificação das políticas de segurança norte-americanas e que destaca o papel do crime organizado e do islamismo militante como forças políticas que afetam a segurança de Estados operando em bases transestatais é Godson (1997).

9. Novamente, a formulação doutrinária oficial da Escola Superior de Guerra do Brasil torna-se no mínimo irrelevante e no máximo perigosa, na medida em que supõe que termos como nação, bem comum, poder nacional e objetivos nacionais permanentes têm significado unívoco, auto-evidente e atemporal, quando na verdade eles representam resultados provisórios e sempre cambiantes dos conflitos de interesse e de opinião na sociedade. A definição oficial de segurança nacional da ESG é a seguinte: “Segurança Nacional é a garantia relativa, para a Nação, da conquista e manutenção dos seus objetivos permanentes, proporcionada pelo emprego do seu Poder Nacional. (...) Quando se trata de ameaças de qualquer origem, forma ou natureza situadas no domínio das relações internacionais, o problema é de Segurança Externa. Quando se trata de ameaças que possam manifestar-se ou produzir efeitos no âmbito interno do país, o problema é de Segurança Interna”. Brasil (1999:158). Além do texto já citado de Proença Jr. & Diniz (1998:55-62), ver também, dos mesmos autores, a crítica mais extensa sobre a falácia envolvida em proposições como “dilema de segurança” e “corrida armamentista”, que supõem implicitamente que a mera existência de Estados soberanos e Forças Armadas implicaria uma “lógica da guerra” separada da política, das intenções, gestos e conflitos concretamente existentes. Ver Proença Jr. & Diniz (2001).

10. Segundo Barry Buzan (1991:52-55), indivíduos e pequenos grupos afetam substancialmente a segurança nacional de quatro formas: 1. como desafiadores do poder de Estado – “subversivos”; 2. como apoiadores de causas estrangeiras – “quinta-coluna”; 3. como fontes de influência sobre as políticas governamentais – “elites” e “opinião

pública"; 4. como líderes e governantes -- "Chamberlain versus Churchill". Nesses casos, os indivíduos não são "objetos" referentes, mas sim o que Buzan, Wæver e Wilde (1998: 35-42) chamam ou de *securitizing actors* ou de *functional actors*. A diferença entre os dois tipos de ator reside no fato de os primeiros serem aqueles que reivindicam que certo tema seja tratado como um problema de "segurança nacional", enquanto os atores funcionais são aqueles que aquiescem ou não com a reivindicação dos primeiros. Por sua vez, *referent objects* são as coisas e pessoas cuja segurança estaria sendo ameaçada.

11. As premissas sobre o sistema internacional que informam essa discussão sobre segurança nacional estão baseadas na abordagem estrutural do neo-realismo formulada originariamente em Waltz (1979) e também em Waltz (1993). Segundo o próprio Kenneth Waltz vem afirmando desde 1959, os problemas de segurança só podem ser exaustivamente compreendidos a partir das causalidades recíprocas entre os três níveis de análise (indivíduo, Estado e sistema). No entanto, isso é absolutamente compatível com a tese fundamental de Waltz (1979) sobre a importância decisiva do nível sistêmico-estrutural. Como disse o autor respondendo às críticas de Robert Keohane (*Theory of world politics: structural realism and beyond*) e de outros em seu texto de 1986 (*Reflections on theory of international politics: a response to my critics*), a abordagem sistêmica não explica tudo em política internacional, apenas o essencial. Ou seja, mantendo-se a consistência com a premissa fundamental sobre a anarquia internacional, é necessário e possível avaliar como as diferentes capacidades das unidades do sistema (inclusive os recursos militares e de inteligência) alteram a distribuição de poder no plano sistêmico. Ver Keohane (1986:158-203 e 322-345).

12. Sobre os atributos da soberania em termos de autoridade e controle, ver Thomson (1995:213-233) e também o recente e polêmico Krasner (1999).

13. Cf. o capítulo XIII (Da condição natural da humanidade relativamente à sua felicidade e miséria) em Hobbes (1974). Para um comentário didático sobre os graus de legitimidade das pretensões de obtenção de obediência por parte dos governantes, indo desde o consentimento baseado no medo da sanção até a concordância normativa ideal, passando pela aquiescência pragmática, ver Held (1995).

14. "*This is because the means by which order is maintained and foreign forces are kept at bay may themselves be as destructive of personal security as those threats which obsessed Hobbes. For every Bosnia or Somalia there have been ten polities in which the population has been brutalized by internal repression and dictatorship, often justified by some ideology or self-serving slogan like communism, anti-communism, or supremacy of some ethnic group or religious dogma*" (Lustgarten & Leigh, 1994:7).

15. Sobre repressão e negociações de direitos na trajetória do Estado moderno, ver Tilly (1996:160-166).

16. Buzan (1991:44-50).

17. Dois exemplos históricos de medidas de segurança consideradas retrospectivamente excessivas e que foram tomadas por regimes democráticos são: 1. a decisão de confinar estrangeiros residentes e cidadãos de descendência japonesa, italiana e alemã suspeitos de simpatia pelo Eixo durante a II Guerra Mundial na Grã-Bretanha e nos Estados Unidos; 2. a invocação do Ato de Medidas de Guerra pelo governo conserva-

dor do Canadá em 1970, colocando toda a província de Quebec sob lei marcial após um atentado terrorista ter vitimado o ministro do Trabalho da província e o adido comercial britânico. Os exemplos poderiam multiplicar-se. Ver Lustgarten & Leigh (1994: 16-19).

18. Nesse caso, não bastaria a suposição de que os governantes têm “boas razões” para propor as medidas de segurança excepcionais, pois eles seriam chamados a demonstrar essas razões, substituindo uma relação assimétrica de autoridade por uma relação igualitária de persuasão. Justamente a coerção (um recurso de última instância) seria trazida para o espaço da discussão política e “obrigada” a justificar-se em termos morais e de eficácia. Sobre as dificuldades não antecipadas por essa proposição, associadas às formas burocratizadas de exercício da autoridade no mundo moderno, ver Reis (1997: 60-69).

19. *Constituição da República Federativa do Brasil*. Ver o Título V (Da Defesa do Estado e das Instituições Democráticas), Capítulo 1 (Do Estado de Defesa e do Estado de Sítio).

20. Para Carl Schmitt (1996:93), a “tendência do Estado de direito de regulamentar detalhadamente o Estado de exceção representa a tentativa de circunscrever o caso no qual o direito se suspende a si mesmo”. Mas essa tentativa não elimina a discussão política sobre o que constitui o interesse público, a segurança nacional etc. Como se sabe com base na conhecida proposição jurisprudencial de Schmitt sobre a dependência da ordem legal em relação ao caso excepcional: “soberano é quem decide sobre o Estado de exceção”. A crítica de Lustgarten & Leigh (1994:19-20) a Schmitt baseia-se no mesmo argumento de Jürgen Habermas (1994b) contra o jurista alemão de Weimar e por algum tempo colaborador do regime nazista, sobre a falta de proporcionalidade entre a ameaça e a resposta defensiva. Medidas excepcionais para preservar a segurança estatal, segundo esses autores, sempre tenderiam a aproximar-se da situação na qual se coloca um “cão pit-bull terrier para tomar conta do jardim de infância”. A própria analogia dá uma noção sobre a fragilidade do consenso liberal diante de situações de conflito substantivo envolvendo o uso dos meios de força. A Constituição certamente não é um pacto suicida, mas também não é simplesmente suspender a e definir politicamente as condições da “excepcionalidade” e as prerrogativas dos órgãos coercitivos do Estado nessas situações. Para uma visão sintética do argumento habermasiano contra Schmitt, ver Habermas (1994b).

21. Além dos textos já citados de Proença Jr. & Diniz (1998 e 2000), nos quais aparece formulada a crítica da renúncia das elites políticas brasileiras em discutir temas de segurança e defesa nacional, ver também – para uma crítica adicional dos discursos de segurança pretensamente baseados na defesa dos direitos humanos e que incorrem em proposições messiânicas e autoritárias para o combate contra a criminalidade e a degradação da ordem pública – o artigo de Diniz (2000). Disponível em: <<http://cevep.ufmg.br/bacp>>.

22. Esse é um dos problemas dos novos regimes democráticos em vários lugares do mundo, inclusive no Brasil. Para uma consideração crítica da hipótese sobre a identidade entre democracia e paz, ver Hurrell (1998). A situação atual do debate teórico sobre a relação entre guerra e democracia encontra-se resumida em Dougherty & Pfaltzgraff (1997:341-366).

23. Enfim, para dizê-lo de outra forma, se poucas pessoas discordariam que a repressão do governo chinês na praça da Paz Celestial em 1989 degradou a situação dos direitos humanos naquele país, é muito menos evidente que aquelas mesmas medidas repressivas venham a solapar ou estejam solapando a segurança estatal da China, mesmo tendo ajudado a salvar *in extremis* o regime. Apesar do enorme custo para os indivíduos e grupos afetados, ou mesmo para o prestígio internacional da liderança de Pequim, a escala atual de violações de direitos humanos na China não tem implicações diretas sobre o grau de segurança do Estado. Mesmo o colapso da Alemanha Oriental como entidade estatal em 1989 constitui um exemplo ambíguo. A escala de violação de direitos individuais pelo regime comunista certamente foi vasta e de fato erodiu as bases de legitimização do regime a um ponto crítico, mas tão importante quanto isso foi a decisão soviética de abandonar a DDR como tentativa de obter o apoio econômico da RFA para as políticas de *Glasnost* e *Perestroika* de Gorbachev. A própria União Soviética em 1991 poderia ser uma corroboração mais forte da hipótese sobre a impossibilidade de gestão autoritária de sociedades complexas, não fosse o fato de o regime dirigido pelo Partido Comunista ter durado mais de 70 anos e ter implodido sem uma participação popular significativa. Sobre as causas e dinâmicas das revoluções modernas, ver Cepik (1999:129-162). Para uma discussão analiticamente mais ambiciosa – e mais otimista – sobre a relação entre complexidade social e governo democrático, ver Bruno Reis (1997:80-112).

24. Salvo nos casos em que os países encontram-se em situação pré-revolucionária ou que a extensão da violência letal entre civis não-combatentes configurar o que alguns autores chamam de “*failed states*” (Buzan, 1991:51).

25. Lipschutz (1995). Nesse volume, ver principalmente os textos de James Der Derian (*The value of security: Hobbes, Marx, Nietzsche, and Baudrillard*) e Ole Wæver (*On securitization and desecuritization*). Para um balanço simpático da produção mais recente das abordagens intersubjetivas na área dos estudos de segurança, ver Derian (1998).

26. Escrito como um *policy paper* para a agência canadense de ajuda internacional (Cida), o artigo do professor Jean Daudelin é muito lúcido e, embora simpático ao uso do termo *human security*, destaca os riscos envolvidos nessa tentativa de ampliação da agenda. Ver Daudelin (1999).

27. Mudanças ambientais podem ter consequências adversas para a segurança estatal. Disputas sobre recursos naturais não-renováveis ou dificilmente renováveis, tais como mananciais aquíferos, reservas petrolíferas ou estoques pesqueiros, podem redundar em confrontos diretos entre Estados. Além disso, mudanças climáticas globais – aquecimento da temperatura média da Terra, perdas da camada de ozônio, desflorestamento, degradação de terras aráveis, chuva ácida etc. – podem ter impactos mais ou menos diretos sobre a dinâmica dos conflitos internacionais. As implicações do conceito de segurança ambiental variam conforme o nível de análise (sistêmico, estatal ou individual). Portanto, o laime entre segurança e meio ambiente, do ponto de vista adotado até aqui e que entende segurança como resultando da capacidade de neutralizar pela força ameaças vitais, só se estabelece legitimamente quando a degradação ambiental é um *issue* conflitivo e ameaçador na agenda de atores políticos concretos, e não quando se toma meramente o ambiente – a litosfera, a biosfera, a atmosfera e a estratosfera – como “objetos de segurança” em si mesmos. Ver, como exemplo dessa abordagem realista do tema, Terriff

(1997). Para uma visão contrária, ver também o capítulo sobre o setor ambiental dos complexos de segurança em Buzan, Wæver & Wilde (1998:71-93).<sup>1</sup>

28. A defesa da “liberdade”, do “socialismo” ou da “pátria” não eram *slogans* menos generosos no século XX do que a defesa dos “direitos humanos” ou do “desenvolvimento sustentável” no século XXI. Não se trata de ser cínico a respeito de quaisquer horizontes normativos ou valores proclamados pelos atores políticos, mas simplesmente não se pode confundir as políticas declaratórias com as práticas concretas e tomar o que os atores acreditam ser pelo que eles de fato são. Isso sem falar nas consequências não-intencionais e efeitos colaterais de ações perfeitamente bem-intencionadas.

29. Embora pagando um tributo excessivo aos atos de fala e construções sociais intersubjetivas das percepções de ameaça e das justificações de medidas excepcionais, em detrimento da afirmação decisiva dos temas de segurança como temas políticos por excelência, o livro de Buzan, Wæver & Wilde (1998) tem contribuições reais para a análise dos problemas de segurança, em particular a noção de desterritorialização dos complexos de segurança.

30. Sobre os componentes de uma política de defesa e o papel da institucionalidade governamental para a defesa, ver Proença Jr. & Diniz (1998:48-96).

31. Para análises mais detalhadas de complexos regionais de segurança, ver os trabalhos já mencionados de Hurrell (1998:529-546), para o caso da América Latina, de Proença Jr. & Diniz (2001), para o caso da Ásia central, e Buzan (1991:186-221), para a formulação analítica da teoria dos complexos regionais de segurança.

32. Sobre segredo governamental, ver principalmente Shils (1996) e também Scheppele (1988). Juntamente como o livro mencionado de Sissela Bok estes foram os trabalhos teóricos sobre segredo que me pareceram mais relevantes. Um documento primário fundamental é US Government (1997c:103-236).

33. Scheppele (1988:12).

34. A edição original do livro de Edward Shils, *The torment of secrecy*, é de 1956, mas utilizei a reimpressão de 1996, na qual há um texto introdutório de Daniel Patrick Moynihan também bastante útil.

35. Para uma teoria da interpretação legal do sigilo de informações econômicas privadas (propriedade intelectual e direito de patentes), bem como do sigilo para a garantia de privacidade individual e dos limites à revelação de informações sigilosas em processos judiciais, cf. Scheppele (1988:109-320). A juridificação dos segredos privados não me interessa diretamente nesse trabalho sobre segredos públicos na área de segurança nacional, embora considerações sobre os limites do segredo governamental venham a ser feitas incidentalmente, principalmente com base no direito do público à informação governamental e no direito dos indivíduos à privacidade.

36. A conhecida proposição kantiana (“todas as ações relativas aos direitos de outros homens, cuja máxima não é compatível com a publicidade, são injustas”) é um imperativo categórico que redunda, para sermos consistentes com ele, na inaceitabilidade de quaisquer formas de segredo, bem como na inaceitabilidade da existência de serviços de inteligência. A proposição de Kant não se sustenta por questões teóricas. A partir de uma série de contra-exemplos de políticas moralmente corretas e formalmente justas,

mas que não poderiam ser tornadas públicas por implicarem riscos de autodestruição ou incentivos perversos ao comportamento de transgressores (*wicked*) , Luban propõe uma reformulação do princípio de publicidade/transparência nos seguintes termos: “*All actions relating to the right of other human beings are wrong if publicizing their maxim would lead to self-frustration by undercutting the legitimacy of the public institutions authorizing those actions*” Luban (1996:192). Além de fazer uma defesa do princípio de publicidade quase que pela sua negação, essa proposição é muito pouco clara, como reconhece seu próprio autor. Como um todo, porém, o ensaio de Luban é bastante provocativo e procura escapar consistentemente do beco sem saída de uma defesa transcendental do princípio de publicidade. Ver Luban (1996). A versão kantiana do princípio da publicidade é enunciada no segundo apêndice ao ensaio sobre a Paz Perpétua, chamado de Sobre o acordo entre política e moral segundo uma concepção transcendental do direito público Cf. Kant (1988). Ver também Kant (1985).

37. David Luban cita o exemplo do escândalo Irã-Contras nos Estados Unidos, mas também discute criticamente a tradição que, de Platão até Hegel, justificou o uso de “nobres mentiras” devido à incapacidade do público para compreender e julgar adequadamente as razões dos governantes. Contra o argumento das “nobres mentiras”, Luban defende o princípio de publicidade com base no que ele chama de “*rational skepticism*” a respeito da própria capacidade dos governantes e de uma expectativa razoável, não ingênua, a respeito da possibilidade de uma opinião pública educada formar juízos sobre as máximas de primeira e segunda ordem apresentadas pelos governantes Cf. Luban (1996:188-195).

38. Bobbio (2000).

39. Na letra dos decretos, a atual regulamentação brasileira sobre segredo governamental é mais frouxa e genérica do que a norte-americana em relação ao que pode ou não ser classificado como sigiloso. Saber o exato significado e os usos do texto legal dependeria de comparações sistemáticas sobre o manejo do segredo governamental nos dois países, o que não é possível fazer aqui. No Brasil, o capítulo III do Decreto nº 2.134/97 prevê ainda uma categoria de classificação de sigilo inferior a essas três, chamada de “reservada”. Essa categoria não é utilizada nos Estados Unidos, mas aparece na legislação britânica, canadense e australiana como “restricted”. Para o caso brasileiro, cf. o Decreto nº 2.134/97, Brasil (1999). Para o caso norte-americano, cf. a Executive Order nº 12.958/95 (Compilation of intelligence laws and related laws and Executive Orders of interest to the national intelligence community), incluída em US Congress (1998b). Para informações sobre classificações de segurança na Grã-Bretanha, Canadá e Austrália, ver Lustgarten & Leigh (1994:104-126).

40. Com base nesse princípio, em 1995 havia nos Estados Unidos 29 agências governamentais com delegações de autoridade para aplicar classificações de sigilo em primeira instância. Segundo o relatório da Comissão sobre Segredo Governamental citado anteriormente, o número de indivíduos com poder de atribuir sigilo caiu de cerca de 60 mil, em 1970, para 5.400 em 1995. No caso do decreto brasileiro, o Decreto nº 2.137/97 prevê que a classificação de ultra-secreto só poderá ser feita pelos chefes dos três poderes da República. Entretanto, as delegações de autoridade previstas para as categoriais secreto, confidencial e reservado são feitas em cascata, começando com governadores e ministros de Estado e indo até coordenadores de projetos em secretarias de governos municipais. Por exemplo, a classificação de segurança de um documen-

to como “reservado” introduz restrições de acesso público por até cinco anos. As autoridades que podem atribuir esse marcador são os chefes dos poderes Executivo, Legislativo e Judiciário federais, governadores, ministros de Estado, titulares de órgãos da administração pública federal, do Distrito Federal, estados e municípios, bem como por agentes públicos formalmente encarregados da execução de projetos, planos e programas. Até onde sei, não existem estudos sistemáticos sobre a eficiência e os problemas do atual sistema de classificação de segredos governamentais no Brasil.

41. Para uma breve introdução aos problemas legais de infosec, cf. o capítulo IX (Defensive measures for intelligence) do trabalho já citado de Krizan (1999:61-70). Para uma abordagem mais técnica e alentada, ver a parte dois (Nuts and Bolts) do livro de Martin (1999). Para o caso do Brasil, cf. o Decreto nº 2.910/98, que estabelece normas para a salvaguarda de documentos, materiais, áreas, comunicações e sistemas de informações de natureza sigilosa. Para o caso do Brasil, cf. Brasil (1999b).

42. Além das referências já mencionadas, no caso dos sistemas de voto de segurança para candidatos a empregos e das investigações de *background* de funcionários para a concessão de credenciais de acesso, ver Lustgarten & Leigh (1994:127-163). Nos Estados Unidos, em 1993, mais de 3,2 milhões de funcionários federais e trabalhadores de firmas contratadas possuíam credenciais de acesso a informações classificadas (2,29 milhões possuíam nível de acesso *secret*, 768 mil *top secret* e 154 mil *confidential*). Cf. o capítulo IV (Personnel security: protection through detection) in US Government (1997c).

43. No caso brasileiro, embora o Decreto nº 2.134/97 preveja medidas adicionais de controle com base no princípio da “necessidade de conhecer”, o único marcador adicional previsto é o DSC – “documento sigiloso controlado”. Nos Estados Unidos, além de uma categoria similar (Orcon – *dissemination and extraction of information controlled by originator*), camadas extras de classificação de segurança envolvem o uso, por exemplo, de marcadores não-sigilosos como Fouo (para uso oficial apenas), Noforn (vetado para estrangeiros) e Nocontract (vetado a empreiteiros ou contratados), até marcadores que aprofundam o sistema de sigilo, tais como Wnintel (nota de alerta: fontes ou métodos de inteligência foram utilizados), Nato *secret* e Nato *high secret*, além das chamadas listas Bigot (listas que necessitam de códigos especiais de acesso), para citar apenas alguns exemplos. Cf. US Government (1997c).

44. Chapter 37 (Espionage and censorship) of Title 18, United States Code. US Congress (1998b).

45. Segundo Holt (1995:182), as poucas pesquisas existentes nos Estados Unidos sobre “vazamentos” (*leaks*) apresentam resultados contraditórios sobre a origem dos mesmos. Num *survey* conduzido pelo Comitê de Inteligência do Senado, nos primeiros seis meses de 1986 houve 147 divulgações de informações classificadas nos oito maiores jornais dos Estados Unidos. Desses *leaks*, 98 foram atribuídos a fontes anônimas no Poder Executivo, 17 foram atribuídos a militares, fontes estrangeiras ou fontes não-governamentais, 13 foram atribuídos a fontes no Congresso e em 19 casos as estórias eram tão vagas que não foi possível atribuir as fontes.

46. No caso do ex-membro da CIA Philip Agee, que publicou em 1975 um livro-denúncia sobre as operações da agência na América do Sul com uma lista de 2.500 nomes reais de operadores e agentes, a justificativa do autor era de que sua campanha

servia aos interesses das vítimas de atividades ilegais da CIA e que os nomes revelados estavam envolvidos em assassinatos e desestabilização de regimes democráticos. A Suprema Corte dos Estados Unidos não aceitou essa justificativa e cassou a cidadania de Agee em 1981. O Congresso americano aprovou uma lei em 1982 (Intelligence Identities Protection Act) criminalizando a revelação da identidade de funcionários norte-americanos de agências de segurança nacional operando sob cobertura. A controvérsia sobre o caso Agee nos Estados Unidos arrasta-se até hoje. Embora tenham surgido denúncias sobre a ligação de Philip Agee com o serviço de inteligência de Cuba, o ex-funcionário da CIA nunca foi processado por espionagem nos Estados Unidos. Cf. Polmar & Allen (1997:6). O caso Agee interessa aqui apenas para ilustrar os mecanismos de sanção à publicização de informações secretas e suas ambigüidades. A literatura de denúncia sobre a CIA na década de 1970 é bastante vasta. Sugiro começar pelo próprio Agee (1976). Ver também Marchetti & Marks (1979).

47. Cf. § 798 (disclosure of classified information) do capítulo 37 (Espionage and censorship) do título 18 do United States Code [USC]. Ver US Congress (1998b).

48. A informação sobre quantas páginas de documentos classificados existem hoje nos Estados Unidos, caso o próprio governo daquele país tenha alguma estimativa, certamente é classificada. Documentos classificados com mais de 25 anos são elegíveis para revisão e desclassificação automática com base na Executive Order 12.958/95. Documentos mais recentes são revisados para desclassificação sob requerimento amparado no Freedom of Information Act (Foia). Ver US Government (1997c).

49. Cf. Michael Herman (1996:90-92) sobre por que a imprensa deveria se abster de publicar informações sigilosas obtidas de um adversário e que aparentemente o inimigo/adversário/competidor já sabe que foram obtidas. O argumento diz basicamente que isso contribuiria apenas para alertar as autoridades superiores do país adversário de que houve uma brecha de segurança, levando-as a investigar e rever os procedimentos, o que interromperia o fluxo de informações potencialmente oriundo daqueles canais.

50. A formulação geral do dilema da representatividade, a distinção entre responsividade (*ex ante*) e *accountability* (*ex post*), bem como a reflexão sobre a centralidade do acesso à informação para a efetividade dos mecanismos de controle público que garantem a representatividade são três temas formulados de maneira mais extensa em: Przeworski, Stokes & Manin (1999:1-27 e 329-344). Para a distinção entre mecanismos verticais de *accountability* (eleições) e mecanismos horizontais derivados da doutrina da separação de poderes e exemplificados pelos *checks-and-balances* previstos pela Constituição dos Estados Unidos, ver O'Donnell (1991:25-40).

51. Embora a bibliografia sobre controle externo das atividades de inteligência seja cada vez mais extensa, existem poucos trabalhos teoricamente orientados sobre o papel e o desempenho institucional dos mecanismos de supervisão e controle de atividades de inteligência e segurança. Por outro lado, como se pode notar lendo o livro recente editado por Przeworski, Stokes & Manin (1999) e mesmo o artigo de O'Donnell (1991) mencionados anteriormente, a reflexão sobre *accountability* na teoria democrática contemporânea prefere simplesmente contornar o problema da segurança nacional. De resto, a maior parte do material existente é bastante descritiva e foca apenas os casos nacionais mais conhecidos (Estados Unidos, Canadá, Grã-Bretanha etc.) ou, quando são estudos comparativos, estes tendem a concentrar-se num tipo de mecanismo ou de agê-

cia. Por sua qualidade, destaca-se também aqui o livro dos juristas britânicos Lustgarten & Leigh (1994), nesse caso, especialmente os capítulos da parte V (Controlling National Security Institutions). Note-se, porém, que os dois autores analisam apenas os serviços de inteligência e segurança (*security intelligence*) "domésticos", voltados para a atuação dentro dos países, excluindo da análise as especificidades da supervisão e dos mandatos legais das agências de inteligência externa (*foreign intelligence*). Lustgarten e Leigh fazem uma comparação exemplar dos mecanismos de controle sobre o MI-5 britânico, o CSIS canadense e o Asio australiano. A motivação inicial dos dois autores foi a introdução de um mandato legal (inédito e muito genérico) para o *Secret Service* (MI-5) em 1989. Para uma avaliação do funcionamento dos novos mecanismos de *oversight* e *accountability* durante o governo conservador de John Major, ver Gill (1996:313-331). Um trabalho recente sobre a reforma dos serviços de inteligência interna (*security intelligence*) na Europa Oriental é: Williams & Deletant (2001). Uma descrição breve dos casos norte-americano e canadense, para fins de contraste com o caso brasileiro, é feita na parte IV (O Poder Legislativo e os Serviços Secretos) do trabalho de Emilio (1992). Na Argentina, autores como Eduardo Estevez, Manuel Ugarte e Eduardo Balbi têm escrito sobre estruturas de controle e tendências. Ver, por exemplo: Estevez (2000). O desempenho institucional dos inspetores-gerais e corregedores de órgãos de inteligência e segurança do Canadá, Estados Unidos, Grã-Bretanha e Austrália é analisado em Weller (1997:383-406). O mesmo autor publicou em 2000 um artigo interessante sobre a fragilidade dos sistemas de supervisão nos países escandinavos: Weller (2000:171-192). Uma "descrição densa" do papel da mídia, do Poder Executivo e do Congresso na supervisão dos serviços de inteligência norte-americanos é oferecida por Holt (1995). São excelentes introduções ao problema os capítulos 10 (*Oversight and accountability*) e 13 (*Ethical and moral issues*) de Lowenthal (2000). Além de outras referências mencionadas ao longo da seção, vale conferir dois relatórios produzidos por analistas do serviço de pesquisa do Congresso norte-americano, US Congress (1994). Além de apresentar sistematicamente a evolução do sistema de supervisão congressual, a estrutura, mandatos e operações dos comitês de inteligência do Senado e da Câmara, essa publicação traz em anexo os principais textos legais e documentos relevantes para o estudo do caso norte-americano. Vale a pena também a leitura de um relatório mais antigo, mas ainda bastante útil, que compara brevemente os mecanismos de supervisão das atividades de inteligência nos Estados Unidos, Dinamarca, Alemanha, Itália, Países Baixos, Austrália, Nova Zelândia, Grã-Bretanha, Canadá e Austrália. US Congress (1990).

52. Para a distinção entre instituições externas e normas sociais internalizadas nas interações entre indivíduos, ver Elster (1989:137-148 e 174-186). Para uma introdução ao problema da atividade de inteligência enquanto profissão sociologicamente reconhecível na práxis social, ver Bruneau (2000:28-33).

53. A discussão sobre traços individuais e características sistêmicas afetando o comportamento dos eleitores é sintetizada criticamente em Reis (1999:157-190).

54. Por definição, governantes não são agentes perfeitos do público, pois têm seus próprios interesses, valores e finalidades. Regimes democráticos contemporâneos são, nos termos de Schumpeter e Dahl, oligarquias selecionadas através de mecanismos relativamente pacíficos e competitivos, principalmente eleições, o que faz toda a diferença para os governados quando o mecanismo é comparado a qualquer outra forma de governo oligárquico não-democrático, i.e., autocracias, tiranias ou ditaduras de qualquer espécie; ver Schumpeter (1984).

55. A relação mais geral entre mídia e democracia é abordada do ponto de vista da teoria social por Thompson (1996).

56. Sobre a mídia e os serviços de inteligência nos Estados Unidos, ver o capítulo 8 (*The Media*) do livro já citado de Pat Holt (1995:171-188). Os trabalhos investigativos de jornalistas como Bob Woodward, Carl Bernstein, Jim Hoagland e Walter Pincus podem ser considerados exemplares de uma cobertura crítica mais ou menos isenta, que se concentra nos problemas substantivos e não apenas na denúncia pontual de um escândalo, falha ou má conduta. Para uma ilustração desse ponto – e também de suas ambigüidades –, vale a pena a leitura do livro bastante criticado do jornalista Bob Woodward sobre as operações encobertas da CIA durante o governo Reagan, Woodward (1987). Um trabalho ainda hoje útil no caso brasileiro é o livro da jornalista Ana Lagôa sobre o Serviço Nacional de Informações na época do regime militar, Lagôa (1983).

57. Para uma sinopse da literatura e da filmografia sobre espionagem e inteligência, ver Polmar (1997:336-338 e 379-382). Um problema relacionado, mas que exigiria um tratamento mais detalhado, é o da utilização de meios de comunicação próprios ou de terceiros para operações encobertas (*covert actions*) ou para fins de guerra psicológica. Para uma descrição sintética das operações de propaganda no contexto de uma tipologia das operações encobertas, ver Godson (1995:120-183) e Shulsky (1992:83-109).

58. Note-se que, do ponto de vista operacional, é bastante diferente a utilização de um cargo num veículo de comunicação como fachada para um oficial de inteligência agindo sem cobertura diplomática (um NOC ou, para utilizar o jargão soviético, um “illegal”) e o recrutamento de um jornalista de carreira para prestar serviços para um órgão de inteligência; do mesmo modo, é diferente a tentativa mais ou menos bem-sucedida de manipular a mídia a respeito de algum tema, do estabelecimento de empresas ou veículos de comunicação inteiramente sob controle do órgão (*‘front’ organizations*). Ver Godson (1995:120-183).

59. Holt (1995:174-175). Segundo Loch Johnson estimou, nos 25 anos anteriores (1950-75) a CIA havia empregado pelo menos 400 jornalistas norte-americanos de vários veículos impressos, rádios e cadeias de televisão para operações no exterior. As diversas trocas de acusações de espionagem entre Rússia e Estados Unidos ao longo da década de 1990 envolveram seguidamente acusações sobre o emprego de jornalistas, o que indica claramente que as declarações de Bush e Primakov não significavam o fim de todo e qualquer uso da mídia para fins de obtenção de humint, mesmo ou principalmente após a Guerra Fria. Ver Johnson (1989:182-203).

60. Sobre terceirização de coleta de inteligência desde fontes ostensivas (osint) e sobre as relações entre empresas de comunicação, firmas de “*business intelligence*” e agências governamentais, ver Steele (2000).

61. Em geral, a divulgação de segredos pela mídia ocorre porque há um “vazamento” do interesse de alguma autoridade, tema já considerado no capítulo anterior. No caso de divulgações passíveis de acusação de traição, o § 798 (disclosure of classified information) do capítulo 37 (Espionage and censorship) do título 18 do United States Code [USC], por exemplo, proíbe explicitamente a publicação de qualquer informação classificada referente a códigos, cifras, sistemas criptográficos, atividades de sigint ou informações obtidas a partir de operações de sigint. Há outras restrições, como a da divulgação da

identidade de oficiais de inteligência operando sob cobertura no exterior, proibida pelo Intelligence Identities Protection Act of 1982. Ver US Congress (1998b).

62. Exemplos de diretrizes executivas mais específicas e na maioria das vezes classificadas são, no contexto norte-americano, as diretrizes presidenciais (ex.: PDD/NSC # 35: *Intelligence Requirements/National Needs Process*, de fevereiro de 1995), as diretrizes do Conselho de Segurança Nacional (ex.: DCID # 2/09 – SECRET: *Management of National Imagery Intelligence*, de janeiro de 1992), bem como as diretrizes do Departamento de Defesa (ex.: DoDD # 5240.12: *DoD Intelligence Commercial Activities*, de janeiro de 1996).

63. US Congress (1998b).

64. Sobre a natureza ambígua da atividade de inteligência em geral e especialmente da espionagem no âmbito do direito internacional, um comentário interessante e que ilustra a necessidade de reflexão adicional está feito em Bowman (1995:321-335).

65. Um ponto decisivo dos mandatos legais concedidos aos serviços de inteligência e segurança em relação à contra-espionagem é a concretização dos princípios de soberania popular e de autogoverno; tentativas de governos ou organizações estrangeiras para influenciar os resultados políticos internos de uma nação soberana são consideradas crimes graves porque violam os direitos democráticos dos cidadãos e devem ser prevenidas através do monitoramento por parte dos serviços de contra-inteligência. No caso dos Estados Unidos, mesmo o *lobby* regular de empresas, governos ou ONGs estrangeiras é monitorado, principalmente através da exigência de registro de atividades de estrangeiros. Ver US Code. Section 951 of title 18. *Agents of Foreign Governments*. Ver também: Foreign Agents Registration Act of 1938 as amended [Fara], incluído em US Congress (1998b).

66. Um exemplo desse tipo de viés: não obstante a legislação australiana vetar o engajamento do serviço de segurança (Australian Security Intelligence Organization – Asio) em operações que violem os direitos de os cidadãos manifestarem-se livremente contra o governo, o mandato do Asio prevê o uso de medidas preventivas contra o crime de “sedição”, ou seja, a promoção de “hostilidade entre diferentes classes de súditos de Sua Majestade”. As implicações dessa relíquia da lei criminal britânica no contexto contemporâneo, na medida em que “classes de súditos” sejam entendidas como categorias “socioeconômicas” representadas por organizações e partidos, vão desde uma autorização potencial para a vigilância de sindicatos e grupos socialistas revolucionários até a expectativa absurda de que todos os conflitos distributivos sejam igualmente acompanhados pelos serviços de inteligência e segurança. Ver Lustgarten & Leigh (1994:405-410).

67. Herman (1994).

68. Procedimentos judiciais especiais, tais como a concessão de credenciais de segurança para os jurados, juízes, promotores e advogados (após procedimentos de checagem de *background*), ou a realização de sessões secretas em locais devidamente protegidos contra o vazamento de informações classificadas associadas às provas do processo são possíveis, embora custosos. Esses custos reforçam a assimetria informacional que favorece o Poder Executivo em casos de litígio contra indivíduos e grupos de cidadãos na área de segurança nacional. Ver Lustgarten & Leigh (1994:353-359).

69. De novo, isso não quer dizer que processos judiciais nunca resultem em revisões independentes e externas de decisões do Poder Executivo na área de segurança nacional. Processos como o da tentativa de cassação do Partido Comunista australiano (1950), em que a Suprema Corte australiana recusou a cassação e estabeleceu nuances importantes para os poderes especiais do Poder Executivo em tempos de guerra e de paz, ou casos como o julgamento dos arrombadores do escritório do Partido Democrata no edifício Watergate (1973), que resultou na abertura de processo de *impeachment* contra o presidente Nixon e, posteriormente, na abertura de investigações sobre as violações de direitos civis por parte das agências de inteligência,<sup>70</sup> ilustram o papel crítico que o Judiciário pode desempenhar em situações muito menos dramáticas que envolvam diferentes interpretações sobre aspectos das políticas de segurança nacional. Para uma avaliação da distância entre a jurisprudência dos casos envolvendo a segurança nacional e as concepções liberais mais sofisticadas sobre o papel do Judiciário, ver também Dworkin (1978 e 1988).

70. US Congress (1984). Para a íntegra do Fisa, ver US Congress (1998b).

71. Na Grã-Bretanha existe a posição de comissário do Security Service (MI-5) e de comissário das outras duas agências principais de *foreign intelligence*, o SIS e o GCHQ. Esses *commissioners* foram instituídos pela legislação de 1989 (MI-5) e 1994 (SIS e GCHQ) e devem ser juízes ou ex-juízes apontados pelo primeiro-ministro. O mandato dos comissários britânicos é restrito. Ambas as posições de comissário têm sido exercidas pela mesma pessoa: até o ano de 2001, o Lord Justice Simon Brown. Existe ainda um comissário para assuntos de interceptação de comunicações, estabelecido pelo Interception of Communications Act 1985, que revisa os pedidos de autorização para vigilância eletrônica feitos pelas agências policiais, de segurança e de inteligência e que assiste ao tribunal especial estabelecido pela mesma legislação em investigações de denúncias sobre abusos na área de interceptação de comunicações. Sobre o desempenho considerado limitado dos comissários britânicos na sua função controladora, ver Gill (1996:313-331) e Weller (1997:390-396). Ver também <<http://www.official-documents.co.uk/document/caboff/nim>>.

72. Sobre a centralidade da auditagem das contas secretas como um problema de *accountability* dos órgãos de inteligência nos países semiperiféricos, ver o artigo de Estevez (2000:6). Ver, principalmente, a análise do Decreto nº 833/2000 da Presidência da República da Argentina, que abriu as contas da ex-Side (Secretaria de Inteligencia de Estado).

73. Para dados adicionais sobre o escritório do inspetor-geral australiano e *links* para as páginas dos serviços de inteligência daquele país na internet, ver <<http://www.igis.gov.au>>.

74. Para mais informações sobre a versão pública dos relatórios do inspetor-geral da CIA disponíveis na internet, ver <[www.cia.gov](http://www.cia.gov)>.

75. Ver <<http://www.loyola.edu/dept/politics/intel/hitzrept.html>>.

76. A discussão mais geral sobre impactos diferenciais dos tipos de governo (república/monarquia, presidencialismo/parlamentarismo, democracia/ditadura etc.) sobre o desempenho dos mecanismos de *accountability* é feita em Cheibub & Przeworski (1999). Para a distinção mais elaborada entre democracias presidenciais e parlamentares, ver

Lijphart (1992). Para uma reflexão específica sobre mecanismos de *accountability* em democracias parlamentares, ver Shepsle & Laver (1999). Para uma discussão do caso britânico, onde a lei de 1994 criou um Intelligence and Security Committee (ISC) formado por nove membros de diferentes partidos, vindos das duas casas do Parlamento e que são apontados pelo primeiro-ministro, ver Gill (1996:313-331).

77. Além do Sirc, cuja principal missão é supervisionar o CSIS, existem grupos especiais de revisão e inspetorias para a organização de sigint e infosec canadense (CCSE), bem como para as atividades relacionadas com inteligência nas Forças Armadas, na diplomacia e nas polícias. Essas instâncias de supervisão estão localizadas nos escritórios do Solicitor General, dos ministros da Defesa e das Relações Exteriores. Para uma visão geral, ver Canada (1996). <<http://www.oag-bvg.gc.ca>>. Para uma descrição mais detalhada das funções e recursos do Sirc, ver <[www.sirc-csars.gc.ca](http://www.sirc-csars.gc.ca)>. Através do site do CSIS na internet também é possível obter algumas (poucas) informações adicionais sobre as demais organizações e atividades de inteligência daquele país: <[www.csis-scrs.gc.ca](http://www.csis-scrs.gc.ca)>.

78. Até mesmo por sua escala, a descrição sumária das organizações que formam o sistema de supervisão e coordenação de atividades de inteligência do Poder Executivo norte-americano pode ser útil para uma comparação com sistemas mais simples, na medida em que isso permite identificar lacunas ou assimetrias organizacionais.

79. A conformação atual do Pfiab é determinada pela Executive Order 12.863, assinada pelo presidente Bill Clinton em 1993. Basicamente, aquele decreto transformou o IOB (que já existia como um *board* separado desde 1976) numa subcomissão do Pfiab. O número de membros do Pfiab foi fixado em no máximo 16 pessoas, que servem à disposição do presidente sem remuneração (fora jetons e despesas). No caso do IOB, são quatro membros indicados pelo *chairman* do *board* maior e que basicamente recebem os relatórios dos inspetores-gerais sobre a legalidade dos atos das agências de inteligência e os repassam para o presidente. Cf. US Congress (1998b).

80. À primeira vista, isso poderia ser um indicador positivo de adaptabilidade institucional, mas o problema é que em áreas de grande complexidade organizacional, especialização tecnológica e sensitividade política isso também pode significar que os diversos arranjos internos do NSC não têm tempo de amadurecer e fazer um trabalho efetivo de supervisão e coordenação política. Pior ainda, considerando-se o escândalo Irã-Contras por esse ângulo, a grande flexibilidade operacional do *staff* do NSC pode tornar-se ela própria um problema de *oversight* quando um presidente resolve tentar contornar o que considera uma excessiva regulação imposta sobre as burocracias regulares da área de inteligência. Além dos textos já mencionados de Amy Zegart e Jeffrey Richelson, ver também sobre o NSC norte-americano Lowenthal (1993) e ainda Shoemaker (1991). Sobre a estrutura atual e as divisões internas do *staff*, ver <[www.whitehouse.gov/nsc/staff.html](http://www.whitehouse.gov/nsc/staff.html)>.

81. Com exceção do inspetor-geral da CIA, os demais inspetores-gerais de agências de inteligência não realizam auditorias financeiras, necessitando de apoio do Office of Management and Budget (OMB) para isso. Também existem órgãos de supervisão da eficiência e da legalidade das operações de inteligência nos departamentos do Tesouro, Energia, Justiça e no Departamento de Estado. Ver Holt (1995:189-208).

82. As NIEs são normalmente classificadas (*top secret*), mas outros relatórios e estudos produzidos pelo NIC são ostensivos. Um exemplo recente que recebeu bastante

atenção da mídia, inclusive no Brasil, foi um estudo de cenários divulgado há algum tempo pelo ODCI. Cf. US Government (2000).

83. Além do IC/Excom, NFIB, CMS e NIC, existem cerca de 31 comitês de coordenação interagências em áreas temáticas e gerenciais tão diversas quanto a política de coleta para os alvos “difíceis” (Hard Targets Principals Forum – HTPF), o comitê para a avaliação das políticas estrangeiras de negação e engodo (Foreign Denial And Deception Committee – FDCC) ou ainda o comitê para inteligência sobre armas e sistemas espaciais (Weapons and Space Systems Intelligence Committee – WSSIC). Para uma listagem desses comitês e das estruturas de gerenciamento e supervisão no ODCI, ver US Government (1999a). Para um comentário (algo assistemático) sobre os documentos, autoridades e escritórios de controle e gerenciamento de inteligência dos Estados Unidos, ver também Richelson (1999:374-403).

84. O controle sistemático da legalidade das atividades de inteligência no âmbito do Pentágono só entrou na agenda norte-americana após as investigações congressuais e escândalos dos anos 1970. Para uma história e uma descrição das atividades desse escritório, ver <<http://www.dtic.mil/atsdio>>. Para uma visão geral da organização do gabinete do secretário de defesa (um dos três componentes principais do Pentágono, ao lado do JCS e dos departamentos das FFAA), ver <<http://www.defenselink.mil/osd>>.

85. Existem estudos sobre episódios específicos (ex.: sobre o trabalho da Comissão Rockefeller em 1975, ou sobre as falhas de supervisão nas operações encobertas contra a Nicarágua), mas nada sistemático. A máxima segundo a qual numa democracia nenhum poder deveria fiscalizar a si próprio sem mecanismos adicionais de controle externo é correta, mas ela não quer dizer que não se deva tentar aperfeiçoar os mecanismos de controle internos ao Poder Executivo. Para uma avaliação da complexidade do gerenciamento de um aparato com dezenas de agências e vários bilhões de dólares anuais de orçamento, ver Elkins (1997).

86. Para uma ilustração desse ponto, ver os capítulos sobre gestão de recursos em Odom (1997:1-68) e Elkins (1997:35-112).

87. A ênfase norte-americana a respeito da necessidade de os serviços de inteligência manterem certa distância dos processos de *policymaking* para evitar os riscos de “politicização”, somada ao grande volume de produtos de inteligência derivados de fontes singulares, tem suscitado questionamentos sobre a baixa responsividade dos produtores de intel em relação aos usuários. Ver Herman (1996:281-338).

88. Segundo Adam Przeworski, a refutação das teses de Niskanen é definitiva a partir do novo institucionalismo: “Miller e Moe (1983) mantêm a premissa de Niskanen (1971) de que o órgão pode mentir sobre verdadeiros custos e ainda assim obtêm um resultado verdadeiramente poderoso: se o órgão governamental é forçado a fornecer a escala de custos sem conhecer a escala de demanda da comissão legislativa, o órgão vai achar de seu melhor interesse a revelação de seus verdadeiros custos. Intuitivamente, a razão é a seguinte: se o órgão mentisse à comissão, fornecendo um custo marginal acima do nível verdadeiro, estaria escolhendo um nível de atividade mais baixo do que sob a verdadeira escala de custos, algo que eles gostariam de evitar. Se revelasse um custo marginal abaixo do nível verdadeiro, a comissão poderia escolher um nível de atividade que o órgão governamental não conseguiria de fato fornecer. Sendo assim, a estratégia Stackelberg, por parte do órgão governamental, é revelar seus verdadeiros custos”. Ver Przeworski (1985:82).

89. Para uma introdução didática ao funcionamento do Congresso norte-americano, de um ponto de vista que não descreve apenas o processo de tramitação dos projetos de lei, mas também analisa as diferentes instituições que estruturam a política dentro do Congresso (partidos, comissões, líderes, *caucuses* e órgãos assessores), ver Löwi & Ginsberg (1992:89-124).

90. Os 45 comitês do Congresso norte-americano e seus inúmeros subcomitês formam o núcleo vital do debate e da política legislativa em Washington, DC. A centralidade adquirida pelos *committees* deslocou o plenário como o centro da atividade parlamentar e tem sido utilizada para explicar por que não se verifica o fenômeno das maiorias cíclicas nos parlamentos. Tratar-se-ia, portanto, de um tipo de equilíbrio majoritário induzido por instituições, ou seja, por organizações e regras ("structure induced equilibrium"). Como os diferentes modelos explicativos sobre o funcionamento interno do Congresso norte-americano (distributivo, informacional e partidário) discordam em relação ao problema que precisa ser resolvido pelos parlamentares enquanto indivíduos racionais, discordando portanto sobre qual é a solução institucional adequada, basta por agora listar esses objetivos/problemas: 1. Reeleição, produção de boas políticas e busca de influência no Parlamento. 2. Reeleição como objetivo dominante (Arnold, 1990). 3. Reeleição como objetivo intermediário e decisivo. 4. Informação e endogeneização das preferências. O modelo distributivo é desenvolvido em Arnold (1990). O modelo partidário de explicação do funcionamento do Congresso é desenvolvido principalmente em Cox & McCubbins (1993). A obra mais importante sobre o papel da informação na lógica da ação parlamentar é Arnold (1990) e Cox & McCubbins (1993). Para um balanço desses três modelos, ver Shepsle & Weingast (1995).

91. Sobre a origem, composição interna dos comitês e evolução histórica da supervisão congressual na área de inteligência nos Estados Unidos, ver US Congress (1994) e, ainda, Holt (1995:209-236). Ver também Wagenen (1997).

92. Entre outras leis que tratam diretamente das agências de inteligência, pode-se mencionar o Central Intelligence Agency Act of 1949, o National Security Agency Act of 1959, o Foreign Intelligence Surveillance Act of 1978, o Intelligence Identities Protection Act of 1982, o Intelligence Renewal and Reform Act of 1996, o Economic Espionage Act of 1996 e o Classified and Related Information Disclosure Act of 1998. Cf. US Congress (1998b).

93. O ano fiscal nos Estados Unidos vai de 1º de outubro até 30 de setembro. Anualmente, o projeto de lei orçamentário é apresentado em fevereiro aos comitês de inteligência do Senado e da Câmara pelo DCI (no caso do NFIP) e para os comitês de Forças Armadas nas duas casas pelo secretário da Defesa (no caso do JMIP e do Tiara). Entre fevereiro e maio são feitas audiências para discussões formais (*Hearings*), visitas técnicas e estudos por parte dos parlamentares dos comitês de inteligência. A partir de maio, os comitês recebem as recomendações das assessorias e dos demais comitês envolvidos naquela área temática. Entre junho e setembro o projeto de lei (*bill*) tramita no plenário (*floor action*) de cada casa do Congresso. Depois de aprovados separadamente nas duas casas do Congresso, os projetos de lei tornam-se atos legislativos (*Acgs*) e têm a sua compatibilidade conferida por um comitê especial do Congresso (*Conference Committee*). Somente depois dessa etapa, que ocorre em setembro ou outubro de cada ano, as leis são aprovadas pelo Congresso e tornam-se então *Public Laws*. Por

exemplo, o Intelligence Authorization Act for Fiscal Year 1997 é referido também como Public Law 104-293, sendo que 293 é o número da lei e 104 significa que a lei foi aprovada na 104<sup>a</sup> reunião do Congresso (1995/96). Cada reunião do Congresso divide-se em duas sessões anuais e, em muitos relatórios, se poderá encontrar ainda a especificação *1st Session ou 2nd Session*. Se o presidente não sancionar a lei aprovada em 10 dias úteis enquanto o Congresso estiver reunido ela torna-se lei mesmo assim. Caso ele não a sancione em 10 dias úteis durante um recesso congressional a lei “morre” (*pocket veto*). No caso de um veto formal do presidente, ele só pode ser derrubado pelo voto de dois terços dos parlamentares de cada casa. Ver Elkins (1997:159-179) e Pickett (1985).

94. Através desse mecanismo, são evitados os percalços e polêmicas associados à tramitação de legislação ordinária adicional. Atos como, por exemplo, o CIA Inspector General Act of 1990, o Intelligence Oversight Act of 1991 e o Intelligence Organization Act of 1992, são na verdade títulos específicos dos Authorization Acts daqueles anos. Mesmo a criação de uma nova agência, como a Nima (a qual, juntamente com a CIA, é uma das duas únicas agências nacionais de inteligência dos Estados Unidos criadas através de lei federal), foi feita através de um ato (National Imagery and Mapping Agency Act of 1996) que faz parte do National Defense Authorization Act of 1996 (também referido como Public Law 104-201). Assim, mesmo descontando os extratos classificados (secretos) das autorizações orçamentárias anuais, por vezes é bastante confuso acompanhar as regulações públicas da atividade de inteligência introduzidas pelo Congresso. Por outro lado, quando os comitês congressuais ou o Executivo julgam necessário, também são discutidos projetos de lei específicos sobre algum tema, fora das leis anuais de autorização fiscal (esses projetos específicos são chamados de “*free standing bills*”). Além das leis mencionadas, ver também US Congress (1994).

95. Na verdade, a única vez em que um Intelligence Authorization Act foi vetado pelo presidente foi em agosto de 1990, quando George Bush vetou a lei de autorização de gastos para o ano fiscal de 1991 porque os congressistas haviam incluído na lei uma determinação exigindo que qualquer operação encoberta do governo norte-americano deveria ser comunicada aos comitês de inteligência da Câmara e do Senado em no máximo 48 horas, quando o entendimento legal anterior dizia apenas que essa comunicação se daria prontamente (“*in a timely fashion*”). Um acordo informal com o Congresso permitiu que os gastos fossem realizados até que uma nova lei de autorização fosse aprovada, o que aconteceu apenas em agosto de 1991, menos de dois meses antes do ano fiscal terminar (Holt, 1995:224). Sobre a regra de 48 horas, atualmente em vigor, cf. o título V (Accountability for Intelligence Activities) do National Security Act of 1947.

96. Tanto o DCI quanto o secretário da Defesa (SecDef) são atualmente obrigados por lei a enviar um relatório anual das atividades de inteligência sob sua responsabilidade, além de outros relatórios específicos sobre temas tão diversos quanto as práticas de direitos humanos em diversos países ou o impacto dos acordos de controle de armas sobre a pesquisa e o desenvolvimento de novos sistemas de armas. Ver, como exemplo, US Government (1999b).

97. Para uma comparação entre um processo de confirmação praticamente unânime (o do atual DCI George Tenet) e outro altamente controverso (o do ex-DCI da administração George Bush, Robert Gates), ver US Senate (1997). Como contraponto, ver

os três volumes do processo de Gates: Nomination of Robert M. Gates to be DCI. Senate Hearing 102-799. 102nd Congress, 1st Session. Sept. 16, 17, 19, 20 (v.1); Sept. 24, Oct. 1 and 2 (v.2); Oct. 3, 4 and 18 (v.3), 1991. 961pp [v.1]; 740pp [v.2]; 318 pp [v.3].

98. Para uma noção geral das atividades do comitê de inteligência do Senado dos EUA, ver US Senate (1999). Ver também: <<http://intelligence.senate.gov>>. As audiências anuais sobre ameaças têm algumas sessões secretas e documentos classificados, mas tendem a gerar *statements* (na forma de relatórios ou discursos) de caráter público por parte dos dirigentes das agências. Ver, por exemplo, Wilson (2000). As investigações que deram origem aos comitês permanentes de inteligência no Congresso estão documentadas em US Congress (1975 e 1976). Sobre as investigações recentes do SSCI em relação à China, ver o relatório de atividades do SSCI mencionado bem no início desta nota. Embora tediosas, as audiências públicas são transmitidas pelo canal de TV do Senado, o C-SPAN.

99. Título V (Accountability for Intelligence Activities), seções 501 e 502 do National Security Act of 1947.

100. Por exemplo, dado o custo astronômico de um satélite de reconhecimento, se o NRO afirmar que é necessário construir mais três satélites com um novo *design* e maior capacidade, cabe aos comitês congressuais responsáveis pela aprovação do orçamento realizar audiências para que os órgãos envolvidos expliquem suas demandas. Para saber se o novo satélite irá funcionar adequadamente, o comitê pode requerer uma avaliação técnica independente, externa ao NRO (mas quem seria capaz de fornecer isso?). Por outro lado, se o comitê tenta envolver-se na discussão sobre a melhor freqüência de rádio para transmissão das imagens do novo satélite para as estações de terra, isso então seria considerado microgerenciamento. Ver Holt (1995:231).

101. Johnson (1996) e Smist (1991).

102. Para um primeiro aprofundamento da discussão sobre democracia e inteligência, especialmente nas chamadas “novas democracias” em fase de consolidação, ver Bruneau (2000).

103. Note-se que para a existência desse desafio não é preciso supor qualquer tipo de monopólio autoritário dos serviços de inteligência em termos de fornecimento de informações relevantes para o processo decisório governamental. A mera existência de grandes organizações privadas e estatais que controlam importantes fluxos de produção e disseminação de informações tende a reduzir a capacidade de controle individual dos cidadãos sobre as decisões políticas mais importantes a uma fração infinitesimal no mundo contemporâneo. Sobre o tema da tecnocracia nos regimes democráticos, ver Dahl (1985).

104. Na verdade, essa afirmação corresponde mais à posição original de Bobbio no debate sobre as “promessas não cumpridas da democracia”, entre as quais ele situava o desafio da eliminação do “poder invisível e secreto”. Ver Bobbio (1986). Para a posição mais recente e pragmaticamente matizada do mesmo autor, ver Bobbio (1989:412-415).

105. Para Robert Dahl, essas condições *sine qua non* seriam garantias para o exercício individual de três capacidades: formular preferências, exprimir preferências e ter pre-

ferências igualmente consideradas na conduta do governo. Essas garantias traduzem-se em oito condições institucionais: 1. liberdade de formar e aderir a organizações; 2. liberdade de expressão; 3. direito de voto; 4. elegibilidade para cargos públicos; 5. direito de políticos disputarem apoio e votos; 6. fontes alternativas de informação; 7. eleições livres e idôneas; 8. instituições para fazer com que as políticas governamentais dependam de eleições e de outras manifestações de preferências. Como os regimes “variaram enormemente na amplitude com que as oito condições institucionais estão abertamente disponíveis, são publicamente utilizadas e plenamente garantidas ao menos para alguns membros do sistema político que queiram contestar a conduta do governo” (Dahl, 1997:27), em princípio se poderia medir o impacto dos serviços de inteligência e segurança sobre a democracia verificando o quanto a atuação rotineira dessas agências restringe essas garantias. Isso não é feito neste livro, mas trata-se de uma possibilidade interessante para futuras pesquisas.

106. Para retomar o problema discutido anteriormente nos termos do próprio Bobbio: “Um debate dedicado ao segredo na esfera pública não pode se desenvolver senão sobre a vertente da exceção, e não da regra. E estará diante de dois clássicos paradoxos que tornam todo discurso moral ambíguo: a) o paradoxo da incompatibilidade ou da antinomia dos princípios, no caso específico a antinomia entre o princípio da segurança do Estado e o princípio da liberdade dos indivíduos; b) o paradoxo da exceção à regra que é consentida porque permite salvar a própria regra (...). Um caso realmente exemplar desse paradoxo foi oferecido pelo próprio sistema democrático: vimos que a democracia exclui, como linha de princípio, o segredo de Estado, mas o uso do segredo de Estado, através da instituição dos serviços de segurança, que agem em segredo, é justificado entre outras coisas como um instrumento necessário para defender, em última instância, a democracia” Bobbio (1989:415).

107. Tais custos estão longe de ser apenas financeiros, mas estimativas do governo norte-americano sobre os gastos com sistemas de classificação de segurança para informações, instalações, procedimentos de gestão de segredos e investigações pessoais para concessão de credenciais de acesso (*background investigations*) indicaram gastos de US\$5,6 bilhões anuais em 1996, sendo US\$2,9 bilhões nas empresas contratadas pelo Pentágono e US\$ 2,7 bilhões nas agências governamentais (a CIA não foi incluída no levantamento). Essas estimativas são encontradas na parte II do relatório US Government (1997c). Report of the Commission on Protecting and Reducing Government Secrecy.

108. Para uma breve verificação dessa assertiva, basta uma leitura de três trabalhos seminais publicados também no Brasil: Dahl (1997), ou o extenso tratado de Sartori (1994). Sobre a incidência de regimes democráticos na década de 1990 (menos de 45% do total), ver Huntington (1994). Os dois textos curtos de Bobbio (1984 e 1999) sobre o segredo são praticamente as únicas referências sistemáticas sobre esses temas a partir da teoria democrática contemporânea.

## **Considerações finais**

*Like people growing old, governments may have been acquiring more and more powerful glasses but nevertheless becoming able to see less and less.*

May (1984:532).

Em dezembro de 1999, o Parlamento brasileiro aprovou a lei de criação da Agência Brasileira de Inteligência (Abin) e do Sistema Brasileiro de Inteligência (Sisbin), sancionada em seguida pelo presidente da República.

Para instruir as missões e o mandato da agência, a legislação em vigor define a atividade de inteligência como aquela que visa a “obtenção, análise e disseminação de conhecimentos 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” (Lei nº 9.883/99, art. 1º, § 2º).

O problema é que essa definição é excessivamente vaga, mesmo quando comparada à generalidade costumeira com que o tema é tratado na legislação de outros países. Ela implica, no limite, a idéia absurda de que a agência de inteligência está legalmente encarregada do provimento da onisciência para o governo brasileiro. Se a Abin e os demais órgãos policiais e militares do Sisbin se aferrarem à letra desse artigo aparentemente anódino em sua lei de criação, correrão o risco de se tornarem rapidamente irrelevantes para o processo decisório governamental ou, o que seria pior ainda, tentarão acumular poder irrestritivamente, protegidos pelo segredo governamental que a própria lei os encarrega de gerenciar.

*Sed quis custodiet ipsos custodes?* A seriedade da pergunta do poeta e satirista romano Juvenal sobre quem vigia os guardiões não admite respostas retóricas. Não basta dizer que são os cidadãos que controlam, em última instância, os mandatos concedidos aos legisladores, juízes, governantes e suas diversas agências executivas. Tampouco resolve o dilema estabelecer uma comissão parlamentar para supervisionar as atividades de inteligência, embora esse seja um passo necessário e muito bem-vindo que o Congresso brasileiro deu recentemente. A existência da Abin e do Sisbin tem agora amparo legal, mas ainda resta um longo caminho para que possam usufruir da legitimidade

derivada da percepção pública de que seu trabalho de proteção da Constituição e dos cidadãos contra ameaças externas e internas não é em si mesmo uma ameaça à segurança dos brasileiros. A lei de criação e os seus dirigentes da área de inteligência, especialmente na Abin e no Gabinete de Segurança Institucional (GSI) da Presidência da República, declararam reiteradamente os altos padrões de ética profissional e o respeito do novo órgão aos direitos humanos, à Constituição e aos tratados internacionais assinados pelo Brasil.

No entanto, assim como na política de defesa nacional e no também recém-criado Ministério da Defesa, a distância entre a intenção declarada e o gesto ainda terá que ser percorrida. Dadas as reiteradas denúncias de violações e os questionamentos sobre a missão dos órgãos de inteligência, nos próximos anos a Abin e os demais órgãos de inteligência e segurança do Estado brasileiro caminharão sobre um fio de espada para tentar equilibrar dois desafios normativos, o da agilidade e o da transparência.

Mas agilidade em relação a qual missão? E transparência em relação a que dinâmicas operacionais e mecanismos de controle? Como se sabe, o debate sobre o futuro das atividades de inteligência no Brasil arrastou-se fracamente desde a extinção do Serviço Nacional de Informações (SNI), em 1990. O duplo contexto de origem desse debate foi marcado pela transição para a democracia no plano nacional e pelas mudanças no ambiente de segurança internacional decorrentes do colapso da União Soviética e do fim da Guerra Fria. Depois de quase 10 anos, o impasse institucional foi resolvido com a criação da Abin. Mesmo assim, pouca gente, no governo ou fora dele, tem manifestado uma formulação consistente sobre o que é, afinal, a atividade de inteligência tal como realmente praticada no Brasil e o que ela deveria ser no novo contexto.

O que o Poder Executivo e os legisladores, para não falar dos cidadãos, esperam que a Abin faça? Quais são as ameaças internacionais e internas plausíveis contra o Brasil, ou os temas e problemas que geram requerimentos informacionais? Quais os recursos e os métodos necessários e aceitáveis para que a Abin possa conhecer melhor essas ameaças e informar tempestivamente o presidente da República, os ministros, os comandantes militares? Qual a relação da nova agência com as capacidades de inteligência do Ministério das Relações Exteriores, da Justiça ou da Defesa? Como controlar esses órgãos e os governantes que são responsáveis por eles de forma efetiva para que violações aos direitos dos cidadãos não se repitam? Esses e muitos outros questionamentos associados às atividades de inteligência e segurança têm sido negligenciados no rarefeito debate público brasileiro sobre o que colocar no lugar da Doutrina de Segurança Nacional (DSN).

Embora todas essas questões me preocupei como cidadão e pesquisador, decidi não tratar do caso brasileiro neste livro.<sup>1</sup> Para tentar entender os

problemas envolvidos nessa área da atuação governamental, preferi tomar distância das atribulações da conjuntura nacional e estudar as características gerais dos serviços de inteligência no Estado contemporâneo, bem como os desafios associados ao segredo governamental e aos mecanismos de controle público em regimes democráticos.

Decidi não estudar a atividade de inteligência tal como praticada no Brasil, mas sim os problemas analíticos associados à práxis dos serviços de inteligência no exterior. Exatamente por ter feito isso, considero o trabalho realizado pleno de consequências para a reflexão sobre o futuro dessas agências no Estado brasileiro. Em particular, espero ter contribuído para um conhecimento um pouco mais preciso sobre as dinâmicas operacionais características das agências de inteligência de outros países, a partir das quais se poderá verificar de que tipo de atividades de inteligência estamos falando quando se discutem as missões e prioridades das agências brasileiras. Da mesma forma, dadas as dificuldades associadas à tentativa de manter sob controle do público tais atividades, os diversos mecanismos de supervisão e prestação de contas analisados no trabalho podem ser contrastados com os mecanismos disponíveis no Brasil. Além de fornecer alguma evidência empírica e comparativa a partir da qual se poderá debater os rumos da atividade de inteligência no Brasil, o horizonte normativo sugerido pelo binômio agilidade/transparência permite uma reavaliação periódica dos avanços e recuos observados.

Obviamente, isso significa que considero a agilidade e a transparência como dois valores positivos, necessários para o “bom” desenho institucional de qualquer agência governamental. Ao reconhecer a existência dessa dimensão normativa ao longo de todo o texto, é preciso também destacar que a tentativa de interpretar a trajetória dos serviços de inteligência em termos de dificuldades organizacionais e operacionais empiricamente identificáveis para um desempenho institucional “ágil” e “transparente” não implica qualquer tipo de adesão comprehensiva ao objeto. Não gosto ou desgosto de serviços de inteligência, eles simplesmente existem, e embora eu preferisse viver num mundo em que eles não existissem porque o próprio Estado não mais precisasse existir, creio que não é boa atitude intelectual e moral simplesmente fingir que o problema não é de todos nós, cidadãos.

Foi a consideração realista da existência dessas organizações governamentais, contrastada com o desconhecimento cabal que a ciência política manifesta em relação às características mais importantes da área de inteligência (*modus operandi*, funções desempenhadas, desenho organizacional, *ethos* profissional, infra-estrutura tecnológica etc.), que motivou inicialmente este livro. Ao longo do trabalho, entretanto, passei a considerar o objeto e os problemas a ele associados ainda mais relevantes, porque sua análise crí-

tica permite considerar desde um ângulo particularmente difícil o tema da compatibilização entre mecanismos de prestação de contas (*accountability*) e o desiderato de capacidade governativa em situações complexas. Correspondendo à dimensão analítica do problema, creio também que as políticas públicas e as organizações da área de segurança nacional constituem um dos desafios político-práticos mais salientes de nosso tempo. Com tudo isso, só não chega a ser surpreendente que esse tipo de objeto tenha sido negligenciado tanto tempo entre nós porque devemos levar em conta o contexto da Guerra Fria no plano internacional e as seqüelas da ditadura militar no plano nacional.

Ao cabo, o que o estudo realizado aponta são severos constrangimentos para que os órgãos de inteligência e de segurança atualmente existentes na maioria dos países democráticos possam ser ágeis e transparentes. Como foi discutido nos capítulos 1 e 2, tais limitações são decorrentes não apenas do contexto político, mas da própria natureza operacional e organizacional dessas atividades.

Do ponto de vista operacional, a própria complexidade dos fluxos informacionais envolvidos na coleta de informações a partir de fontes singulares e sua integração adequada num ciclo produtivo que envolve ainda a análise e a disseminação para múltiplos usuários com demandas também especializadas é uma primeira limitação à operação ágil de qualquer sistema de inteligência. O segundo grande constrangimento operacional decorre das várias dinâmicas conflitivas envolvidas nas interações entre os esforços de obtenção de informações e a construção de redes de segurança, que envolvem medidas defensivas e ofensivas de proteção às informações.

Do ponto de vista organizacional, o segredo e a complexidade técnica associados aos fluxos informacionais na área de inteligência contribuíram ao longo do século para forjar as escolhas que consolidaram sistemas nacionais com muitas organizações, subsistemas verticalizados e delimitações funcionais precárias, responsáveis por disputas interburocráticas persistentes e que limitam a agilidade daqueles sistemas. Os mesmos fatores, ou seja, a especialização funcional, a complexidade organizacional, os requisitos tecnológicos e o segredo governamental também constrangem severamente o funcionamento dos mecanismos de controle externo que poderiam garantir a transparência das atividades governamentais na área de segurança nacional em geral, mas que são ainda mais agudos na área de inteligência.

As limitações à operação simultaneamente ágil e transparente de sistemas de inteligência podem e precisam ser reduzidas através de esforços de reforma e de controle, mas dificilmente serão eliminadas completamente em qualquer horizonte visível. Os conflitos políticos e a estrutura do siste-

ma internacional tendem a ser mais duradouros do que a própria ciência política fora capaz de antecipar no século XX. De todo modo, não seria uma empreitada simples “desinventar” os serviços de inteligência e de segurança, assim como não se pode simplesmente “desinventar” uma série de “males necessários” à operação de uma aparelhagem estatal complexa no mundo contemporâneo.

Portanto, mesmo reconhecendo que o Estado é simultaneamente uma fonte de segurança e de ameaça para os indivíduos, escrevi no capítulo 3 que a natureza do sistema internacional e das sociedades nacionais torna a segurança coletiva irredutível ao bem-estar dos indivíduos. Isso nos condena a tentar conviver da melhor forma possível (embora freqüentemente convivamos da pior forma imaginável) com as tensões inerentes à segurança nacional. E implica também uma atenção constante às instituições que materializam e simbolizam a segurança coletiva, desde as Forças Armadas e polícias até os sistemas judiciais e os serviços de inteligência.

Finalmente, o estudo das atividades de inteligência e de segurança do Estado também demonstrou a necessidade de revisão das abordagens que insistem em negar que os problemas associados ao uso da força e ao conhecimento instrumental sejam partes constitutivas da política em contextos democráticos.<sup>2</sup>

Os problemas abarcados pelos estudos estratégicos não são fenômenos “externos” à política, fenômenos que poderiam ser ignorados pelos cientistas políticos e pelos cidadãos, para não falar dos governantes e daqueles que têm a política como sua vocação. Pelo contrário, estou convencido ao final desse percurso que, da correta decifração dos problemas associados ao uso da força e da informação enquanto partes constitutivas da política depende, cada vez mais, aquilo que Charles Lindblom chamou certa vez de a “inteligência da democracia”.

## Notas

1. Para uma opinião mais detalhada sobre os desafios e dilemas da nova agência brasileira, ver Cepik & Antunes (1999). Entre os documentos oficiais, ver Oliveira (1999). Ver também, no âmbito do Programa Nacional de Proteção ao Conhecimento, a brochura Brasil. Agência Brasileira de Inteligência. (s.d.). Algumas poucas informações complementares podem ser obtidas na página da agência na internet: <[www.abin.gov.br](http://www.abin.gov.br)>. Existem poucos trabalhos acadêmicos sobre o caso brasileiro recente, e os melhores que conheço foram produzidos como dissertações de mestrado: Emilio (1992), Diniz (1994), Antunes (2000) e Quadrat (2000).

2. Para uma qualificação e um aprofundamento do debate sobre a extensão em que o liberalismo contemporâneo é capaz de reconhecer o duplo problema representado pelo capitalismo e pelo poder de Estado para a manutenção e a radicalização da democracia

no mundo contemporâneo, ver Barry (1991). Para um breve mapeamento do estado da teoria política contemporânea, ver os quatro ensaios de Isis M. Young, Bhikhu Parekh, Klaus von Beyme e Brian Barry na Parte VI (Political Theory) do volume editado por Goodin & Klingemann (2000).

## Referências bibliográficas

- ADLER, Emanuel; BARNETT, Michael (Ed.). *Security communities*. Cambridge: Cambridge University Press, 1998.
- AGEE, Philip. *Dentro da companhia: diário da CIA*. São Paulo: Civilização Brasileira, 1976.
- AID, Matthew M. The time of troubles: the US National Security Agency in the twenty-first century. *Intelligence and National Security*, v. 15, n. 3, p. 1-32, 2000.
- ALBERTS, David S. *Defensive information warfare*. Washington, DC: National Defense University, 1996.
- ALBUQUERQUE, Eduardo M. Aquém do ótimo: Kenneth Arrow, o mercado e a alocação de recursos para a pesquisa e a invenção. In: ALBUQUERQUE, Eduardo M. *Invenções, mutações: o progresso científico-tecnológico em Habermas, Offe e Arrow*. Belo Horizonte: UNA, 1996.
- ALMEIDA, Paulo Roberto. Relações internacionais. In: MICELI, Sérgio. (Org.) *O que ler na ciência social brasileira (1970-1995)*. São Paulo: Sumaré/Anpocs, 1999. v. 3, p. 191-255.
- ALMOND, Gabriel; POWELL Jr., G. Bingham. *Comparative politics: a developmental approach*. Boston: Little, Brown and Company, 1966.
- ANDREW, Christopher. France and the German menace. In: MAY, Ernest R. (Ed.) *Knowing one's enemies: intelligence assessments before the two World Wars*. Princeton-NJ: Princeton University Press, 1986a.
- \_\_\_\_\_. *Her majesty's secret service: the making of the British intelligence community*. New York: Viking Press, 1986b.
- \_\_\_\_\_; GORDIEVSKY, Oleg. *KGB: the inside story of foreign operations from Lenin to Gorbachev*. London: Hodder and Stoughton, 1990.
- \_\_\_\_\_; \_\_\_\_\_. *Instructions from the center*. London: Hodder and Stoughton, 1991.
- ANTUNES, Priscila. *Agência Brasileira de Inteligência: gênese e antecedentes históricos*. 2000. Dissertação (Mestrado em Ciência Política) – Universidade Federal Fluminense – UFF, Niterói.
- \_\_\_\_\_. *SNI e Abin: uma leitura da atuação dos serviços secretos brasileiros no século XX*. Rio de Janeiro: FGV, 2001.
- ARNOLD, Douglas. *The logic of congressional action*. New Haven: Yale University Press, 1990.

ARRIGHI, Giovanni. *O longo século XX: dinheiro, poder e as origens de nosso tempo*. São Paulo: Unesp, 1996.

ARROW, Kenneth. J. *The economics of information*. London: Harvard University Press, 1984. Collected Papers, v. IV.

BALACHADRAN, V. Intelligible intelligence: an alchemy of collation and coordination. *The Times of India*, 21 Sept. 2000. Disponível em: <<http://www.timesofindia.com>>.

BALL, Desmond; WINDREM, R. Soviet signals intelligence: vehicular systems and operations. *Intelligence and National Security*, v. 4, n. 1, 1989a.

\_\_\_\_\_, \_\_\_\_\_. Soviet signals intelligence: organization and management. *Intelligence and National Security*, v. 4, n. 4, 1989b.

BANCO MUNDIAL. *Relatório sobre o desenvolvimento mundial – o Estado num mundo em transformação*. Washington, DC: World Bank Group, 1997.

BARKER, Anthony; PETERS, B. Guy. (Eds.). *The politics of expert advice: creating, using and manipulating scientific knowledge for public policy*. Edinburgh: Edinburgh University Press, 1992.

BARRY, Brian. Is democracy special? In: BARRY, Brian. *Democracy and power: essays in political theory*. Oxford: Clarendon Press, 1991. v. 1, p. 24-60.

BAYLEY, David H. The police and political development in Europe. In: TILLY, Charles. (Ed.). *The formation of national states in Western Europe*. Princeton: Princeton University Press, 1975. p. 328-379.

BERKOWITZ, Bruce; GOODMAN, Allan. *Strategic intelligence for American national security*. 3 ed. Princeton: Princeton University Press, 1991.

\_\_\_\_\_, \_\_\_\_\_. *Best truth: intelligence in the information age*. New Haven: Yale University Press, 2000.

BOBBIO, Norberto. *O futuro da democracia: uma defesa das regras do jogo*. Rio de Janeiro: Paz & Terra, 1986.

\_\_\_\_\_. Público/privado. In: *Encyclopédia EINAUDI*. Lisboa: Imprensa Nacional – Casa da Moeda, 1989. v. 14 Estado – Guerra.

\_\_\_\_\_. Democracia e segredo. In: BOBBIO, Norberto; BOVERO, Michelangelo (Org.). *Teoria geral da política: a filosofia política e as lições dos clássicos*. Rio de Janeiro: Campus, 2000, p. 399-415.

\_\_\_\_\_, BOVERO, Michelangelo (Org.). *Teoria geral da política: a filosofia política e as lições dos clássicos*. Rio de Janeiro: Campus, 2000.

BOK, Sissela. *Secrets: on the ethics of concealment and revelation*. New York: Vintage Books, 1989.

BORCHERDING, Thomas (Org.). *Budgets and bureaucrats: the sources of government growth*. Durham: Duke University Press, 1977.

- BOWMAN, M. E. Intelligence and international law. *International Journal of Intelligence and Counterintelligence*, v. 8, n. 3, p. 321-335, 1995.
- BOYES, Jon L. (Ed.) *Issues in C<sup>3</sup>I program management: requirements, systems and operations*. Washington, DC: AFCEA Press, 1985.
- BRASIL. Agência Brasileira de Inteligência. *Legislação pertinente à salvaguarda de assuntos sigilosos*. Brasília, Abin, 1999a. 49p.
- \_\_\_\_\_. *Algumas dicas para salvaguardar o conhecimento na sua organização*. Programa Nacional de Proteção ao Conhecimento (PNPC), 1999b.
- \_\_\_\_\_. Escola Superior de Guerra. *Fundamentos doutrinários da ESG*. Rio de Janeiro, ESG, 1999.
- \_\_\_\_\_. Ministério da Ciência e Tecnologia. *Constituição da República Federativa do Brasil*. Brasília: Senado Federal, MCT, 1999. Constituições Brasileiras, v. VII.
- BRINT, Steven; KARABEL, Jerome. Institutional origins and transformations: the case of American community colleges. In: POWELL, Walter W.; DiMAGGIO, Paul J. (Ed.). *The new institutionalism in organizational analysis*. Chicago: University of Chicago Press, 1991, p. 337-360.
- BROWNE, J. P. R.; THURBON, M. T. *Electronic warfare*. London: Brassey's, 1998.
- BRUNEAU, Thomas C. *Intelligence and democratization: the challenge of control in new democracies*. Monterey: The Center for Civil-Military Relations at Naval Postgraduate School (NPS), Mar. 2000.(Occasional Paper n. 5).
- BUCHANAN, J. M. Why does government grow? In: BORCHERDING, Thomas (Org.). *Budgets and bureaucrats: the sources of government growth*. Durham: Duke University Press, 1991.
- BURROWS, William E. *Deep black: space espionage and national security*. New York: Berkeley Books, 1988.
- \_\_\_\_\_. Imaging space reconnaissance operations during the cold war: cause, effect and legacy. 1999. Disponível em: <<http://webster.hibo.no/asf>>.
- BUZAN, Barry. *People, states & fear: an agenda for international security studies in the post-cold war era*. 2 ed. rev. and updated. Boulder: Lynne Rienner Publishers, 1991.
- \_\_\_\_\_; WÆVER, Ole; WILDE, Jaap de. *Security: a new framework for analysis*. Boulder: Lynne Rienner Publishers, 1998.
- CALVINO, Italo. *Seis propostas para o próximo milênio*. São Paulo: Companhia das Letras, 2000.
- CAMPBELL, James. *Introduction to remote sensing*. New York: Guilford, 1987.
- CANADA. *The Canadian intelligence community: control and accountability*. Report of the Auditor General of Canada, Nov.1996. Disponível em: <<http://www.oag-bvg.gc.ca>>.

\_\_\_\_\_. Ministry of Supply and Services. *Canadian Security Intelligence Service Act.* R.S. 1985, as amended. Ottawa, 1999.

CAVAGNARI, Geraldo. Estratégia e defesa – 1960/1990. *Premissas*, n. 7, 1994.

CEPIK, Marco; ANTUNES, Priscila. A crise dos grampos e o futuro da Abin. *Conjuntura Política*, n. 8, jun. 1999. Disponível em: <<http://cevep.ufmg.br/bacp>>.

CHEIBUB, José A.; PRZEWORSKI, Adam. Democracy, elections and accountability for economic outcomes. In: PRZEWORSKI, Adam; STOKES, Susan; MANIN, Bernard (Eds.). *Democracy, accountability, and representation*. Cambridge: Cambridge University Press, 1999, p. 222-249.

COAKLEY, Thomas P. (Ed.). *C<sup>3</sup>I: Issues of command and control*. Washington, DC: NDU Press, 1991.

COMBS, Richard E.; MOORHEAD, John D. *The competitive intelligence handbook*. London: The Scarecrow Press, 1992.

CONSTANTINIDES, George C. *Intelligence and espionage: an analytical bibliography*. Boulder: Westview Press, 1983.

COX, Gary; McCUBBINS, Mathew. *Legislative Leviathan. Party government in the house*. Berkeley: University of California Press, 1993.

CREVELD, Martin van. *Command in war*. Cambridge: Harvard University Press, 1985.

CRONIN, Blaise; DAVENPORT, Elisabeth. *Elements of information management*. London: The Scarecrow Press, 1991.

DAHL, Robert. *Controlling nuclear weapons: democracy versus guardianship*. Syracuse: Syracuse University Press, 1985.

\_\_\_\_\_. *Poliarquia: participação e oposição*. São Paulo: Edusp, 1997.

DANDEKER, C. *Surveillance, power and modernity: bureaucracy and discipline from 1700 to the present day*. Cambridge, UK: Polity Press, 1990.

DANIEL, Donald C.; HERBIG, Katherine L. (Ed.). *Strategic military deception*. New York: Pergamon Press, 1982.

DAUDELIN, Jean. *Human security and development policy*. Ottawa: The North-South Institute/L'Institut Nord-Sud, 1999, 31p.

DAVIDSON, R. Social intelligence and the origins of the Welfare State. In: DAVIDSON, R.; WHITE, P. (Ed.). *Information and government: studies in the dynamics of policy-making*. Edinburgh: Edinburgh University Press, 1988, p. 14-38.

\_\_\_\_\_; WHITE, P. (Ed.). *Information and government: studies in the dynamics of policy-making*. Edinburgh: Edinburgh University Press, 1988.

DAVIES, Jack. *The challenge of opportunity analysis*. An intelligence monograph from CSI/CIA, CSI # 92-003U. Jul. 1992.

- \_\_\_\_\_. *Intelligence changes in analytic tradecraft in CIA's directorate of intelligence*. Washington, DC: DI/CIA, Apr. 1995.
- DAVIS, Curtiss O. *Hyperspectral imaging: utility for military, science, and commercial applications*. Washington, DC: Naval Research Laboratory, 1996.
- DEDIJER, S.; JÉQUIER, N. (Ed.). *Intelligence for economic development: an inquiry into the role of the knowledge industry*. Oxford: Berg, 1987.
- DERIAN, James Der. *Anti-diplomacy: spies, terror, speed and war*. Oxford: Blackwell, 1992.
- \_\_\_\_\_. Anti-diplomacy, intelligence theory and surveillance practice. *Intelligence and National Security*, v. 8, n. 3, p. 29-51, Jul. 1993.
- \_\_\_\_\_. The scriptures of security. *Mershon International Studies Review*, v. 42, p. 117-122, 1998.
- DEUTSCH, Karl. *The nerves of government*. New York: Free Press, 1966.
- DINIZ, Eugênio. *Antecedentes do Projeto Calha Norte*. 1994. Dissertação (Mestrado) – Universidade de São Paulo (USP).
- \_\_\_\_\_. Comentários ao plano de segurança do Executivo Federal. *Conjuntura Política*, n. 19, jun. 2000. Disponível em: <<http://cevep.ufmg.br/bacp>>.
- DOUGHERTY, James E.; PFALTZGRAFF, Robert L. Jr. *Contending theories of international relations: a comprehensive survey*. 4 ed. USA: Addison-Wesley, 1997.
- DUNLEAVY, Patrick. *Democracy, bureaucracy and public choice*. London: Harvester Wheatsheaf, 1991.
- \_\_\_\_\_; O'LEARY, Brendam. *Theories of the State: the politics of liberal democracies*. London: MacMillan, 1987.
- DUNNIGAN, James F. *How to make war: a comprehensive guide to modern warfare for the post-cold war era*. 3 ed. New York: William Morrow and Company, 1993.
- DURANT, A. Intelligence: issues in a word or in a field? *Social Intelligence*, v. 1, n. 3, 1991.
- DUTTON, Lyn et al. *Military space*. London: Brassey's, 1990.
- DWORKIN, Ronald. *Taking rights seriously*. Cambridge: Harvard University Press, 1978.
- \_\_\_\_\_. *Law's empire*. Cambridge: Harvard University Press, 1988.
- ELKINS, Dan. *An intelligence resource manager's guide*. Washington, DC: Joint Military Intelligence Training Center at DIA, 1997.
- ELSTER, Jon. *Pecas e engrenagens da ciências sociais*. São Paulo: Relume-Dumará, 1989.
- EMILIO, Luis A. Bitencourt. *O Poder Legislativo e os serviços secretos no Brasil: 1964-1990*. Dissertação (Mestrado) – Universidade Federal de Brasília (UnB), 1992.

ERICKSON, John. Threat identification and strategic appraisal by the Soviet Union: 1930-1941. In: MAY, Ernest (Ed.). *Knowing one's enemies: intelligence assessment before the two World Wars*. Princeton: Princeton University Press, 1984, p. 375-423.

ESTEVEZ, Eduardo E. Estructuras de control de los sistemas, organismos y actividades de inteligencia en los Estados democráticos. In: SEMINÁRIO INTERNACIONAL SOBRE LA INTELIGENCIA EN LAS ORGANIZACIONES DEL SIGLO XXI. Santiago. Anais... Santiago de Chile: Universidad de Chile, Oct. 2000.

EVANS, Peter B.; RUESCHEMEYER, Dietrich; SKOCPOL, Theda (Orgs.). *Bringing the State back in*. Cambridge: Cambridge University Press, 1985.

FERRIS, J.; HANDEL, Michael I. Clausewitz, intelligence, uncertainty and the art of command. *Intelligence and National Security*, v. 10, n. 1, Jan. 1995.

FISCHER, Ben B. *Okhrana: the Paris operations of the Russian imperial police*. Unclassified monography from the Center for the Study of Intelligence at CIA. 1997. Disponível em: <<http://www.cia.gov/csi/monograph>>.

FITZSIMONDS, James R. Intelligence and the revolution in military affairs. In: GODSON, Roy; SCHMITT, G.; MAY, E. (Eds.). *US intelligence at the crossroads: agendas for reform*. New York: Brassey's, 1995, p. 265-287.

FORD, H. P. *Estimative intelligence: the purposes and problems of national estimating*. Lanham-MD/London, University Press of America, 1993.

FRY, Michael G.; HOCHSTEIN, Miles. Epistemic communities: intelligence studies and international relations. *Intelligence and National Security*, v. 8, n. 3, p. 14-28, Jul. 1993.

GALEOTTI, Mark. *The Kremlin's agenda*. London: Jane's Intelligence Review Press, 1996.

GELLNER, Ernest. *Nações e nacionalismo*. Lisboa: Gradiva, 1993.

GIDDENS, Anthony. *The nation-State and violence*. Berkeley, Los Angeles: University of California Press, 1987.

GILL, Peter. *Policing politics: security intelligence and the liberal democratic State*. London: FrankCass, 1994.

\_\_\_\_\_. Reasserting control: recent changes in the oversight of the UK intelligence community. *Intelligence and National Security*, v. 11, n. 2, p. 313-331, Apr. 1996.

GODSON, Roy. (Ed.). *Intelligence requirements for the 1980's: intelligence and policy*. Lexington: Lexington Books, 1986.

\_\_\_\_\_. (Ed.). *Comparing foreign intelligence: the US, the USSR, the U. K. & the Third World*. London, Pergamon-Brassey's, 1988.

\_\_\_\_\_. *Dirty tricks or trump cards: US counterintelligence and covert action*. Washington, DC: Brassey's, 1995.

\_\_\_\_\_. Transstate security. In: GODSON, R.; SHULTZ, R.; QUESTER, G. *Security studies for the 21<sup>st</sup> century*. Dulles: Brassey's, 1997, p. 81-130.

- \_\_\_\_\_; ROBERTSON, Kenneth G. (Ed.). *British and American approaches to intelligence*. New York: St. Martin's, 1987.
- \_\_\_\_\_; SCHMITT, G.; MAY, E. (Ed.) *US intelligence at the crossroads: agendas for reform*. New York: Brassey's, 1995.
- \_\_\_\_\_; SHULTZ, Robert; QUESTER, George. *Security studies for the 21<sup>st</sup> century*. Dulles: Brassey's, 1997.
- GOLDSTEIN, R. J. *Political repression in nineteenth-century Europe*. London: Croom Helm, 1983.
- GOODIN, Robert E. Institutions and their design. In: GOODIN, Robert E. (Ed.). *The theory of institutional design*. Cambridge: Cambridge University Press, 1996a.
- \_\_\_\_\_. (Ed.). *The theory of institutional design*. Cambridge: Cambridge University Press, 1996.
- \_\_\_\_\_; KLINGEMANN, Hans-Dieter. *A new handbook of political science*. Oxford: Oxford University Press, 2000.
- HABERMAS, Jürgen *The structural transformation of the public sphere: an inquiry into a category of bourgeois society*. Cambridge: MIT Press, 1994a.
- \_\_\_\_\_. Carl Schmitt: los terrores de la autonomía. In: HABERMAS, Jürgen. *Identidades nacionales y postnacionales*. Madrid: Tecnos, 1994b.
- HALL, Peter; TAYLOR, Rosemary. Political science and the three institutionalisms. [editado posteriormente em *Political Studies*], 1996.
- HANDEL, Michael I. (Ed.). *Intelligence and military operations*. Great Britain: Frank Cass, 1990.
- HANSEN, James H. *Japanese intelligence: the competitive edge*. Washington, DC: NIBC Press, 1996.
- HASTED, Glenn P. Towards the comparative study of intelligence. *Conflict Quarterly*, p. 55-72, Summer 1991.
- HEDLEY, John Hollister. *Checklist for the future of intelligence*. Washington, DC: Institute for the Study of Diplomacy at Georgetown University, 1995.
- HELD, David. *Modelos de democracia*. Belo Horizonte: Paidéia, 1995.
- HENDERSON, Conway W. *International relations: conflict and cooperation at the turn of the 21st century*. New York: McGraw-Hill, 1998.
- HERMAN, Michael. Intelligence and policy: a comment. *Intelligence and National Security*, v. 6, n. 1, Jan. 1991.
- \_\_\_\_\_. Assessment machinery: British and American models. In: CONFERENCE ON INTELLIGENCE ANALYSIS AND ASSESSMENT: THE PRODUCER AND POLICYMAKER RELATIONSHIP IN A CHANGING WORLD. Proceedings Canada: Casis, 1994.

- \_\_\_\_\_. *Intelligence power in peace and war*. Cambridge: Cambridge University Press, 1996.
- \_\_\_\_\_. *Intelligence services in the information age*. London: FrankCass, 2001.
- HEUER Jr., Richards J. *Psychology of intelligence analysis*. Washington, DC: CSI/CIA, 1999.
- HEYMAN, Hans. Intelligence/policy relationships. In: MAURER, A. C.; TUNSTALL, Marion D.; KEAGLE, James M. (Ed.). *Intelligence: policy and process*. Boulder and London: Westview Press, 1985.
- HIBBERT, R. Intelligence and policy. *Intelligence and National Security*, v. 5, n. 1, Jan. 1990.
- HINDLEY, Meredith. First annual list of dissertations on intelligence. *Intelligence and National Security*, v. 13, n. 14, p. 208-230, Winter 1998.
- \_\_\_\_\_. Teaching intelligence project. *Intelligence and National Security*, v. 15, n. 1, p. 191-218, Spring 2000.
- HINSLEY, F. H. *British intelligence in the Second World War*. Abridged edition. London: HMSO, 1993.
- HOBBES, Thomas. *Leviatã, ou matéria, forma e poder de um Estado eclesiástico e civil*. [1651] São Paulo: Abril, 1974.
- HOLT, Pat M. *Secret intelligence and public policy: a dilemma of democracy*. Washington, DC: Congressional Quarterly Press, 1995.
- HULNICK, A. S. The intelligence producer-policy consumer linkage. *Intelligence and National Security*, v. 1, n. 2, May 1986.
- \_\_\_\_\_. The ames case: how could it happen? *International Journal of Intelligence and Counterintelligence*, v. 8, n. 2, Summer 1995.
- \_\_\_\_\_. Intelligence and law enforcement: the “spies are not cops” problem. *International Journal of Intelligence and Counterintelligence*, v. 10, n. 3, p. 269-286, Fall 1997.
- HUNTINGTON, Samuel P. *A ordem política nas sociedades em mudança*. [1968] São Paulo: Forense, 1975.
- \_\_\_\_\_. *A terceira onda: a democratização no final do século XX*. São Paulo: Ática, 1994.
- HURRELL, Andrew. Latin America’s new security agenda. *International Affairs*, v. 74, n. 3, p. 529-546, Jul. 1998.
- JARDIM, José Maria. *Transparência e opacidade do Estado no Brasil: usos e desusos da informação governamental*. Niterói, RJ: Eduff, 1999.
- JASANI, B. *Exploiting space for conventional defense and security*. London: Rusi, 1990.
- JELEN, George F. The defensive disciplines of intelligence. *International Journal of Intelligence and Counterintelligence*, v. 5, n. 4, p. 381-399, Winter 1991-1992.

- JESSOP, B. *State theory: putting capitalist States in their place*. Cambridge: Polity Press, 1990.
- JOHNSON, Loch K. Decision costs in the intelligence cycle. In: MAURER, A. C.; TUNSTALL, Marion D.; KEAGLE, James M. (Ed.). *Intelligence: policy and process*. Boulder, London: Westview Press, 1985, p. 181-198.
- \_\_\_\_\_. *America's secret power: the CIA in a democratic society*. Oxford: Oxford University Press, 1989.
- \_\_\_\_\_. *Secret agencies: US intelligence in a hostile world*. New Haven: Yale University Press, 1996.
- JONES, Archer. *The art of war in the western world*. Oxford: Oxford University Press, 1987.
- KAHANER, Larry. *Competitive intelligence: from black ops to boardrooms*. New York: Simon and Schuster, 1996.
- KAHN, David. *Hitler's spies*. New York: Macmillan, 1978.
- \_\_\_\_\_. Toward a theory of intelligence. *Military History Quarterly*, v. 7, n. 2, p. 92-97, 1995.
- \_\_\_\_\_. *The codebreakers: the comprehensive history of secret communication from the ancient times to the Internet*. New York: Scribner, 1996. [New edition revised and updated.]
- KANT, Immanuel. To perpetual peace: a philosophical sketch. In: KANT, Immanuel. *Perpetual peace and other essays*. Indianapolis: Hacket. [1795] 135-139. 1988.
- \_\_\_\_\_. *Textos seletos*. 2 ed. Petrópolis: Vozes, 1985.
- KENNEDY, Paul. *Ascensão e queda das grandes potências*. Rio de Janeiro: Campus, 1989.
- KENNEDY, William V. *The intelligence war*. London: Salamander Books, 1983.
- KENT, Sherman. *Strategic intelligence for American world policy*. Princeton: Princeton University Press, 1949.
- KEOHANE, Robert O. (Ed.). *Neorealism and its critics*. New York: Columbia University Press, 1986.
- KNIGHT, Amy. *Spies without cloaks: the KGB's successors*. Princeton: Princeton University Press, 1996.
- KRASNER, Stephen D. *Sovereignty: organized hypocrisy*. Princeton: Princeton University Press, 1999.
- KREHBIEL, Keith. *Information and legislative organization*. Ann Arbor: The University of Michigan Press, 1992.
- KRIZAN, Lisa. *Intelligence essentials for everyone*. Washington, DC: JMIC, 1999.
- LAFFIN, John. *The Brassey's book of espionage*. London: Brassey's, 1996.

- LAGÔA, Ana. *SNI: como nasceu, como funciona*. São Paulo: Brasiliense, 1983.
- LIBICKI, Martin C. *What is information warfare?* Washington, DC: Institute for National Strategic Studies at the National Defense University, 1995.
- LIJPHART, Arend (Ed.). *Parliamentary versus presidential government*. Oxford: Oxford University Press, 1992.
- LIMONGI, Fernando. O novo institucionalismo e os estudos legislativos: a literatura norte-americana recente. In: *BIB – Boletim de Informação Bibliográfica em Ciências Sociais*, n. 37, p. 3-38, 1º sem. 1994.
- LIPSCHUTZ, Ronnie (Ed.). *On security*. New York: Columbia University Press, 1995.
- LOWENTHAL, M. K. The burdensome concept of failure. In: MAURER, A. C.; TUNSTALL, Marion D.; KEAGLE, James M. (Ed.). *Intelligence: policy and process*. Boulder, London: Westview Press, 1985.
- \_\_\_\_\_. Tribal tongues: intelligence consumers, intelligence producers. *The Washington Quarterly*, p. 157-168, Winter 1992.
- \_\_\_\_\_. *The national security council: an organizational assessment*. Washington, DC: Library of Congress, 1993.
- \_\_\_\_\_. *US intelligence community: an annotated bibliography*. New York: Garland, 1994.
- \_\_\_\_\_. *Intelligence: from secrets to policy*. Washington, DC: CQ Press, 2000.
- LÖWI, Theodore. *The end of liberalism*. 2 ed. New York: W.W. Norton, 1979.
- \_\_\_\_\_; GINSBERG, Benjamin. *American government*. New York: W. W. Norton, 1992.
- LUBAN, David. The publicity principle. In: GOODIN, Robert E. (Ed.). *The theory of institutional design*. Cambridge: Cambridge University Press, 1996, p. 154-198.
- LUSTGARTEN, L.; LEIGH, Ian. *In from the cold: national security and parliamentary democracy*. Oxford: Clarendon Press, 1994.
- LYMAN, Michael D. *The police: an introduction*. Upper Saddle River: Prentice Hall, 1999.
- MARCH, James G.; OLSEN, Johan P. The new institutionalism: organizational factors in political life. *American Political Science Review*, v. 78, n. 3, p. 734-749, 1984.
- \_\_\_\_\_. *Rediscovering institutions: the organizational basis of politics*. New York: Free Press, 1989.
- \_\_\_\_\_. *Democratic governance*. New York: Free Press, 1995.
- MARCHETTI, Victor; MARKS, John. *The CIA and the cult of intelligence*. New York: Times Books, 1979.

- MARSHALL, Mark. Teaching vision. In: SWENSON, Russell (Ed.). *A flourishing craft: teaching intelligence studies*. Washington, DC: JMIC, 1999, p. 57-84.
- MARTIN, Frederick T. *Top secret intranet: how US intelligence built Intelink*. Upper Saddle River: Prentice Hall, 1999.
- MAURER, A. C.; TUNSTALL, Marion D.; KEAGLE, James M. (Ed.). *Intelligence: policy and process*. Boulder, London: Westview Press, 1985.
- MAY, Ernest R. (Ed.). *Knowing one's enemies: intelligence assessments before the two World Wars*. Princeton: Princeton University Press, 1984.
- MCDONALD, John W. Exploiting battlespace transparency: operating inside an opponent's decision cycle. In: PFALTZGRAFF, Robert L. Jr.; SHULTZ, Richard H. Jr., *War in information age: new challenges for US security*. Washington/London: Brassey's, 1997, p. 143-168.
- MCLEAN, Ian. (Ed.). *Concise dictionary of politics*. Oxford: Oxford University Press, 1996.
- MELO, Carlos Ranulfo Félix. *Retirando as cadeiras do lugar: migração partidária na Câmara dos Deputados (1985-1998)*. 1999. Tese (Doutorado) – Universidade Federal de Minas Gerais, Belo Horizonte.
- MELTON, H. Keith. *The ultimate spy book*. New York: DK Publishing, 1996.
- MILNER, Helen V. *Interests, institutions and information: domestic politics and international relations*. Princeton: Princeton University Press, 1997.
- MIYAMOTO, Shiguenoli. O estudo de relações internacionais no Brasil: o estado da arte. *Revista de Sociologia e Política*, n. 12, p. 83-98, 1999.
- MOE, Terry. The politics of structural choice: toward a theory of public bureaucracy. In: WILLIAMSON, Oliver E. (Ed.). *Organizational theory: from Chester Barnard to the present and beyond*. New York: Oxford University Press, 1990.
- NISKANEN, W. A. *Bureaucracy and representative government*. Chicago: Aldine Atherton, 1977.
- NORTH, Douglas. *Institutions, institutional change and economic performance*. 1990.
- ODOM, William. *Modernizing intelligence: structure and change for the 21st century*. Washington: National Institute for Public Policy, 1997.
- O'DONNELL, Guillermo. Democracia delegativa?. *Novos Estudos Cebrap*, n. 31, 1991.
- OLIVEIRA, Lúcio Sérgio Porto. *A história da atividade de inteligência no Brasil*. Brasília: Abin, 1999.
- OLLIGSCHLAEGER, Andreas M. Criminal intelligence databases and applications. In: PETERSON, Marilyn (Ed.). *Intelligence 2000: revising the basic elements*. Sacramento: Ialeia/Leiu, 2000.
- OSTROM, Elinor. *Governing the commons: the evolution of institutions for collective action*. New York: Cambridge University Press, 1990.

- \_\_\_\_\_. Rational choice theory and institutional analysis: toward complementarity. *American Political Science Review*, v. 85, n. 1, p. 237-243, Mar. 1991.
- O'TOOLE, George J. A. Kahn's law: a universal principle of intelligence? *International Journal of Intelligence and Counterintelligence*, v. 4, n. 1, p. 39-46, 1990.
- OXLEE, G. J. *Aerospace reconnaissance*. London: Brassey's, 1997.
- PARRISH, Michael. *Soviet security and intelligence organizations (1917-1990): a biographical dictionary and review of literature in English*. Westport: Meckler Corp, 1991.
- PARSONS, D. Wayne. *Public policy: an introduction to the theory and practice of policy analysis*. London: Elgar, 1995.
- PERROW, Charles. *Complex organizations: a critical essay*. 3 ed. San Francisco: McGraw-Hill, 1986.
- PETERSON, Marilyn. (Ed.). *Intelligence 2000: revising the basic elements*. Sacramento: Ialeia/Leiu, 2000.
- \_\_\_\_\_. *Applications in criminal analysis*. Westport: Greenwood Press, 1994.
- PETTIT, Philip. Institutional design and rational choice. In: GOODIN, Robert E. (Ed.). *The theory of institutional design*. Cambridge: Cambridge University Press, 1996.
- PFALTZGRAFF, Robert L. Jr.; SHULTZ, Richard H. Jr. *War in information age: new challenges for US security*. Washington/London: Brassey's, 1997.
- PICKET, George. Congress, the budget and intelligence. In: MAURER, A. C.; TUNSTALL, Marion D.; KEAGLE, James M. (Ed.). *Intelligence: policy and process*. Boulder, London: Westview Press, 1985.
- POGGI, Gianfranco. *A evolução do Estado moderno: uma introdução sociológica*. Rio de Janeiro: Zahar, 1978.
- POLMAR, N. ; ALLEN, T. B. *Spy book: encyclopedia of espionage*. New York: Random House, 1997.
- PORCH, Douglas. *The French secret services: from the Dreyfus affair to the Gulf war*. New York: Farrar, Straus & Giroux Publishers, 1995.
- POWELL, Walter W.; DiMAGGIO, Paul J. (Ed.). *The new institutionalism in organizational analysis*. Chicago: The University of Chicago Press, 1991.
- PRADOS, John. *President's secrets wars: CIA and Pentagon covert operations from World War II through the Persian Gulf*. Chicago: Elephant Books, 1996.
- PRATES, Antônio Augusto. Organização e instituição no novo institucionalismo. *Teoria & Sociedade*, n. 5, p. 123-146, Jun. 2000.
- PROENÇA Jr., Domício; DINIZ, Eugênio. *Política de defesa no Brasil: uma análise crítica*. Brasília: UnB, 1998.
- \_\_\_\_\_. Segurança e estudos estratégicos. In: BRIGAGÃO, Clóvis. (Org.). *Estratégia de negociações internacionais*. Rio de Janeiro: Aeroplano-Faperj, 2001, p. 341-380.

- \_\_\_\_\_; RAZA, Salvador. *Guia de estudos de estratégia*. Rio de Janeiro: Jorge Zahar, 1999.
- PRZEWORSKI, Adam. *Ama a incerteza e serás democrático*. *Novos Estudos Cebrap*, n. 9, p. 36-46, Jul. 1984.
- \_\_\_\_\_. *Estado & economia no capitalismo*. Rio de Janeiro: Relume-Dumará, 1985.
- \_\_\_\_\_; STOKES, Susan; MANIN, Bernard (Ed.). *Democracy, accountability, and representation*. Cambridge: Cambridge University Press, 1999.
- PUTNAM, Robert. *Comunidade e democracia: a experiência da Itália moderna*. Rio de Janeiro, FGV, 1996.
- QUADRAT, Samantha Viz. *Poder e informação: o sistema de inteligência e o regime militar no Brasil*. Dissertação (Mestrado) – Universidade Federal do Rio de Janeiro, 2000.
- REIS, Bruno P. W. *Modernização, mercado e democracia: política e economia em sociedades complexas*. Tese (Doutorado) – Rio de Janeiro, Instituto Universitário de Pesquisa Econômica do Rio de Janeiro, 1997.
- REIS, Fábio Wanderley. Institucionalização política (comentário crítico). In: MICELI, Sérgio. (Org.) *O que ler na ciência social brasileira (1970-1995)*. São Paulo: Sumaré/Anpocs, 1999.
- RICHELSON, Jeffrey T. *Sword and shield: soviet intelligence and security apparatus*. Cambridge: Ballinger, 1986.
- \_\_\_\_\_. *Foreign intelligence organizations*. Cambridge: Ballinger Publishing Company, 1988.
- \_\_\_\_\_. *A century of spies: intelligence in the twentieth century*. Oxford: Oxford University Press, 1995.
- \_\_\_\_\_. *The US intelligence community*. Cambridge: Ballinger Publishing Company, 1999.
- \_\_\_\_\_; BALL, Desmond. *The ties that bind: intelligence cooperation between the Ukusa countries*. Boston: Allen & Unwin, 1985.
- ROBERTSON, Kenneth G. (Ed.). *British and American approaches to intelligence*. London: Macmillan Press; New York: St. Martin's, 1987. (RUSI Defence Studies Series.)
- SAINT-PIERRE, Hector. Racionalidade e estratégias. *Premissas*, n. 3, 1993.
- SARTORI, Giovanni. *A teoria da democracia revisitada*. São Paulo: Ática, 1994. v. 1-2.
- SCHEPPELE, Kim Lane. *Legal secrets: equality and efficiency in the common law*. Chicago: Chicago University Press, 1988.
- SCHUMPETER, Joseph. *Capitalismo, socialismo e democracia*. [1942] Rio de Janeiro: Zahar, 1984.

- SHEPSLE, Kenneth; LAVER, Michael. Government accountability in parliamentary democracy. In: PRZEWORSKI, Adam; STOKES, Susan; MANIN, Bernard. (Ed.). *Democracy, accountability, and representation*. Cambridge: Cambridge University Press, 1999, p. 279-296.
- \_\_\_\_\_; WEINGAST, Barry. (Ed.). *Positive theories of congressional institutions*. Ann Arbor: The University of Michigan Press, 1995.
- SHILS, Edward A. *The torment of secrecy*. Chicago: Ivan R. Dee Inc., 1996.
- SHOEMAKER, Christopher C. *The NSC staff: counseling the council*. Boulder: Westview Press, 1991.
- SHULSKY, Abram. *Silent warfare: understanding the world of intelligence*. New York: Brassey's, 1992.
- \_\_\_\_\_. What is intelligence? Secrets and competition among states. In: GODSON, Roy; SCHMITT, G.; MAY, E. (Ed.). *US intelligence at the crossroads: agendas for reform*. New York: Brassey's, 1995.
- SHULTZ, Richard; GODSON, Roy. *Dezinformatzia: active measures in Soviet strategy*. McLean: Pergamon-Brassey's, 1984.
- SIMS, Jennifer. What is intelligence? Information for decision makers. In: GODSON, Roy; SCHMITT, G.; MAY, E. (Ed.). *US intelligence at the crossroads: agendas for reform*. New York: Brassey's, 1995.
- SMIST, Frank J. Jr. *Congress overseas the United States intelligence community: 1947-1989*. Knoxville: University of Tennessee Press, 1991.
- SNIDER, L. Britt. Intelligence and law enforcement. In: GODSON, Roy; SCHMITT, G.; MAY, E. (Ed.). *US Intelligence at the crossroads: agendas for reform*. New York: Brassey's, 1995.
- SPRUYT, Hendrik. *The sovereign state and its competitors*. 2 ed. Princeton: Princeton University Press, 1996.
- STANLEY, Harold W.; NIEMI, Richard G. *Vital statistics on American politics*. 5 ed. Washington, DC: Congressional Quarterly Press, 1995.
- STARES, P. B. *Command performance: the neglected dimension of European security*. Washington, DC: Brookings, 1991.
- STEELE, Robert D. *On intelligence: spies and secrecy in an open world*. United States: AFCEA Intl., 2000.
- STEINMO, Sven; THELEN, Kathleen; LONGSTRETH, Frank. (Ed.). *Structuring politics: historical institutionalism in comparative analysis*. Cambridge: Cambridge University Press, 1992.
- STEPAN, Alfred. *Rethinking military politics: Brazil and the Southern Cone*. Princeton: Princeton University Press, 1988.

- STRAYER, Joseph. *On the medieval origins of the modern State*. Princeton: Princeton University Press, 1970.
- SUN TZU. *A arte da guerra*. 5 ed. Rio de Janeiro: Record, 1985.
- SWENSON, Russell. *Intelligence for multilateral decision and action*. Washington, DC: JMIC, 1997.
- \_\_\_\_\_. *A flourishing craft: teaching intelligence studies*. Washington, DC: Joint Military Intelligence College, 1999 [Occasional Paper n. 5].
- TERRIFF, Terry. Environment degradation and security. In: GODSON, Roy; SHULTZ, Robert; QUESTER, George. *Security studies for the 21<sup>st</sup> century*. Dulles: Brassey's, 1997, p. 253-287.
- THOMPSON, James W.; PADOVER, Saul K. *Secret diplomacy, espionage and cryptography: 1500-1815*. New York: Ungar Publisher, 1965.
- THOMPSON, John B. *The media and modernity: a social theory of the media*. Stanford: Stanford University Press, 1996.
- THOMSON, Janice E. State sovereignty in international relations: bridging the gap between theory and empirical research. *International Studies Quarterly*, n. 39, p. 213-233, 1995.
- TILLY, Charles. Western state making and theories of political transformation. In: TILLY, Charles. *The formation of national State in Western Europe*. Princeton: Princeton University Press, 1975a.
- \_\_\_\_\_. (Ed.). *The formation of national States in Western Europe*. Princeton: Princeton University Press, 1975b.
- \_\_\_\_\_. War making and state making as organized crime. In: EVANS, Peter B.; RUESCHEMEYER, Dietrich; SKOCPOL, Theda. (Orgs.). *Bringing the State back in*. Cambridge: Cambridge University Press, 1985, p. 169-191.
- \_\_\_\_\_. *Coerção, capital e Estados europeus: 1990-1992*. São Paulo: Edusp, 1996.
- US CONGRESS. *Senate select committee to study governmental operations with respect to intelligence activities* (Church Committee). 94th Cong., 1st Session (1975): v.1: *Unauthorized storage of toxic agents*; v. 4: *Mail opening*; v.5: *National security agency and fourth amendment rights*; v.7: *Covert action; final report*, S. 94-755, Books I-VI. 1975.
- \_\_\_\_\_. *House select committee on intelligence* (Pike committee). *US intelligence agencies and activities*. Hearings, 94th Cong., 1st Session (1975). Pt. 1, *Intelligence costs and fiscal procedures*; Pt. 2, *The performance of the intelligence community*; Pt. 5, *Risks and control of foreign intelligence; final report*. House report. 94-833. 1976.
- \_\_\_\_\_. *The foreign intelligence surveillance act of 1978: the five first years*. Senate Report 98-660, 98th Congress, 2nd session. p. 8-23, 1984.

- \_\_\_\_\_. *Intelligence oversight in selected democracies*. A report prepared by John Prados and Richard A. Best Jr. Congressional Research Service (CRS). Sept. 21 1990.
- \_\_\_\_\_. *James Woolsey testimony*. SSCI, February the 2nd, 1993. 1993a.
- \_\_\_\_\_. *Intelligence successes and failures in operation Desert Shield/Desert Storm*. House Committee on Armed Services. 103th Congress, 1st Session, 1993. House Print 103-05. 1993b.
- \_\_\_\_\_. *Legislative oversight of intelligence activities; the US experience*. Senate Select Committee on Intelligence (SSCI). Report, 103<sup>rd</sup> Congress, Second Session, Oct. Senate Print. 1994.
- \_\_\_\_\_. *IC21: Intelligence community in the 21st century*. Staff Study. House Permanent Select Committee on Intelligence. Washington, DC, GPO. 1996.
- \_\_\_\_\_. *US national security programs and issues: statement of Keith R. Hall, Director of the NRO*. Washington, DC, Senate Armed Services Committee Strategic Force Subcommittee, Mar. 1998a.
- \_\_\_\_\_. *Compilation of intelligence laws and related laws and executive orders of interest to the national intelligence community*. Washington, DC, GPO. 1998b.
- US GOVERNMENT. *National security strategy of engagement and enlargement*. Washington, DC, White House, 1995.
- \_\_\_\_\_. *Evaluation report on measurement and signature intelligence*. Washington, DC, Office of the Inspector General at the Defense Department, Jun. 30. [PO97-301]. 1997a.
- \_\_\_\_\_. *Intelligence community information systems strategic plan: enabling a more agile intelligence enterprise (AIE)*. Washington, DC, Intelligence Systems Board/CMS, Nov. 1997b.
- \_\_\_\_\_. *Report of the commission on protecting and reducing government secrecy*. Pursuant to public law. Chairman of the Commission: Daniel P. Moynihan. Washington-DC, GPO. 1997c.
- \_\_\_\_\_. *Multispectral applications: the final report on the joint DIA-OSAF/DSPO merit program for evaluating Landsat, SPOT and aircraft multispectral imagery*. Washington, DC, DIA. 1998.
- \_\_\_\_\_. *A consumer's guide to intelligence*. Washington, DC, CIA Public Affairs Office. 1999a.
- \_\_\_\_\_. *Annual report for the United States intelligence community*. Washington, DC, Office of the Director of Central intelligence (ODCI), May. 20 1999b.
- \_\_\_\_\_. *Community operational definition of the AIE* (Coda). Washington, DC, Office of Advanced Analytical Tools/CIA. 1999c.
- \_\_\_\_\_. *Joint Intelligence Virtual Integration (Jiva)*. Washington, DC, Jiva Integration Management Office/DIA. 1999d.

- \_\_\_\_\_. *Global trends 2015: a dialogue about the future with nongovernment experts*. Washington, DC, NIC/ODCI, Dec. 2000.
- \_\_\_\_\_. *Public disclosure of the aggregate intelligence budget figure*. Washington, DC, HPSCI/GPO. 103<sup>rd</sup> Congress, 2<sup>nd</sup> Session. 1994.
- US SENATE. *Nomination of George J. Tenet as DCI*. Senate Hearing 105-314. 105<sup>th</sup> Congress, 1<sup>st</sup> Session. May 6, 1997.
- \_\_\_\_\_. *Special report of the select committee on intelligence activities: 1997-1998*. Washington, DC, SSCI/GPO. 106th Congress, 1st Session, Report 106-3. 1999.
- VARLEJS, J. (Ed.). *The economics of information in the 1990's*. London: McFarland, 1995.
- VICKERS, Michael J. The revolution in military affairs and military capabilities. In: PFALTZGRAFF, Robert L. Jr.; SHULTZ, Richard H. Jr. *War in information age: new challenges for US security*. Washington/London: Brassey's, 1997.
- WÆVER, Ole. Insecurity, security and a-security in the West European non-war community. In: ADLER, E.; BARNETT, M. (Eds.). *Security communities*. Cambridge, UK: Cambridge University Press, 1998.
- WAGENEN, James Van. A review of congressional oversight. 1997. In: *Studies in intelligence*: Disponível em: <<http://www.odci.gov.csi/studies/97unclass/wagenen.html>>.
- WALT, Stephen M. The renaissance of security studies. *International Studies Quarterly*, n. 35, p. 211-239, 1991.
- WALTZ, Kenneth M. *Theory of international politics*. Reading: Addison-Wesley Publishing Company, 1979.
- \_\_\_\_\_. The emerging structure of international politics. *International Security*, p. 44-79, Fall 1993.
- WATSON, Patrick. The FBI's changing mission. In: GODSON, Roy; SCHMITT, G.; MAY, E. (Eds.). *US intelligence at the crossroads: agendas for reform*. New York: Brassey's, 1995.
- WEBER, Max. *Economía y sociedad*. Buenos Aires: Fondo de Cultura Económica, 1992.
- \_\_\_\_\_. *Ciência e política: duas vocações*. São Paulo: Cultrix, 1993a.
- \_\_\_\_\_. *Parlamento e governo na Alemanha reordenada*. [1918]. Petrópolis, Vozes. 1993b. Ver principalmente os capítulos II (Domínio dos burocratas e liderança política) e IV (A direção burocrática na política externa).
- WELLER, Geoffrey. Comparing Western inspectors general of intelligence and security. *International Journal of Intelligence and Counterintelligence*, v. 9, n. 4, p. 383-406, 1997.
- \_\_\_\_\_. Political scrutiny and control of Scandinavia's security and intelligence services. *International Journal of Intelligence and Counterintelligence*, v. 13, n. 2, p. 171-192, 2000.

- WILENSKY, Harold. *Organizational intelligence: knowledge and policy in government and industry*. New York: Basic Books, 1967, p. viii.
- WILLIAMS, Kieram; DELETANT, Dennis. *Security intelligence services in new democracies: the Czech Republic, Slovakia and Romania*. London: St. Martin's Press, 2001.
- WILLIAMSON, Oliver E. (Ed.). *Organizational theory: from Chester Barnard to the Present and beyond*. New York: Oxford University Press, 1990.
- WILSON, James Q. *Bureaucracy: what government agencies do and why they do it*. United States: Basic Books, 1989.
- WILSON, Vice Admiral Thomas R. [Director of DIA]. *Military threats and security challenges through 2015: statement for the record*. Washington, DC: SSCI, Feb. 2000.
- WOHLSTETTER, Roberta. *Pearl Harbor: warning and decision*. Stanford: Stanford University Press, 1962.
- WOLF, Marcus; McELVOY, Anne. *O homem sem rosto*. Rio de Janeiro: Record, 1997.
- WOODWARD, Bob. *Veil: the secret wars of the CIA: 1981-1987*. New York: Simon & Schuster, 1987.
- YOUNG, Robert J. French military intelligence and nazi Germany, 1938-1939. In: MAY, Ernest R. (Ed.). *Knowing one's enemies: intelligence assessments before the two World Wars*. Princeton: Princeton University Press, 1984, p. 273-274.
- ZEGART, Amy. *Flawed by design: the evolution of the CIA, JCS and NSC*. Stanford-CA: Stanford University Press, 1999.
- ZIEGLER, C.; JACOBSEN, David. *Spying without spies: origins of America's secret nuclear surveillance system*. Connecticut: Praeger, 1995.