Inteligência: dinâmicas operacionais

Marco Cepik

1 O que é inteligência?

Há três usos do termo - como toda informação coletada para atender demandas de um tomador de decisão, ou uma camada específica do tratamento analítico numa pirâmide informacional. A sofisticação dos sistemas de informação tornou corrente o uso do termo para designar uma função de suporte informacional à tomada de decisões - nessa acepção, inteligência é o mesmo que conhecimento ou informação analisada.

Inteligência, para nossos propósitos, refere-se a fluxos informacionais estruturados. Mas a inteligência a que nos referimos é a feita sobre informação coletada sem o consentimento, cooperação ou conhecimento dos alvos da ação. Esta inteligência pode ser *segredo* ou informação secreta. O conceito deve ser mantido à vista, diante dos conceitos de *informação* excessivamente amplo e *espionagem* excessivamente estrito.

Para superar esta tensão, é necesssário uma segunda dimensão do conceito estrito - a dimensão analítica, ou seja, a inteligêcia se diferencia da informação por sua capacidade explicativa ou preditiva, através de um trabalho sequencial num estágio de coleta e um estágio de análise a partir da *single-sources collection* e de outras fontes (*all-sources analysis*).

A diferença entre a análise de inteligência e a análise de outros órgãos está nos fins - o conhecimento sobre adversários e problemas (*situational awareness*), ou seja, compreensão de relações adversariais nas quais há esforços de desinformar e negar conhecimento, mesmo que o alvo seja doméstico. Quanto mais públicas as fontes de informação e menos conflitivos os temas, menos a inteligência tem a contribuir.

Diplomatas e adidos também enviam relatórios a seus países de origem, mas suas fontes são mais ostensivas e não cessam seu fluxo de informação quando o alvo aumenta suas contramedidas de segurança. Isso explica por que diplomatas suspeitos de espionagem são declarados *personae non grata* e expulsos - sua coleta de informações é de uma natureza diferente.

No caso de operações militares há também a diferença entre informações de combate e inteligência - aquelas obtidas no contato com o inimigo e controladas pelo *staff* de operações. Nem sempre é fácil aplicar este critério de controle e meios de coleta, como na guerra do Golfo de 1991, na qual a coalizão era apoiada por satélites, analistas da CIA, Pentágono, bem como recursos comandados pela *staff* de inteligência. Ou seja, uma maior integração operacional pode turvar o controle operacional de recursos específicos de inteligência. A confusão é especialmente grande em inteligência de sinais[1]. Recentemente o conceito de guerra informacional (IW) tem sido usado tanto para a coleta quanto para a negação de informação de combate quanto de inteligên-

[1] Durante a II Guerra Mundial, na batalha da Inglaterra foi decisiva a informação de combate dos radares britânicos, enquanto na batalha do Atlântico foi decisivo o esforço de longo prazo de inteligência de decodificação de sinais.

cia.

Os pontos centrais de distinção, portanto, são o grau de intervenção humana requerido para análise e disseminação, grau de vulnerabilidade de fontes e necessidade de segredo.

1.1 O ciclo da inteligência

As descrições convencionais destacam 10 passos, mas destacaremos especialmente as etapas de coleta e análise.

1. Requerimentos informacionais
2. Planejamento
3. Gerenciamento dos meios de coleta
4. Coleta de fontes singulares
5. Processamento
6. Análise de fontes diversas
7. Produção de relatórios
8. Disseminação dos produtos
9. Consumo pelos usuários
10. Avaliação (*feedback*).

O ciclo de inteligência é um modelo ideal que não existe em nenhum sistema real. No entanto, o processo é complexo e dinâmico, e a parte importante do conceito de ciclo é entender a existência de fluxos informacionais entre diferentes atores.

Pode-se pensar no ciclo da inteligência também como parte do ciclo de políticas públicas, com o surgimento de problemas, estabelecimento de agendas, formulação de linhas de ação, tomadas de decisão, implementação e avaliação. Nesse sentido, as informações coletadas e analisadas deveriam ser determinadas pelas necessidades dos usuários.

A principal diferença entre planejamento geral da coleta e gerenciamento dos meios é a atividade altamente técnica e complexa do gerenciamento. Um dos problemas que surge com o ciclo é que autores assumem que ele é dirigido pelos requerimentos informacionais dos usuários finais, o que induz expectativas exageradas sobre a orientação dos processos decisórios governamentais - que em geral não especificam as informações de que precisam nem sua finalidade. A agência também pode falhar em entender que informações seriam úteis ao usuário.

Caberia aos responsáveis pela área detalhar, completar e priorizar demandas, portanto. Embora crucial, há aqui também um risco de "intromissão", a ser mitigado por avaliação sistemática da satisfação dos usuários e por mecanismos de controle. Há ferramentas para identificar as necessidades dos usuários, como taxonomia de problemas, listas de questões-chave e matriz de tempestividade e escopo - mas muitos usuários comunicam suas necessidades diretamente à coleta, enquanto analistas têm requerimentos mais amplos para atualizações de bases de dados ou compreensão mais ampla de alvos.

1.2 Coleta e processamento

Atividades especializadas de coleta absorvem até 90% dos investimentos na área de inteligência. O volume de dados brutos coletados é muito maior do que os relatórios recebidos pelos usuários finais. Os meios de coleta definem disciplinas especializadas:

1.2.1 HUMINT

Obtida a partir de fontes humanas. É a mais antiga e barata, e o uso do termo evita o uso da palavra *espionagem* - à qual a atividade não se resume. Distinguem-se os oficiais de inteligência e suas fontes, algumas das quais são agentes. Apenas as fontes são espiões *per se*, geralmente dissidentes locais.

Na base da pirâmide de *HUMINT* estão as fontes com acesso de menor sensitividade, como turistas e viajantes, especialistas, refugiados e as-

sim por diante, que as organizações entrevistam para manter um mapa geral de informações.

Quando se passa para a busca *ativa* por informações, tentando solicitar certa informação (*tasking*), entramos numa camada intermediária de informantes *ad hoc*, exilados, partidos de oposição, etc., que podem ter consciência ou não que têm um relacionamento com um serviço de inteligência.

No topo da pirâmide estão fontes secretas e regulares de maior valor agregado, ainda que menos numerosas. São agentes conscientes, recrutados (por dinheiro, ideologia, chantagem) ou voluntários (*walk-ins*). Agentes voluntários são vistos com muita desconfiança, mas desconfiança excessiva pode impedir acesso a uma boa fonte. A história mostra que fontes em cargos menos importantes tendem a ser mais estáveis.

Cabe ainda distinguir os oficiais de inteligência que operam com "cobertura oficial" - os que operam num corpo diplomático com outro papel oficial, protegidos pela imunidade diplomática. O uso excessivo da cobertura oficial facilita o trabalho de contra-inteligência e limita os tipos de pessoas com quem os oficiais podem trabalhar.

Os oficiais "sem cobertura oficial" (NOCs ou "ilegais") dão maior variedade ao disfarce empregado e flexibilidade às operações. Por outro lado, pode limitar o acesso ao mundo oficial, e expor os quadros do serviço a um risco muito maior.

HUMINT é também o tipo mais problemático de inteligência, com a imensa pressão sofrida por agentes recrutados até o controle de credibilidade de informações. Além de esforços de contra-espionagem, há tendência das próprias fontes de preencher vácuos com informações fabricadas (*paper mills*). Há grandes riscos, bem como longos processos de recrutamento e problemas de comunicação

Apesar das limitações, HUMINT é insubstituível, especialmente para descobrir intenções. Até hoje outras disciplinas não puderam substituir o grau de compreensividade que documentos fornecem, e é crucial também para outras disciplinas - como na obtenção de livros de códigos para uso pela SIGINT. Diante desse traço flexível e especializado, organizações de HUMINT tendem a ser multifinalitárias e também desenvolver novas formas de coleta técnica.

1.2.2 SIGINT

Historicamente a SIGINT se originou com a interceptação, decodificação, tradução e análise de mensagens por uma terceira parte. Atualmente, se divide em COMINT (*communications intelligence*) e ELINT (*electronics intelligence*).

A primeira se dá na interceptação e pré-análise de comunicações, excetuando-se rádio e televisão. Também se pode obter informação analisando o tráfego de mensagens (*traffic analysis*) e técnicas de localização de transmissores (*direction finding* - DF).

A segunda se trata de interceptar sinais eletromagnéticos não-comunicacionais, com exceção dos sinais emitidos por explosões nucleares, que são analisados pela MASINT. Durante a guerra fria, se expandiu para aquisição de alvos, navegadores, detecção submarina, teleguiagem e sistemas de comando, controle, comunicações e inteligência (C3I).

A facilidade de interceptação depende do método de transmissão, frequências empregadas e o uso ou não de medidas defensivas. A forma mais segura de transmitir informações é não transmiti-las, mas comunicações cabeadas também são mais seguras. A interceptação de cabos de fibra ótica é especialmente custosa e pouco eficiente. A coleta de dados transmitidos pelo ar

é mais simples, aumentando a importância de medidas de segurança (*comsec*) e a necessidade de contramedidas eletrônicas (ECM) no caso de sistemas militares.

Somente pelos satélites Intelsat, passa mais de dois terços de todo o tráfego eletrônico internacional. A capacidade de países grandes de garantir a segurança de suas comunicações, portanto, é muito superior a países menores. Já em 1995 a agência central de SIGINT americana, a NSA, era capaz de interceptar 125 terabytes a cada três horas.

O problema, portanto, é a agilidade no processamento de tantos dados, considerando a relação de 1 milhão de *inputs* para cada informação relatável. Nos anos 1990 a NSA não era capaz de processar mais de 1% da informação coletada.

Desde 1960, a plataforma mais importante de coleta são satélites de vigilância eletrônica e interceptação, que constituem a maioria dos satélites-espiões. Há três tipos de satélites de SIGINT:

- Os satélites para interceptação de sinais eletrônicos não comunicacionais, em órbitas circulares de baixa altitude, ou *ferrets*, que após upgrades na década de 1990 podem interceptar sinais de telemetria de mísseis;
- Os satélites de interceptação de comunicações, em órbitas geossíncronas e ângulos de inclinação próximos ao zero, são capazes de cobrir, cada um, 42% da superfície da terra;
- Os satélites de interceptação de comunicações de alta latitude, considerando que acima dos 70 graus a órbita geoestacionária só intercepta sinais muito distorcidos. Em órbitas elípticas com altitude de 450km no perigeu e 40.000km no apogeu, passam pelos polos a cada 12 horas.

As fontes de SIGINT também podem ser classificadas numa pirâmide de sensitividade, quantidade e valor. Na base estão comunicações sem codificação, no meio está a análise de tráfego e DF, e no topo está a comunicação codificada de alto valor estratégico.

1.2.3 IMINT

O surgimento da inteligência de imagens como disciplina especializada é posterior ao uso da aviação militar para reconhecimento e vigilância (como os balonistas da Revolução), especialmente a partir da associação entre o uso de câmeras e plataformas aeroespaciais na Primeira Guerra Mundial. Com a posterior sofisticação tecnológica, os sistemas especializados de IMINT marcaram a dinâmica competitiva e conflitiva entre Estados Unidos e União Soviética.

Os riscos da violação do espaço aéreo e a ameaça da defesa aérea levou a uma limitação do uso de voos clandestinos, mas até 1960 os EUA utilizaram aviões de altitude U-2, por algum tempo inalcançáveis por interceptores soviéticos, mas isto não durou muito.

No começo da década de 1960 os primeiros satélites espiões já foram postos em órbita. Desde então as potências que conseguem coletar IMINT a partir do espaço aceitou tacitamente a inevitabilidade desses sobrevoos. Além de não serem uma violação de espaço aéreo, é possível compensar a rotação da terra em torno do Sol de forma a obter sempre a mesmas condições de luz solar. Operam a baixas altitudes - os KH-11 Advanced operavam a um perigeu de apenas 241km.

Desde 1980 as imagens são transmitidas diretamente aos analistas ou usuários, e uma única missão de satélite corresponde à amplitude de muitos esquadrões inteiros de aviões especializados em condições ideais. Hoje os satélites são também capazes de explorar outras partes do espectro eletromagnético - como sensores

infravermelhos capazes de operar à noite, e a formação de imagens a partir do uso de radares de abertura sintética (SAR) - que, ainda que com resolução pior, podem ser usadas através de coberturas de nuvens.

Há certas limitações - especialmente os custos de obtenção, que limita muito os países capazes de obter a tecnologia necessária. Herman destaca três aspectos: a interpretação essencialmente humana, que demanda pessoas de formação demorada; a limitação das imagens fixas, considerando o *trade-off* entre cobertura e passagens sobre uma mesma coordenada; e que não se pode ver o que está devidamente escondido. A "revolução da imagem" tornou a camuflagem muito mais poderosa.

1.2.4 MASINT

Esta é a área de inteligência derivada de mensuração e 'assinaturas'. O termo não tem a coerência das três disciplinas tradicionais, mas agrupa uma série de sensores especializados como, por exemplo, imagens hiperespectrais e multiespectrais, a interceptação de sinais de telemetria de mísseis estrangeiros, fenômenos geofísicos (magnéticos, sísmicos e acústicos), mensuração de radioatividade, etc.

De acordo com Richelson, há pelo menos três tipos de satélites americanos dedicados à coleta de MASINT: o *Defense Support Program*, capaz de detectar o lançamento e monitorar a trajetória de mísseis, identificando seu tipo de combustível e as assinaturas espectrais de diferentes sistemas; o *Navstar Global Positioning System* (GPS), equipado com sistemas de detecção de explosões nucleares Nudet por raios X, gama e pulso eletromagnético; e os satélites meteorológicos de uso militar (DMSP), equipados com sensores de radiação eletromagnética e *tracking* de fragmentos nucleares na atmosfera.

Outros meios envolvem plataformas aerotransportadas para coletar amostras de agentes químicos e bacteriológicos, estações fixas para vigilância de mísseis, laboratórios sismológicos, radares passivos para monitorar veículos de reentrada, redes de hidrofones, entre outras. A principal função é a coleta de informações sobre características singulares - assinaturas - de diferentes sistemas de armas e equipamentos.

1.2.5 OSINT

A inteligência de fontes ostensivas (*open source intelligence*) tem se tornado cada vez mais importante a partir da explosão informacional. Consiste na obtenção de informações não restritas, cujo acesso é permitido sem restrições especiais, como pelo monitoramento da mídia e de fontes disponíveis.

Durante a Guerra Fria um programa da CIA e da US Air Force resumia e/ou traduzia quase todas as publicações técnicas e científicas da União Soviética, e em 1992 a CIA monitorava 790 horas semanais de programação de TV em 50 países e 29 línguas diferentes. Os responsáveis pela coleta tendem a ser os departamentos encarregados da etapa da análise.

Uma característica comum é a enorme necessidade de processamento e pré-análise de grandes volumes de informação. A quantidade de dados brutos é desproporcional. Uma consequência da dificuldade no processamento de grandes volumes de informação é o envio de inteligência efêmera ou de uso imediato para o usuário final sem passar pela análise e produção final.

Segundo Herman, os coletores são especialistas em "disciplinas", com fontes, tecnologias e técnicas peculiares, e os analistas são especialistas em temas, áreas e problemas.

1.3 Análise e disseminação

Nesta atividade é crucial diferenciar a produção de conhecimento relevante da defesa de um curso de ação específico. Isto é mais uma norma que uma realidade, mas permanece relevante. Nesse sentido, a ética profissional da atividade de análise é a da pesquisa, e como na pesquisa os padrões de qualidade, isenção e relevância podem estar abaixo do esperado.

Por outro lado, os problemas variam conforme as necessidades dos usuários, que devem ser classificadas de acordo com os tipos de inteligência resultantes. Kent (1949) as dividia segundo a função esperada e o foco temporal - em inteligência sobre fatos correntes (relatorial), características estáveis (descritiva) ou tendências futuras (prospectiva). Um quarto tipo seria sobre ameaças menos imediatas, ou de alerta.

As categorias mais utilizadas ainda se organizam em disciplinas acadêmicas, como inteligência política, militar, científica e tecnológica, econômica e sociológica. Os alvos se dividem em transnacionais, regionais, nacionais e subnacionais. De acordo com Kahn e Herman, a diferença crucial seria entre as "coisas e capacidades" e "significados". Diferentes métodos de coleta e análise seriam adequados a cada um desses tipos - mas na prática a maioria dos meios lida com ambos os tipos de inteligência. Em geral a SIGINT fornece tanto localizações quanto comunicações, mas isso não quer dizer que seja inerentemente superior à IMINT.

O que existe são diferentes tipos de adaptabilidade e afinidade entre disciplinas e áreas de análise. A vulnerabilidade da inteligência de sinais a contramedidas é maior que a da IMINT, por exemplo - por isso o que importa são os problemas analíticos a serem resolvidos.

O próprio esforço de categorizar a atividade é uma necessidade administrativa e um imperativo epistemológico, para organizar categorias de investimento, por exemplo. A alocação hipotética da OTAN, nesse sentido, indica continuidade em relação à Guerra Fria nesse ponto específico.

Além de avaliar tendências e descrever a realidade, os produtos visam também antecipar eventos cruciais. As bases de dados para referência são uma camada intermediária fundamental que alimenta produtos de curto e longo prazo. A qualidade das bases de dados e dos analistas são os principais indicadores da qualidade de uma organização de inteligência.

Disseminação tende a ser o elo mais sensível do ciclo, porque a diversidade de usuários é muito grande e suas necessidades respondem a ritmos temporais específicos. Já que a avaliação é uma espécie de usuário, e certos relatórios não passam pela avaliação, a disseminação e avaliação tendem a se confundir. Há também a avaliação e indicadores de desempenho e qualidade dos produtos de inteligência, bem como formas de monitorar a satisfação dos usuários durante e após a disseminação.

O Intelink, rede que integra as organizações americanas, mostra ainda outra novidade, os fluxos virtuais de trabalho. A complexidade, problemas de relacionamento, requisitos, limitações e problemas de *feedback* são desafios à dinâmica operacional interna do ciclo da atividade de inteligência.

2 Segurança de informações e contra-inteligência

A dinâmica operacional mais importante da inteligência é seu conflito com as medidas tomadas por um alvo para proteger suas informações. Enquanto a inteligência busca obter informações para direcionar a decisão, a segurança de infor-

mações (*infosec*) busca proteger a informação contra essa descoberta.

A incompreensão da dinâmica conflitiva é comum - não se tratam da mesma coisa. As missões são cumpridas por organizações distintas, sendo a *infosec* uma responsabilidade dos comandos militares e função gerencial das organizações civis. A confusão vem da relação algo sinérgica entre estas funções - mas sua relação é mais complexa que uma dicotomia ofensivo/defensivo.

Segurança informacional se forma por três componentes: contramedidas de segurança (SCM), formada pelas medidas de proteção que espelham as capacidades de coleta do oponente (como armazenamento especial, regras de custódia, restrições de acesso, criptografia, camuflagem na área militar, treinamentos para resistir a interrogatórios, etc.); contra-inteligência (CI), que além de contra-espionagem alcança a neutralização de operações de coleta, varredura de meios de coleta, interceptação de aeronaves, etc; e segurança de operações (Opsec), como o conjunto de procedimentos que visam identificar informações sobre equipamentos, capacidades e intenções que seriam críticas para um adversário, buscando negar seu acesso. Envolve, também, redução de emissões (EMCON), bem como áreas na fronteira com a SCM, como as operações de desinformação.

Estes componentes vão do defensivo ao ofensivo, mas a razão principal para sua diferenciação é organizacional. Ainda é comum referir-se à CI para designar o conjunto de funções da Infosec como um todo.

Isto não é tão importante, mas sim a clareza sobre especificidades operacionais e os fins de cada componente. DE modo geral as funções de CI são alocadas a organizações de inteligência exterior e interna, enquanto as de segurança são parte de organizações civis e militares especializadas. Opsec é por definição uma função do estado maior das organizações militares.

A contra-inteligência tende a construir todo um ciclo em contraposição às operações de inteligência, considerando a diversidade de meios da inteligência "positiva". No entanto, é especialmente a dimensão ativa da contra-espionagem que distingue a contra-inteligência dos demais aspectos da *infosec* e recomenda a alocação de responsabilidades. Assim, a CI pertence simultaneamente à inteligência e segurança de informações.

A atividade da CI pode ser vista como em muitas camadas, tomando uma série de conflitos interminaveis entre inteligência e contra-inteligência - havendo mesmo infiltração entre serviços de contra-inteligência. Como nos conflitos clausewitzeanos "reais", não acompanham a descida aos extremos, o que impede regressões infinitas. Esta é, porém, uma área nebulosa e esotérica.

A CI tem, também, muito conhecimento defensivo a oferecer à *infosec* em geral. Melhores capacidades defensivas ajudam também a obter inteligência, de forma indireta. Ainda que ameaças se tornem mais difíceis de identificar, os temas da segurança de informações se tornam cada vez mais centrais.

3 Operações encobertas

Estas operações têm nomes distintos e atividades variadas. Há dois aspectos fundamentais a serem analisados - os tipos de operações e a relação entre as operações encobertas e as atividades de coleta, análise e contra-inteligência.

Estas operações são usadas para manipular aspectos econômicos, sociais e políticos de outro ator. Enquanto recurso de poder, são instrumentais para implementar políticas e precisam manter plausibilidade na negação da autoria. São,

portanto, coercitivas e enfatizam a negação da autoria.

Podem ser classificadas em escala e intensidade do uso de força e em plausibilidade da negação de autoria. Quanto maior a escala e o uso da força, menor é a plausibilidade que a negação enseja. Destacam-se quatro tipos de operações encobertas.

O primeiro tipo é o mais extremado, envolvendo o apoio a grupos existentes para operações paramilitares e de guerrilha. O envolvimento varia de fornecimento de equipamento até envolvimento em treinamento e forças especiais. Um segundo grupo, os *wet affairs*, são apoio a golpes, assassinatos e incursões irregulares. O terceiro tipo envolve operações de sabotagem econômica e política e assistência secreta, como na campanha da CIA para evitar a vitória comunista nas eleições italianas de 1947. O quarto tipo abarca um conjunto de medidas para influenciar as percepções de um governo ou da sociedade por desinformação e agentes de influência, além de propaganda. Este é o tipo mais comum.

A intensidade do uso dessas operações variou ao longo da Guerra Fria e declinou de modo geral com seu fim. Em anos recentes, as mais importantes ocorreram no Iraque, Líbia e Iugoslávia, além do suporte a governos aliados no combate a insurgências e operações de guerra informacional. Em 1998, o orçamento em operações encobertas para a derrubada de Hussein chegou a 97 milhões de dólares. A principal razão do uso dessas operações é a economia de meios políticos, permitindo a negação do envolvimento aberto.

Se a inteligência é um *input* informacional para processos de decisão, operações encobertas não tem esse caráter, e a conexão é principalmente histórica e pela capacidade de gerir recursos de HUMINT. Há algo arbitrário na conexão - o serviço secreto britânico conduziu operações encobertas desde sua fundação, mas durante a Segunda Guerra Mundial o SOE e o PWE não estavam sob o comando do serviço de inteligência. A CIA só concentrou estas responsabilidades em 1952.

A condução das operações tende a impactar a dinâmica operacional das funções informacionais, além de dividir duas culturas diferentes. Este é um dos problemas menores, mas afeta diretamente a dinâmica operacional da área de inteligência.

4 A função da inteligência

A resposta mais direta é que governantes esperam maximizar seu poder desenvolvendo capacidades de inteligência. A literatura destaca oito utilidades principais: contribuir para um processo decisório racional e realista; produção de especialização de tomadores de decisão; o apoio direto ao planejamento de capacidades defensivas; o apoio direto de negociações diplomáticas; o subsídio do planejamento de planos militares; o alerta contra ataques surpresa; o monitoramento de alvos e ambientes prioritários para reduzir incertezas; e a preservação do segredo sobre as necessidades informacionais, fontes, fluxos, métodos e técnicas.

Grandes eventos históricos são relativamente raros - o papel da inteligência é menos dramático do que se poderia pensar. Normalmente a atividade otimiza o papel do ator estatal, ao invés de transformá-lo radicalmente; mesmo na guerra predominam os efeitos de otimização, permitindo uma gestão eficiente de recursos humanos, melhor sobrevivência em combate e bom desempenho do comando. Permite também reduzir o tempo para o ciclo de tomada de decisões (e do ciclo OODA).

Quando a inteligência causa grandes transfor-

mações, normalmente o resultado se dá por boa qualidade de análise, não apenas de coleta. O excesso de coleta sem análise pode, inclusive, prejudicar as instâncias de comando.

Para Kahn, a função predominante de otimização seria uma das três características centrais da inteligência - as outras duas seriam mais visíveis no meio militar, envolvendo a capacidade combatente e a associação com a defesa. Segundo O'Toole, disso se desdobram quatro corolários - a ênfase na defesa tende a ser acompanhada pela ênfase na inteligência; a ênfase no ataque tende a ser acompanhada pela ênfase na contra-inteligência; em situações de empasse os dois lados tendem a buscar inteligência; e operações ofensivas que se tornam defensivas tendem a aumentar a ênfase na inteligência.

Herman, porém, indica que historicamente estas "leis" não são absolutas, pois a superioridade em inteligência reflete uma superioridade militar já existente - destacando-se que o desenvolvimento de capacidades de inteligência é demorado e depende de experiência prévia.

Em resumo, inteligência não garante a vitória nem prevê o futuro. A complexidade e o volume de informações, bem como os riscos associados a contramedidas, obrigam a coleta a conviver com uma dose de segredo, refreamento e redundância com limites claros à agilidade e transparência. Por fim, em geral os governos contam com a inteligência para reduzir incertezas nas decisões e aumentar a segurança nacional e seu posicionamento internacional, embora a mesma ser decisiva em certos momentos de crise e conflito.

Intelligence Power

Michael Herman

1 3 - Recursos, etapas e objetos

Faz-se uma distinção formal entre a inteligência 'estratégica', as agências centrais e nacionais, e os recursos 'táticos', sob o controle de comandos militares. A maioria dos países emprega apenas inteligência estratégica, que serve, se necessário, também a propósitos táticos.

As instituições russas, embora muito menores que as soviéticas, podem ainda trazer consigo muito poder, considerando seus recursos e satélites de inteligência. Os EUA empregam mais de 10% do orçamento de defesa em inteligência (até 200.000 pessoas, incluindo a inteligência tática), enquanto outros países continentais da OTAN tipicamente utilizam de 3% a 5% (a Grã-Bretanha utiliza cerca de 10.000 pessoas).

Inteligência é comparativamente barata, e um governo pode comprar muita pelo preço de um fragata. Mas o total é alto, e a inteligência tem precisado de grandes organizações.

A inteligência é um processo sequencial e interno - da coleta 'de fonte única', na forma de relatórios escritos, à análise 'de fonte múltipla', que busca transformar toda a informação disponível num produto de inteligência finalizado. Chega-se então à disseminação ao mundo externo de decisão e política (usuários). Pode também haver um passo intermediário entre análise e disseminação, a criação de relatórios interdepartamentais especiais.

1.1 Coleta

O maior investimento está na coleta. As fontes coletadas são muito mais volumosas do que os relatórios produzidos, na proporção de 10 para 1. Durante a Guerra Fria esta proporção pode ter passado de 100 para 1.

O modelo de investimento se aproxima da indústria petrolífera - em altos custos de entrada e extração e maior valor agregado ao longo de etapas de refino de menor custo. 90% dos custos estão na coleta, e nos EUA da década de 1970 87% dos custos da coleta estavam na coleta técnica - SIGING e IMINT, frente aos 13% em HUMINT. A coleta é uma mistura de linhas de produção estabelecidas com uma busca constante por novas fontes, conforme as antigas falham.

Outra razão deste balanço é que a coleta técnica também inclui pré-processamento, exploração e interpretação - o *output* não são dados brutos. Outras tarefas, como transcrições e traduções, são igualmente intensivas no uso de mão de obra.

Esta pré-interpretação que integra a coleta também fornece *feedback* à coleta inicial, guiando-a ao material mais rico - os resultados iniciais da coleta de imagens determinam que cobertura extra será necessária. Agências de HUMINT também integram testes em suas fontes, buscando sinais de inconfiabilidade ou desinformação.

Pode haver, hoje, tantas pessoas no pré-processamento quanto há na coleta em si. Isso permite que algumas linhas de inteligência efê-

mera vão direto ao usuário, sem passar pela análise de fonte múltipla.

Agências 'de fonte única' usam também os resultados de outras agências para guiar seu próprio processo de coleta - ou seja, a coleta, não apenas a análise, se dá à luz de todo o conhecimento disponível. Fluxos de aliados estrangeiros podem também integrar o processo.

1.2 Análise e finalização

A coleta moderna, portanto, se funde à própria análise, e a interpretação permeia ambas. A inteligência se guia por evidência, que surge no processamento. Há uma troca contínua entre fatos e interpretação, e não uma separação rígida.

A interpretação de agências de coleta de fonte única carrega autoridade considerável, também diante de seu pessoal muito mais numeroso que as agências de fonte múltipla. Ainda assim, a análise de fonte múltipla tem alguma capacidade de questionar as interpretações e chegar à evidência original - um sistema saudável tem intersecções e trocas constantes.

É ainda valioso separá-las. Produtores de fonte única analisam legitimamente, e para tal usam outras fontes e relatórios de fonte múltipla como fundo. A diferença crucial está nas *responsabilidades* - a coleta se faz por especialistas em técnicas, a análise se faz por especialistas em assuntos - e é da análise a responsabilidade final pela interpretação e avaliação da evidência.

Cabe também à análise não dar valor especial à evidência secreta simplesmente porque ela é secreta, e sim construir uma visão diante de todo o conhecimento disponível. Os resultados de boa coleta podem ser perdidos se não forem bem interpretados pela análise de fonte múltipla.

A etapa interagências é rara, cara e restrita a assuntos importantes aos tomadores de decisão. No entanto, permanece uma base importante para conclusões de alto nível.

1.3 Disseminação

O objetivo da disseminação é entregar um produto útil na hora certa ao tomador de decisão. Inteligência eficaz depende de boa comunicação com os usuários - como redes dedicadas inteligência-usuário, como o Ultra. Na guerra do Golfo, uma investigação congressional concluiu que uma das maiores falhas da inteligência foi não conseguir disseminar inteligência, especialmente imagens, aos usuários no interior do teatro.

Toda inteligência é produzida contra pressões de tempo - há, ainda, que se considerar a agenda burocrática dos tomadores de decisão. Disseminação tende a ser o calcanhar de Aquiles da inteligência.

A relação entre a inteligência e seus usuários externos é o que determina sua utilidade - ainda que a maior parte das ligações se deem entre coletores e analistas. Daí se tem que a inteligência precisa tratar os receptores externos como se fossem os "clientes" finais - boas organizações veem muito bem seus usuários dentro e fora do mundo da inteligência. Compreender as necessidades dos usuários é importante, e *vender* a informação não deixa de ser crucial à consideração dada ao relatório final. Inteligência não é um processo impessoal.

A variedade de usuários finais também é relevante, incluindo leitores de alto nível, mas um grande número de departamentos inferiores que usam a inteligência como forma de desenhar suas recomendações de políticas. Também diplomatas, comandos militares, polícias e forças militares policiais fazem uso da inteligência, e algumas empresas podem precisar dela para executar contratos públicos.

Não há treinamento em como ser um usuário de inteligência e levá-la a sério. O misticismo ajuda nisso, mas dificulta a compreensão. É uma parte menor da vida de oficiais do que telegramas diplomáticos e estatísticas.

A inteligência, portanto, desafia a definição como uma lista de produtos entregue a usuários limitados, excessivamente ampla para tal. Há ainda, porém, outra foma de defini-la, em categorias separadas - importante para objetivos gerenciais e orçamentários. Pode ser dividida em interna e externa, em alvos geográficos, ou de acordo com seus assuntos. Na prática estas distinções se misturam.

1.4 Categorias

1.4.1 Inteligência externa e de segurança

A maioria da inteligência é colhida de alvos externos. A de segurança tem alvos muito diferentes, inclusive incluindo a contra-inteligência interna. Na prática, porém, se misturam - o IRA cruza fronteiras, e a inteligência britânica o acompanha. Ameaças internas não são, necessariamente, advindas dos próprios cidadãos de um Estado.

Por isso não há distinções rígidas, mas a inteligência de segurança tem algumas características próprias. Tem alguma afinidade com forças policiais, no tema de detectar atividades internas; seu *status* menor reflete o estado das ameaças internas. Por isso a tradição da KGB foi de segurança interna, com extensões externas para monitorar a ameaça contra-revolucionária externa.

1.4.2 Alvos geográficos

A divisão em alvos geográficos sempre fez sentido, do Pacto de Varsóvia ao Oriente Médio e China. Ameaças específicas, como o contencioso das ilhas Malvinas, também tendem a criar categorias.

As estatísticas geográficas não refletem corretamente o orçamento direcionado a alvos não-estatais e alvos internacionais sem uma identidade geográfica específica, visto que a inteligência colhida de alvos soviéticos nunca se restringiu à URSS geográfica. Esta divisão tem aumentado, e os alvos hoje são menos países e mais assuntos, como a proliferação nuclear.

1.4.3 Assuntos

A divisão comum é entre rótulos de inteligência política, militar e econômica. Esta classificação tem outras fraquezas, visto que alguns sistemas cobrem múltiplos alvos, satélites são rapidamente reorientados para categorias diferentes e outros sistemas são aspiradores imensos que só classificam sua coleta após a obtenção. A inteligência política cobre tanto política interna quanto externa.

Algo pode ser dito sobre classes arbitrárias, porém - o maior segmento da inteligência externa sempre foi a de defesa, no sentido amplo, e provavelmente permanece a maior classe em orçamento. Os alvos se estendem a empresas de defesa, exportadoras e tentativas internacionais de controle de proliferação de armas. Há também a enorme massa de informação necessária dos locais onde as forças de um Estado estão engajadas.

A inteligência de defesa se estende a atividades militares estrangeiras, insurreições com e sem apoio externo, violência, subversão inspirada pelo exterior, e uso de forças armadas. A inteligência nessas áreas se une a notícias públicas, mas a história mostrou a necessidade pela suplementação em situações militares complexas.

Outras áreas são menores. Inteligência 'política' de outros Estados (interna) é extremamente barata, com o apoio de fontes abertas e relatórios

de embaixadas. Inteligência política externa - sobre o pensamento e política externa de outros Estados - é o outro lado da moeda, e se une ao que pode ser visto como 'apoio diplomático'. Inteligência encoberta adiciona aos relatórios diplomáticos algo como 10% de seu conteúdo, adicionando confirmações e praticidades. Apoio imediato a negociações é também importante, e 'ver a mão alheia' sempre foi uma parte significativa da diplomacia.

A inteligência econômica viu um crescimento desde os 3% americanos de 1975, mas a 'interna' sempre foi relativamente barata - visto que muitas das fontes mais valiosas são abertas. Informação tática assim obtida é valiosa, mas não torna os serviços de inteligência uma grande autoridade no assunto.

A categoria também se une a outras, conforme inteligência sobre lavagens de dinheiro, *bad actors* e inteligência econômica colhida sobre comércio de material físsil pode também ser descrita sob outras categorias.

Há também contra-inteligência, usada numa variedade de sentidos: uma divisão especializada na agência nacional de HUMINT é comum. Aqui é utilizada para se referir a toda 'inteligência sobre a inteligência estrangeira', por qualquer meio.

No Ocidente sempre teve um orçamento reduzido, mas sua penetração na KGB e GRU foi valiosa. Trata-se de uma 'batalha entre profissionais', mas os riscos são altos, porque um agente numa posição sênior tem resultados muito maiores do que na batalha entre agências.

O que se chama de 'contra-espionagem' detecta ataques estrangeiros de espionagem e os neutralizando - enquanto a contra-inteligência ataca a inteligência adversária 'de dentro'. Hoje, o maior alvo é o terrorismo, o que foi três quartos do trabalho do BSS em 1994, com foco no terrorismo irlandês.

1.4.4 Categorização

O esforço de inteligência não pode ser facilmente categorizado, considerando suas intersecções e meios que se confundem e auxiliam - uma qualidade caleidoscópica que se aproxima da diplomacia.

Uma divisão hipotética, porém, pode ser construída a partir de dados da primeira metade da década de 1990:

Defesa, incluindo proliferação e comércio de armas 35% Vigilância de conflitos e insurgência 15% Política e economia de outros Estados 10% Apoio tático à diplomacia e negociações 10% Terrorismo (interno e externo) 20% Contra-inteligência, contra-espionagem e outros 10%

1.5 Atividades associadas

A mais importante atividade associada é preservar a segurança dos próprios segredos, num apoio que vai além da contra-espionagem. Há também o apoio internacional da inteligência, bem como o engano, militar e de desinformação. Conecta-se também com a guerra eletrônica, embora esta seja um esforço separado.

O esforço mais bem conhecido é a 'ação encoberta', de agentes de influência e propaganda até o apoio direto a grupos de oposição - coisas feitas em tempo de paz que não estão nos canais diplomáticos e oficiais. Agências de HUMINT tendem a se relacionar à ação encoberta por seus contatos e habilidades de organização de recursos humanos.

A ação encoberta, porém, é apenas uma pequena parte das agências de HUMINT. Se é ou não

parte da inteligência é uma questão de semântica - todas as agências têm diversas atividades correlacionadas. Em 1987, apenas 3% do pessoal da CIA estava envolvido.

1.6 Conclusão

A inteligência ocidental é duas coisas - a coleta de informação por *meios* especiais, e o estudo de *assuntos* especiais a partir desta informação. Na prática a ligação não é sempre completa, e as etapas se modificam de acordo com necessidades e circunstâncias.

É uma atividade considerável, mas não enorme, definida por orçamentos nacionais. A coleta é a etapa mais custosa, e SIGINT e IMINT são mais custosas do que HUMINT.

Em termos de organização, distingue-se inteligência externa de inteligência de segurança, embora as duas se interseccionem. Geograficamente o maior alvo era o alvo soviético, e presumivelmente hoje os alvos são mais espalhados, embora a proliferação de agentes não-estatais complique estas descrições.

Os fatores marcantes são o tamanho grande e continuado da inteligência de defesa, a importância da ameaça do terrorismo e o papel de apoio à diplomacia.

2 10 - Inteligência e segurança

Governos não querem apenas boas informações e previsões, mas controlar que informações próprias os outros podem acessar. Nesse sentido, analisaremos os efeitos da inteligência.

A proteção de informação é *segurança de informação*, ou *infosec*. Ela não deve ser confundida com a *inteligência de segurança* ou inteligência interna, já discutida. A segurança de informação apoia a segurança nacional, mas não se limita a esta área de atuação.

Os esforços internos de segurança de informação incluem tentativas de frustrar espionagem externa, e a segurança externa emprega medidas militares para proteger segredos militares e diplomáticos.

Na prática, alguns tipos de segurança de informação se misturam com proteção física contra ameaças, como o controle de acesso a prédios oficiais. Mas a segurança aqui considerada é aquela que protege a informação - a que traz consigo um ampla comunidade de oficiais e supervisão. A inteligência faz parte e apoia esta atividade.

Isto não significa que segurança desse tipo é parte integral da inteligência, mais do que a ação encoberta. Na doutrina da OTAN, "inteligência e segurança são atividades próximas, então o planejamento de inteligência executiva requer o conhecimento de medidas de segurança" (OTAN, Intelligence Doctrine, 1984). O aparato de segurança é melhor visto como um *usuário* especial da inteligência, com íntimo envolvimento em suas atividades.

2.1 Técnicas e organização

A segurança de informação tem três componentes: segurança *protetiva*, a derrotar a coleta de inteligência; a detecção e neutralização de ameaças de inteligência; e o engano. O primeiro é passivo e defensivo; o segundo é defesa ativa; e o terceiro derrota a inteligência hostil a confundindo ou enganando.

2.1.1 Segurança protetiva

Consiste em medidas protetivas que espelham a inteligência ofensiva - assim a proteção contra HUMINT inclui pessoal, segurança física e segurança de documentos, e assim por diante.

Segurança de comunicações ("Comsec") inclui contramedidas à COMINT, etc. EMCON, ou controle de emissões, é um termo militar para a limitação na emissão de emissões eletrônicas de todo tipo. A segurança de computadores ("Compusec") lida com a segurança de informação digital.

Os princípios são simples - limitar as emissões ao mínimo, eliminar radiação acidental, limitar o que pode ser deduzido da aparência externa da assinatura de sistemas e negar acesso ao conteúdo informacional de sistemas de computadores.

Camuflagem é a contramedida à IMINT. Redução de ruído é a contramedida à inteligência acústica. "Redução de assinatura" é o termo genérico que se refere à redução de visibilidade de alvos ao radar e outros mecanismos de detecção. O *bugging* de microfones tem sua contramedida no *sweeping*. Vazamentos de informação à fonte aberta são enfrentados pela censura de guerra. Cada forma de inteligência ofensiva tem sua contramedida defensiva.

2.1.2 Detecção e neutralização

A defesa as vezes tem a possibilidade de neutralizar os esforços ofensivos detectados. Agentes podem ser presos, oficiais sob cobertura diplomática podem ser expulsos, e assim por diante.

O enfrentamento ativo da inteligência inimiga inclui a eliminação física de coletores, a contra-espionagem e a contra-inteligência. Centros de inteligência podem sofrer ataques como parte da interdição de sistemas de comando e controle.

O escopo é sempre limitado - agentes são vulneráveis, mas a maior parte da coleta técnica é de longo alcance e passiva, não vulnerável a impedimentos.

2.1.3 Engano

O engano (*deception*) é definido pela OTAN como "medidas designadas a enganar o inimigo pela manipulação, distorção e falsificação de evidência de forma a induzi-lo a reagir de forma prejudicial a seus interesses" (OTAN, 1984).

É integrada pela desinformação (evidência falsa) disponível a coletores adversários, enquanto a segurança busca esconder a evidência real. O objetivo é fazer com que a vítima engane a si mesma, minimizando a quantia de informação real necessária para tornar a fonte crível.

É usada primariamente na guerra. Seu significado em tempos de paz tende a ser exagerado; é melhor compreendida como parte de um *plano* específico, orquestrado para induzir a vítima a alguma ação. Nas circunstâncias corretas pode ser um adjunto potente à segurança e surpresa - no entanto seu excesso faz com que toda inteligência seja tratada com cautela, causando dúvidas nem sempre produtivas.

A história mostrou que políticas e ações de segurança organizada são necessárias. Autoridades de segurança são usuários especializados.

2.2 Contribuições da inteligência para a segurança

2.2.1 Avaliações de ameaça

A segurança é baseada em avaliações de inteligência. As ameaças de inteligência de outros Estados são analisadas pela contra-inteligência - elas são os alvos mais focados em segurança, e portanto o alvo mais duro. SIGINT pode fornecer certas informações úteis sobre suas comunicações - a descoberta dos dispositivos técnicos dá certa ideia da capacidade do oponente. Normalmente, porém, as principais fontes sobre ameaças de inteligência são as infrequentes fontes humanas.

O estudo é intensivo, e levanta dúvidas sobre seu custo-benefício. Na Guerra Fria a cobertura da inteligência soviética fora da contra-inteligência e contra-espionagem era de prioridade duvidosa, e por vezes era difícil saber se era realmente necessário saber as capacidades exatas dos satélites de inteligência soviéticos.

2.2.2 Contra-espionagem

A detecção e neutralização da espionagem é o maior esforço da ação direta. Como parte da inteligência de segurança, é distinta da grande comunidade de inteligência ofensiva - pode ser vista, também, como uma contribuição discreta à segurança de informações.

Esta é uma imagem incompleta. A contra-espionagem lida apenas com um tipo de ameaça hostil - fontes humanas. Além disso, a contra-espionagem detecta e elimina casos individuais de espionagem, o que pode levar às próprias organizações-fonte de onde as ameaças emanaram. Apesar da separação institucional, portanto, a contra-espionagem se liga aos esforços da contra-inteligência em penetrar a inteligência oponente.

2.2.3 Penetrando a inteligência estrangeira

No sentido amplo de "inteligência sobre a inteligência estrangeira", a contra-inteligência não apenas contribui com a avaliação de ameaças, mas produz evidências específicas sobre a penetração estrangeira atual nas próprias estruturas de inteligência. Nesse sentido os agentes entram num conflito de contra-inteligência, buscando penetrar organizações e capturar agentes, e evitar a invasão inimiga e a própria captura.

2.2.4 Inferências operacionais

Inferências sobre atividades adversárias de inteligência podem também ser feitas a partir da vigilância de suas atividades de não-inteligência - observando quaisquer ações que reflitam conteúdo de inteligência.

Observar a atividade adversária desta forma, porém, necessita de um esforço organizado particularmente para esse propósito. A inteligência alemã durante a Segunda Guerra Mundial, diante de evidência de inteligência aliada superior, se recusou a acreditar na possibilidade de que a Enigma pudesse ser quebrada analiticamente. Os EUA, durante os anos 1970, parecem ter sido pegos de surpresa pela quebra soviética de seus códigos navais.

2.2.5 Caçadores e protetores, conselhos e padrões

O descrito é apenas a metade da contribuição da inteligência. A outra metade é onde a inteligência age como um aparato de segurança em si - utilizando sua *expertise* ofensiva em papéis defensivos. Ela determina padrões de segurança e fornece material especializado de segurança. As responsabilidades defensivas do BSS são extensas a ponto de tornar o Serviço uma organização híbrida ofensiva e defensiva.

Quebradores de cifras sempre foram vistos como boas pessoas para elaborarem cifras, desde o século XVIII na Inglaterra. Os mesmos princípios se aplicam nas outras áreas - as áreas de *Comsec* e *Compusec* têm recaído sobre organizações de SIGINT.

Esta função de apoio representa a contribuição mais consistente da inteligência aos esforços de segurança. Quaisquer que sejam as dificuldades de avaliar a ameaça, a inteligência ofensiva tem *expertise* a oferecer, cuja qualidade ajuda a determinar a qualidade da defesa desenvolvida.

2.3 Responsabilidades e conflitos

Os responsáveis pela segurança são os braços operacionais de um governo, mas a inteligência ofensiva traz as contribuições aqui discutidas. Um efeito é dar a partes da comunidade de inteligência papéis importantes, e outro é dedicar parte da inteligência a um conflito de contra-inteligência com os adversários.

Toda coleta de inteligência é parte de um conflito com sistemas opostos de segurança, incluindo a construção de uma 'base técnica' de conhecimento sobre tais sistemas. Daí a superioridade ofensiva dá resultados - como visto na Batalha do Atlântico, na qual a quebra da Enigma mostrou que a Alemanha havia também quebrado uma importante cifra naval. Sucessos ocidentais dependeram de uma grande coleta de mensagens alemãs, e da virtual invulnerabilidade das próprias cifras aliadas.

Isto mostra como um pequeno avanço pode levar a outros, de forma a criar uma progressão de vantagens. Uma pequena brecha permite que forças móveis a explorem, "virando" as defesas da retaguarda e expandindo a brecha. A inteligência pode ver o mesmo tipo de *breakthrough*.

O conflito de contra-inteligência, porém, pode ser separado deste conflito principal entre inteligência e segurança - é, ao invés disso, as tentativas especializadas da inteligência de penetrar a inteligência estrangeira, tomando portanto a forma de uma série de sub-conflitos. Um nível são as ações da contra-inteligência contra a inteligência oponente; outro está na tentativa da contra-inteligência oponente em penetrar na própria contra-inteligência, e assim por diante. A essência de cada nível é a busca por evidência de penetração oponente ocorrida no nível acima.

A contra-inteligência nunca é tão completa, mas alguns exemplos mostram a realidade do conflito - como redes de agentes ocidentais descobertas na URSS que foram então operadas sob controle soviético. Outro exemplo foi a entrega, por Blake, dos detalhes do desvio ocidental de cabos soviéticos em Berlim à URSS.

Este acesso também permite o controle detalhado do engano, como foi o caso da grande operação de engano antes da invasão da Normandia. A Guerra Fria também viu esforços de penetração no nível subordinado da contra-inteligência, como quando Philby, agente soviético no comando da contra-inteligência do SIS, pôde avisar a contra-inteligência soviética de potenciais desertores.

Em geral, a ideia é derrotar a inteligência inimiga conforme se vence o conflito principal buscando a informação geral inimiga, assim como a derrota da força aérea inimiga é uma precondição da supremacia aérea e uso pleno da própria força aérea.

2.4 Apoio nos anos 1990

Mesmo durante a Guerra Fria o apoio da inteligência à segurança precisava apenas de uma proporção modesta dos recursos alocados. Mesmo a contra-inteligência era minoritária e especializada - os práticos de inteligência poderiam fazer inteiras carreiras sem nunca encontrá-la.

Durante os anos 1990 a incerteza de ameaças se tornou muito grande. A espionagem continuava, assim como a coleta técnica e todas as necessidades militares e diplomáticas que justificavam a inteligência há séculos. Até Estados amigos podem ser tentados a espionar seus aliados para obter informações sobre seus inimigos, como a Israel que aceitou a oferta de Pollard de inteligência americana sobre alvos no Oriente Médio.

A coleta ofensiva continua a ser importante, assim como a revolução eletrônica - que aumenta a

importância da *Comsec* e *Compusec* em muitas vezes. Algum esforço de contra-espionagem ainda é necessário; no entanto, um grande esforço de contra-inteligência deixou de se justificar, hoje restrito a tempos de guerra. Este envolvimento no mundo defensivo teve efeitos sobre o tamanho das organizações, mas de forma complexa - afinal, Estados que buscam alta segurança defensiva precisam de capacidades de coleta ofensiva capaz de aconselhá-los.

Democracies at War

Dan Reiter, Allan C. Stam

1 1 - A Quarta Virtude da Democracia

A virada do século foi um momento de quase consenso sobre as virtudes da demogracia, sob a percepção de que a democracia traz consigo liberdade, prosperidade e paz. Os dissidentes são cada vez menos numerosos e menos fervorosos.

A crença na liberdade venceu antigas críticas marxistas de identificação do indivíduo com o Estado mesmo na Europa Oriental, e a crença na prosperidade levou o antigo bloco soviético a buscar a prosperidade do Ocidente. A crença na paz a partir da democracia levou a administração Clinton a enfatizar a democratização como sua política externa.

Juntas, estas crenças ofereceriam a partir da democracia ocidental o "fim da história". No entanto, democracias podem se mostrat vulneráveis. Serão os atributos os mesmos que dão ao Estado democrático sua segurança?

Pouco apreciada tem sido a quarta virtude da democracia: ela vence guerras. Desde 1815 países democráticos venceram mais de três quartos dos conflitos.

Sua eficácia marcial vem como surpresa para alguns, que veem na ameaça externa algo que pode exigir o sacrifício de alguma liberdade interna. Alguns pessimistas chegaram a recomendar a subversão da democracia para fazer política externa efetiva, e duvidaram que o experimento democrático fosse sobreviver.

Sobre a democracia, busquemos as características que levam democracias a prevalecer no campo de batalha. São criaturas complexas, e as mais importantes entre elas. Sobre a guerra, exploremos por que os Estados as vencem, passando da visão míope exclusivamente sobre suas causas. Pensar como as guerras são vencidas prova-se importante também para entender as causas de seu início - afinal líderes consideram suas chances de vitória antes de iniciá-las.

Nosso argumento central é que democracias vencem guerras pelos efeitos do consenso público e pela transparência de líderes a eleitores, diante do risco político de remoção.

Em primeiro lugar, ser vulnerável à vontade da população impede o início de guerras arriscadas ou fúteis. Demonstramos também que as críticas de Tocqueville - que o medo eleitoral paralisaria líderes - são infundadas, e democratas estão preparados para usar a força, ainda que desenclinados a arriscar a derrota. Como resultado, as guerras de democracias tendem a ser mais curtas e menos arriscadas.

Uma segunda vantagem está no próprio campo de batalha. Os soldados advindos de sociedades baseadas em consenso têm certas vantagens - a ênfase em seus direitos produz líderes melhores e soldados mais dispostos a tomar a iniciativa.

Apresentemos, pois, quatro perspectivas que podem explicar a prevalência marcial da democracia.

1.1 O esqueleto - estruturas políticas

Os conjuntos de regras que criam a estrutura dos Estados democráticos tornam os líderes responsáveis por suas ações. Esta responsabilidade vem na forma de voto retrospectivo (punição ou recompensa a líderes), voto prospectivo (seleção baseada em competência percebida) e consenso popular ao momento da adoção de uma política (consenso contemporâneo).

Eleitores podem se focar no futuro se acreditarem que ele será diferente do passado, mesmo deixando de eleger bons líderes passados. O voto retrospectivo é menos sofisticado, e um foco algo míope no passado. Nossa visão é que eleitores e líderes tendem a se focar nas questões imediatas - buscando aprovação contemporânea conforme as decisões são tomadas. Atrás do voto há, é claro, todo um sistema de freios e contrapesos.

Em geral, as pessoas que pagam o maior preço em impostos e sangue removeriam qualquer líder que jogasse a nação numa guerra arriscada ou fútil. Para um líder autocrático, cujo poder é garantido, a derrota traz um risco político pessoal menor.

Quando um governo democrático busca uma política encoberta, à sombra do consenso popular, ele começa a se aproximar de outros tipos de Estados, sendo então mais comuns as violações de direitos e os atos violentos contra outras democracias.

1.2 O espírito - cultura política

Sociedades com regimes diferentes exibem culturas políticas diferentes. A hipótese apresentada é que a democracia promove mudanças nas quais os cidadãos têm normas e valores diferentes que vencem guerras, mas não da forma mais direta - e sim que, ao empoderar o indivíduo, a democracia empodera o coletivo, gerando líderes e soldados melhores.

1.3 A família - comunidade internacional

Kant já via uma oportunidade especial de democracias encontrarem uma comunidade entre nações comuns que buscam interesses compartilhados e relações pacíficas. A hipótese é que este senso de democracia tem efeitos, como a baixa frequência de guerras entre democracias e o auxílio militar entre democracias.

1.4 O poder - força econômica

A parte central da guerra é o conflito militar e industrial. O equilíbrio de poder industrial-militar é um determinante importante nos resultados da guerra. Uma explicação possível a nosso assunto é que democracias reúnem mais poder material e militar, em primeiro lugar porque são mais prósperas, em segundo lugar porque são capazes de maiores sacrifícios materiais do que outros Estados. A maior popularidade do regime influi e gera maior contribuição popular.

1.5 Conclusão

Concluímos, ao longo do livro, que democraias não vencem guerras por algum senso de comunidade internacional, nem por serem mais ricas ou maiores economias. Em nossa opinião, o poder da democracia não está na elite, mas nos cidadãos - democracias que iniciam guerras têm maior probabilidade de vencê-las. Também apoiamos a hipótese de que os militares advindos de democracias são superiores em iniciativa e liderança - o esqueleto e o espírito da democracia, pois, são as causas que vemos como as mais relevantes.

2 2 - Democracia, início da guerra, e vitória

Guerras são intencionais, iniciadas por líderes baseando-se em circunstâncias e decisões humanas. Tanto a decisão inicial de iniciar hostilidades quanto a condução das operações militares podem afetar quem é vitorioso e derrotado.

É isto o que chamamos de efeito de seleção - líderes selecionam suas guerras, o que leva ao efeito da vitória da democracia. É possível também que líderes escolham não iniciar uma guerra. Além disso, democracias vencem por serem mais efetivas após o início de hostilidades.

2.1 Uma teoria do início e resultado da guerra

Propomos que líderes tomam decisões acerca da guerra da mesma forma que em outras políticas, ou seja, buscando benefícios e minimizando custos, agindo de forma racional de acordo com uma probabilidade percebida de vitória, diante da existência de uma probabilidade real que pode ou não ser bem analisada. Durante a guerra do Vietnã, o governo americano fez estudos estatísticos muito detalhados acerca das probabilidades de sucesso de cada operação - precisos, embora errôneos. Durante a Crise dos Mísseis, o presidente Kennedy acreditava que as chances de guerra nuclear estavam entre um terço e um meio.

O pessimismo quanto a nossa possibilidade de julgar probabilidades não é inteiramente justificado. Um dos modelos existentes previu corretamente 90% dos resultados de todas as guerras de 1816 a 1990. No entanto, será possível julgar as estimativas dos líderes da mesma forma?

A análise histórica revela que, de fato, o Estado que inicia a guerra tende a vencê-la, diante da do efeito de seleção. Da mesma forma, Estados melhores em estimar suas chances de vitória tendem a vencer caso decidam iniciar hostilidades.

Há um outro ponto, sendo, caso ambos os beligerantes estimassem corretamente o resultado, a guerra em si poderia ser quase sempre evitada, como na rendição da Dinamarca em 1940 - atingindo os mesmos resultados de uma guerra sem pagar seu preço. Ainda assim, guerras são comuns. Uma resposta a este dilema foca na má interpretação de capacidades militares, quando um dos beligerantes julga mal suas chances de vitória. Tipicamente Estados, ainda que conheçam bem suas capacidades, subestimam aquela de seus inimigos. Nesta perspectiva, guerras ocorrem quando um agressor pede concessões, um alvo julga mal suas capacidades, as nega, é atacado e perde; ou quando um agressor confiante demais pede concessões, um alvo bem informado as nega, o agressor luta e perde.

No entanto, não há chance maior de um dos beligerantes ser aquele que estima mal suas chances, e nesse caso o agressor erraria em cerca de 50% das vezes. Isto não é o caso. Assumimos, pois, que alvos não evitam guerras mesmo quando acreditam que perderão.

Uma razão é quando o alvo subestima a seriedade da ameaça, pagando para ver uma mão forte. Hussein não acreditava que os EUA de fato entrariam em guerra, e a Argentina não levou a sério a seriedade britânica nas negociações pré-1982 - afinal, um Estado que não pretende agredir outro pode ainda fazer ameaças.

O agressor pode também acreditar que a guerra é inevitável, passando a empreender um engano para ganhar a surpresa no ataque. Neste caso as negociações terminam antes de um 'ultimato', e se perde a chance de evitar a guerra, como ocorreu na Coréia em 1950 entre os EUA e a China, que abandonou sua posição ameaçadora quando passou a crer na inevitabilidade da guerra.

Um alvo também pode escolher *lutar para perder* ao invés de aceitar concessões. Primeiro porque a rendição traria consigo o fim de carreiras políticas (como na Finlândia em 1939); segundo porque se crê que *a honra traz o poder*, ou uma necessidade de um país soberano (como na península de Hanko em 1939); ou então porque a defesa da própria terra seria um bem *indisponível*, como a defesa da Bélgica na I Guerra Mundial.

Historicamente, de fato alvos lutam mesmo quando a derrota é certa. É por isso que de fato agressores tendem a vencer guerras - caso contrário alvos fracos tenderiam a evitá-las.

Diante do efeito de seleção, Estados agressores venceriam mais guerras de dois jeitos - por acreditarem ter boas chances de vitória, ou porque, tendo melhor capacidade de estimar tais chances, os Estados vencem mais e perdem menos.

N.E.: Somente fichamos a porção do capítulo que importa à inteligência, também por discordarmos fundamentalmente da ideia de que democracias vencem mais - não porque as estatísticas não suportam esta conclusão, mas porque cremos que se trata de um problema ou falácia de pré-seleção, visto que historicamente a maior parte dos Estados democráticos se encontraram no Ocidente, e por razões outras o Ocidente, com poucas exceções, concentrou grande poderio militar. De fato, de forma bastante relevante ao conjunto de dados utilizados pelo autor, a Inglaterra, primeiro país "democrático" do mundo, não necessariamente venceu guerras no século XVIII e XIX por ser democrática, mas porque era o maior império do mundo. O autor de fato nota que nem todos concordam que "democracias vençam mais" no segundo capítulo da obra.

The evolution of international collaboration in the global intelligence era

A. Denis Clift

Após os ataques de 11 de setembro, diversas equipes foram formadas pela CIA, incluindo veteranos, oficiais com habilidades linguísticas em persa e dari, entre outros. A primeira equipe chegou ao Afeganistão em 27 de setembro de 2001, levando três milhões de dólares em espécie.

Contato foi imediatamente feito com a Aliança Norte, criando-se também uma célula conjunta de inteligência compartilhada, e no processo a Aliança recebeu 500 mil dólares.

Nos próximos 2 meses esta parceria cresceu e a inteligência americana indicava unidades e líderes do Taliban conforme suas forças especiais e aliados afegãos as atacavam. Informação humana que só podia ser obtida por afegãos foi crucial ao sucesso inicial das operações.

Com o início da era da inteligência nacional, a cooperação entre agências chegou a níveis inéditos. Nesta nova era, as ameaças não eram apenas Estados, mas indivíduos, células e outros atores não-estatais. O compartilhamento de informações e parcerias internacionais também se tornaram importantes, e um padrão frente ao qual a comunidade de inteligência é julgada.

A *National Intelligence Strategy of the United States of America*, de 2005, definiu como prioridades cooperação com forças aliadas de inteligência para localizar unidades terroristas dentro e fora dos EUA, informá-las e analisá-las também em conjunto, e garantir que o conhecimento resultante informe julgamentos e opções efetivas.

A visão e guia do DNI busca que aqueles responsáveis pela inteligência americana adotem um mandato de gerenciamento de risco, não aversão ao mesmo - método anterior para proteger fontes e resultados. A aversão ao risco não vê que inteligência compartilhada pode ser inteligência multiplicada - abrindo a porta a informações vitais ainda não disponíveis.

Parcerias da inteligência americana vêm da guerra revolucionária, desde 1775, com o Comitê de Correspondência Secreta. Os britânicos também espionaram a comissão Franklin, e seu secretário era um agente duplo britânico.

De uma perspectiva estratégica, a inteligência franco-americana teve um papel positivo na guerra da independência, e nas guerras mundiais novas parcerias internacionais de inteligência foram traçadas. A inteligência aérea em 1917 dava melhores informações sobre a localização, profundidade e composição das linhas inimigas, e os franceses lideraram um grande esforço em reconhecimento aéreo.

A doutrina aérea americana era muitoa trasada, mas ao final do primeiro ano havia estabelecido uma base de compreensão. Inicialmente a força expedicionária americana dependeu de inteligência francesa e britânica, mas logo implementaram um programa para empregar talentos fotográficos.

Vinte anos depois, a cooperação entre a inteligência americana e britânica havia sido substi-

tuída por competitividade. Conforme a ameaça alemã crescia, os americanos relutavam em se aproximar de outro conflito europeu.

A marinha real buscou sua tecnologia mais secreta, o radar, se oferecendo para compartilhá-la com os americanos sem pedir nada em troca. Esta oferta lentamente levou a maior cooperação. Em 1940 o recém-criado SOE iniciou a infiltração de agentes especiais na França, e o OSS americano participou das operações. Até 1944 se criaram os Jedburghs, equipes formadas por um britânico, um americano e um operador do país que seria infiltrado. A primeira equipe entrou na França logo antes da invasão de 1944. Em paralelo, os britânicos quebraram os códigos ENIGMA e os americanos quebraram os códigos japoneses MAGIC.

A atenção saiu do reconhecimento aéreo e se voltou para inteligência humana. Cooperação limitada ocorreu mesmo nos esforços individuais de quebra de códigos, levando em 1943 ao compartilhamento completo do ULTRA. Este programa de inteligência bilateral se tornou a partir de então uma "parceria especial".

Em 1947 a legislação acima foi aprovada, criando a CIA e o NSC. O governo se reorganizou para evitar outro Pearl Harbor, e a ideia do NSC era reunir esforços militares, diplomáticos e de recursos.

Inteligência era uma parte central das novas questões estratégicas. O ato se centrou na organização, mas não estabeleceu novas regras, que seriam objeto de guiagem particular e secreta.

Os problemas de um "relacionamento especial" seriam vistos no começo da Guerra Fria - pelas portas abertas em Washington e Londres agentes soviéticos passavam com maior facilidade. A comunidade de inteligência se expandiu até 1970, e a estrutura para coordenar a inteligência compartilhada se tornou mais sólida e controlada, especialmente na proteção de fontes e métodos de resultados compartilhados com as Nações Unidas.

A URSS emergiu rapidamente como uma superpotência adversária após a guerra. A dissuasão nuclear se tornou parte das atribuições centrais da OTAN, e conforme a OTAN crescia o risco de espionagem de seus membros também aumentava, como no secretário do chanceler da Rep. Federal da Alemanha, Gunter Guillaume, espião da RDA e oficial do exército alemão oriental.

Os desafios eram compartilhar com quem precisava saber ao mesmo tempo que se mantinham fontes e métodos protegidos. Nos anos 60 e 70, voos de SR-71 monitoravam ações militares no Oriente Médio - e os resultados eram compartilhados com os beligerantes para obter confiança nas negociações.

1 Maior gerenciamento de risco

Com a queda da URSS, novas dimensões da inteligência surgiram, como visto nas operações no Iraque e Kuwait em 1990, nas quais a vitória ocidental foi em grande parte atribuída à excelente inteligência obtida.

O compartilhamento teve características particulares que contribuíram em operações mais recentes, como a necessidade de produzir o maior volume possível de produtos, a responsabilidade das organizações de inteligência que se relacionava à responsabilidade democrática dos líderes dos países envolvidos, incluir o máximo de informação possível sem comprometer fontes e métodos, e o conceito de "inteligência de linha perfurada" (*perforated-line intelligence*), na qual relatórios eram enviados na íntegra aos comandantes americanos e censurados nas partes mais

sensíveis às fontes e métodos para serem enviados aos aliados.

Estas técnicas foram utilizadas na intervenção na Iugoslávia, e um problema enfrentado pelos EUA foi a grande variedade de idiomas com que precisava lidar. Seus oficiais de inteligência falavam apenas os idiomas dos conflitos do passado - e os aliados ajudaram muito na habilidade linguística necessária para explorar as fontes de inteligência nos Bálcãs. Lá as unidades de inteligência se tornaram centros pequenos e táticos, células capazes de trabalhar com parceiros nos flancos avançados, e centros capazes de tomar decisões no campo e compartilhar com agilidade quando necessário.

Hoje o ambiente estratégico inclui aliados para garantir dissuasão, estabilidade e enfrentar ameaças domésticas. Toda presença militar, geográfica, cultural, ideológica ou religiosa se tornou relevante.

As antigas compreensões de compreender o equilíbrio entre forças convencionais e nucleares se ampliaram muito. Há novas ameaças, novos meios e tecnologias, novos desafios transnacionais. Indivíduos têm suas forças multiplicadas a níveis que até pouco tempo só se viam disponíveis a países.

Novos compartilhamentos emergem no Iraque e Afeganistão, fluindo para nações aliadas, em fluxos se movendo bilateral e multilateralmente para cima e para baixo. O centro do problema é projetar estabilidade onde ela for necessária - a projeção de estabilidade, ou seja, enfrentar os problemas onde eles surgem, se tornou o centro das operações.

A ISAF oficializou o compartilhamento no centro de operações conjuntas em Kabul, e buscou facilitar operações conjuntas entre os membros da ISAF.

A ordem executiva de 2008 reforçou a necessidade de criar ineligência que melhore a habilidade dos usuários de tomar decisões, negando aos adversários as mesmas vantagens, refletindo a imperatividade de maior colaboração com aliados e parceiros internacionais.

O número de países que coletam imagens e as analisam cresceu muito, assim a construção de conhecimento de inteligência geoespacial compartilhado se tornou muito mais benéfico e capaz em coalizões. O ambiente é técnico, veloz, global e competitivo, e muitas vezes se depende de parcerias internacionais para prevalecer.

Há inovações positivas em outros lugares. O abandono da aversão ao risco e adoção do gerenciamento de risco é complexo e essencial. Velhas práticas estão dando lugar a técnicas mais ousadas e ágeis, conforme a colaboração internacional continua a evoluir.

Intelligence and the revolution in military affairs

Michael Herman

Há extensiva literatura sobre a chamada Revolução em Assuntos Militares, RAM, em parte pelo uso de armamentos de precisão e controle das forças amigas, mas também pela mudança tecnológica na exploração de informações sobre as forças inimigas. Os maiores entusiastas veem um mundo no qual aqueles com as ferramentas adequadas a saberem de 'tudo o tempo todo', tomando ação com armas de precisão quando necessário.

As implicações práticas permanecem incertas. Refere-se a 'informação' sobre o inimigo de forma vaga, sem distingui-la de inteligência. Há diferenças citadas entre inteligência, vigilância e reconhecimento (ISR), mas sem diferenciações.

Dados coletados se tornam informações quando processados, e inteligência quando analisados num contexto específico. No entanto, há distorções epistemológicas, algumas intencionais - a ONU passou a utilizar 'informação' para se referir a inteligência em suas operações. Além disso, a vigilância e aquisição de alvos, que não são inteligência, podem se aproximar dela se incorporadas a análises de inteligência.

Uma forma de solução é ver a diferença entre inteligência, vigilância, reconhecimento e aquisição de alvos como uma diferença unicamente institucional. Não há uma grande diferença entre seus produtos, e o que se vê é um contínuo de coleta de informação sem definições fortes. Um CIC de um fragata utiliza inteligência, 'guerra eletrônica' e 'informação de ação' sem grandes diferenças no conteúdo.

No entanto, esta visão é apenas parcial. A especialização da inteligência é genuína, em **conteúdo**, de forma menos factual que fontes operacionais e mais rica em conteúdo multifontes e contextual; em **imediatidade**, com produtos mais demorados diante da necessidade de análise humana, como na diferença entre o radar imediato e a SIGINT analisada; em **fontes e métodos**, havendo diferenças em robustez, ostensividade e vulnerabilidades entre os métodos; em **localização**, havendo concentração de fontes operacionais no teatro de operações e de fontes de inteligência sob controle central; e em **especialização**, conforme a inteligência tem um papel único e uma autoridade sobre o inimigo e sua compreensão em detalhes.

Há exceções menos especializadas, como a interrogação de prisioneiros e estudo de documentos capturados, que são atividades de inteligência sem vulnerabilidade particular, mas definir as diferenças como institucionais de qualquer forma não é suficiente.

1 Mudanças tecnológicas

A tecnologia da RAM está reduzindo o elemento humano mesmo em aplicações de inteligência, com integração entre fluxos de informação e processamento imediato. A remoção das barreiras entre inteligência e fontes operacionais, nesse sentido, poderia ser uma parte natural da RAM.

Uma proposta, de Libicki, é retornar a um pa-

drão antigo de um corpo de informações unificado, sem especialização específica em informações inimigas, mas com uma concentração de processos de informação sobre amigos e inimigos que teriam contato facilitado também com estruturas civis.

A objeção comum a esta integração é a proteção especial às fontes e métodos da inteligência, numa impressão de que esta precisa de tratamento diferenciado, com base nos canais Ultra da Segunda Guerra Mundial, nos frequentes vazamentos de Washington durante a Guerra Fria e outros. Mas recentemente proteções excessivas foram levantadas, reduzindo, por exemplo, o nível de proteção da maior parte inteligência de satélites de forma que possa ser utilizada pelos corpos operacionais. Uma questão mais importante é se a informação produzida é do mesmo tipo, diferente ou complementar.

2 Conhecimento sobre o inimigo e seu ambiente

A primeira percepção, dominante, é a de um telescópio tecnológico de todas as fontes, incluindo todo tipo de informação, sem deixar claro como se dá a interpretação dos dados - talvez com reconhecimento automático de alvos. A ênfase é em ver *imagens*, tendo comandantes e subordinados uma *imagem* compartilhada da situação de combate.

Isto pode ser atingido pela automação. Julgamento humano não é excluído, mas talvez seja julgamento das operações, não da inteligência. Owens buscou apresentar a possibilidade de obter também um tipo mais profundo de informação - o conhecimento dominante do espaço de batalha (*dominant battlespace knowledge*), que viria de combinar a noção de localizações e outras informações sobre significância e relacionamentos entre estas coisas.

A implicação é que isto aprofundará o conhecimento tradicional da inteligência sobre o inimigo e o fará em tempo real, nos aproximando de um mundo onde decisões poderiam ser tomadas com conhecimento perfeito.

Esta visão é indistinta e improvável. Computadores de fato são capazes de mostrar informação relevante e fornecer conhecimento situacional, mas o uso de AI para fornecer diagnósticos reais ainda é muito incipiente.

Como um grande telescópio, esta RAM precisaria de um grande esforço diretor para alimentá-la e coordenar seus esforços, restrito à "inteligência de tempo real", ainda que a inteligência continuasse a apoiar suas operações. Nesse caso, o novo papel da inteligência seria, em parte, integrar uma organização unificada para conhecimento situacional em tempo real, e em parte apoiar esta atividade com análise pormenorizada.

3 Dualidade da inteligência

A interpretação interior ignora a dualidade da inteligência no sentido de que esta também se foca em mentes, não apenas em objetos, com evidência baseada na linguagem, não em observações. Ambos os papéis contribuem para o resultado, mas de formas diferentes. Esta inteligência 'textual' é capaz de tocar em mentes e ideias, sendo capaz de acessar também localizações e inventários. Este tipo de informação pode ser mais rico, e por isso fontes textuais são altamente protegidas.

Fontes textuais não parecem ser mencionadas pela literatura dedicada à RAM. A tecnologia dará ao comandante excelentes observações e medidas, mas o comandante não terá linguagem ou interpretação alguma.

Em alguma medida isto é de um realismo sau-

dável. Os proponentes assumem que fontes textuais não são garantidas, certamente não em tempo real, e podem valorar o uso da informação observacional. Ainda assim, é estranho ignorar as fontes textuais - conhecimento dominante do espaço de batalha já se viu algumas vezes durante o século XX, sempre graças à quebra de códigos.

Além disso, pode-se defender que novas técnicas de criptografia tornarão quase impossível a exploração de informação textual protegida[1].

4 Perspectivas textuais

Apesar do segredo cercando inteligência textual, alguns pontos podem ser feitos: em primeiro lugar, a criptografia e quebra de códigos sempre flutuaram entre ataque e defesa, encontrando e reencontrando equilíbrios. Além disso, criptanalistas tendem a obter resultados melhores que suas previsões iniciais, e os incentivos para quebrar cifras são maiores que os incentivos para criar boas cifras. Em terceiro lugar, o ganho pelo estudo de textos aparentemente vazios é profundo, permitindo mesmo previsões sobre operações militares, mesmo com ampla censura.

Em quarto, informação textual não se restringe a material de fontes técnicas, e documentos podem ser adquiridos nos restos de forças militares vencidas ou por desertores, bem como por grampos e operações encobertas. Outras ações diretas são, as vezes, necessárias - cortar cabos pode forçar o inimigo a utilizar o rádio. Por último, há a questão da tempestividade. Fontes textuais provavelmente não serão inteiramente automatizadas, mas a Segunda Guerra Mundial mostrou que, às vezes, era possível implementar a decriptação quase imediata.

[1] N.E.: O ainda incerto sucesso da computação quântica tem a perspectiva de quebrar códigos inquebráveis pela computação condicional.

5 Conclusões

A tecnologia pode de fato estar causando uma revolução na informação disponível sobre o inimigo e espaço de batalha. Mas é necessário ser claro sobre que tipo de conhecimento é afetado por estas mudanças. Pode haver conhecimento situacional em tempo real sobre o movimento e localização de forças inimigas, mas um tipo mais profundo de conhecimento dominante do espaço de batalha ainda não pode ser visto. A RAM pode dar ao comandante visão plena, mas não interpretação.

Como o Gen. Horner descreveu, ter dados e entender o que eles significam são coisas muito diferentes, pois injetamos nossos próprios preconceitos na interpretação da capacidade do oponente.

Muitas inferências podem ser feitas, e tecnologia pode torná-las mais confiáveis, mas não se pode obter conhecimento dominante do espaço de batalha baseando-se apenas nessas capacidades. Conhecer a intenção do inimigo, por vezes, é muito mais valioso que saber exatamente seu curso.

A primeira conclusão é que a coleta e exploração de informação textual deve receber um lugar definitivo na RAM e nos investimentos envolvidos. Não há garantias de atingir potes de ouro de quebra de cifras, mas a observação e medida são incompletas sem informação textual de algum tipo.

Daí a segunda conclusão: a necessidade de cuidado sobre a visão da RMA como 'informação perfeita'. A tecnologia promete milagres, mas mesmo com atenção adequada ao futuro das fontes textuais a aura de infalibilidade não é, nem será, realizada no futuro próximo.

Human source intelligence

Frederick P. Hitz

O ato de 2004 buscou uma revitalização e modernização da inteligência de fontes humanas, numa época onde a experiência da Guerra Fria se mostrava limitada. O fracasso de inteligência no que toca as alegadas armas de destruição em massa no Iraque, porém, foi em grande parte causado por falta de boas fontes humanas.

É incerto se as antigas técnicas de recrutamento por oficiais de caso operando de instalações oficiais serão capazes de se transferir a fundamentalistas islâmicos.

O congresso parece ter concluído que maior orçamento e mais espiões é a resposta, baseado numa percepção de atrofia da inteligência humana após a Guerra Fria, bem como uma maior ênfase em falantes de línguas do Oriente Médio.

Não se sabe, porém, se as motivações para espionar para o Ocidente são suficientes. Exploraremos os sete pecados da espionagem e se a HUMINT terá um papel importante ou não no século XXI.

Ainda que a inteligência humana esteja em uso há milhares de anos, foi durante a Segunda Guerra Mundial que os EUA perceberam sua desvantagem em não ter um serviço de inteligência em tempos de paz, sendo criado o Escritório de Serviços Estratégicos (OSS) e depois a CIA em 1947.

Durante a guerra fria, era papel da CIA exercitar a política de contenção por meio de espionagem e ação encoberta, uma papel enorme que nenhum dos outros departamentos estavam dispostos a aceitar. A CIA começou a ter sucessos maiores com infiltrações bem sucedidas nos anos 1960, enquanto os soviéticos já tinham espiões no Ocidente desde a década de 1930. Por 45 anos, este foi o papel da inteligência americana - a contenção do comunismo.

A ação encoberta, diante da impossibilidade atual de manter operações inteiramente em segredo, tende a se tornar menos relevante na luta contra o terrorismo. Portanto, cabe analisar a espionagem em si.

Espiões buscam informação que seu dono quer proteger, independente de sua sensibilidade intrínseca. Seu universo já não é o de "países", mas incui insurgentes no Afeganistão e em Darfur, entre outros grupos transnacionais. De uma forma ou de outra, um espião sempre estará cometendo um ato de traição de confianças, com profundas consequências.

Hoje a inteligência está em modo preventivo, e neste caso informação precisa e ágil sobre ataques futuros é fundamental - o que significa penetrar células enquanto o ataque ainda está sendo planejado, da mesma forma que informação precisa e ágil sobre a falta de unanimidade no Politburo permitiu a resolução pacífica da crise de 1962. Estes sucessos, aplicados ao terrorismo, têm se mostrado infrequentes.

Além disso, os grupos que constituem ameaças não são países, e não sofrem pressão caso passem da linha; suas ações não estão sujeitas à condenação pela comunidade internacional; operam,

ao invés disso, como centros de financiamento e direção a células individuais. Nesse sentido, tomam vantagem de alvos de oportunidade, e talvez sejam mais suscetíveis a infiltração por polícias locais do que por agências de inteligência nacional.

Oficiais de caso não são espiões - eles *recrutam* e *gerenciam* espiões. Considerando a baixa popularidade do Ocidente no Oriente Médio, estas são tarefas muito difíceis. Técnicas utilizadas para espionar a URSS, porém, podem ser adaptadas.

O primeiro ponto de aproximação pode ser ideológico - interesses e identidades que podem ser vistas como compatíveis com os interesses do recrutador. Há, porém, uma grande distância entre a concordância ideológica e o comprometimento de um espião. Na experiência do *spymaster* Viktor Cherkashin, ninguém jamais traiu seu país e amigos por razões puramente ideológicas.

Construir uma rede nesse estilo dentro de uma organização terrorista é um mundo novo, e de sucesso absolutamente incerto. O ideal seria um líder que acredita no renascimenento do poder e prestígio do Islã, mas não na imposição da *sharia* e na oposição ao empoderamento feminino. No presente, os sacerdotes com interpretações alternativas não parecem estar dispostos a lutar por elas.

Certamente o Ocidente está buscando inteligência sobre futuros ataques, mas no momento esta tende a vir de vigilância e inteligência eletrônica mais intensa, visto que células pequenas são particularmente difíceis de penetrar. O sucesso tenderá a vir de melhor policiamento, não de ações encobertas.

O mais comum é que a espionagem ocorra graças a algum benefício individual ao espião, pagamento ou outro auxílio. O pagamento é mais simples do que a ideologia, e muitos serviços o preferem. Em certas regiões, auxílio médico pode ser ainda mais poderoso.

Estas técnicas continuam válidas, e o pagamento auxiliou na captura de Hussein, bem como de diversos operadores da Al Qaeda. Estas técnicas podem também ser utilizadas em oficiais de inteligência dos países da região, que podem ter tido mais sucesso em se aproximar dos alvos. Naturalmente, nem sempre o dinheiro ajuda, e nem sempre deve ser oferecido - especialmente quando são os laços de respeito e amizade que aproximam o espião da agência.

Menos admirável é a vontade de vingança, outra razão para espionar. Diversas vezes durante a Guerra Fria a espionagem foi uma forma de se vingar de um governo que falhava em reconhecer o trabalho de um oficial desapontado.

O que se repete em todas estas situações, porém, é que os espiões em potencial sabiam para quem queriam trair informações e sabiam como fazê-lo - esta situação provavelmente não se repetirá. O foco em contra-inteligência também não se verá novamente - o conhecimento ocidental sobre o processo de tomada de decisão da Al Qaeda é inexistente. Assim, penetrá-la é muito mais difícil. A própria identificação de alvos é dificílima.

Outros pecados que levam à espionagem são escândalos que potenciais espiões querem manter em segredo, permitindo assim a intimidação pelo recrutador; o medo do recrutador; e a solidariedade étnica ou religiosa.

O uso de escândalos sexuais contra oficiais soviéticos nunca se mostrou efetivo às agências do Ocidente, mas os soviéticos os utilizaram extensivamente contra oficiais dos EUA, lançando "andorinhas" em oficiais ocidentais solitários - oficiais soviéticas treinadas em sedução ocidental. Imagens eram obtidas, e então utilizadas para forçar a cooperação. Esta técnica parece

ser promissora em seu uso em zelotas islâmicos. No entanto, o histórico de tentativas não é bom - a inteligência ocidental é muito inocente quanto à sexualidade de islamistas para utilizá-la com sucesso.

Por sua vez, o uso de intimidação também não entregou bons resultados quando utilizado contra o Oriente, mas há um elemento de coação em todo relacionamento entre espião e oficial - após cruzar o Rubicão, um espião é um traidor, e seu oficial sabe disso. O ato de espionar cria uma pressão eterna e intimidadora para continuar e para se conformar.

Tendo dito isto, o uso de tortura e intimidação pode ter efeitos contrários, desincentivando o recrutamento de novos espiões. As agências de inteligência dos EUA não são inteiramente imunes à Emenda McCain de 2005, que proíbe o uso de tratamento desumano.

A simples amizade, como demonstrado pela proximidade entre Oleg Penkovsky e Charles MacLean Peeke, pode também ser poderosa, especialmente quando acompanhada pela perda da crença no próprio sistema. Nestes casos a oferta de dinheiro pode ser prejudicial.

Este incentivo é mais relevante no que tange oficiais de serviços de inteligência do Oriente Médio, capazes de se aproximar dos alvos e com um imenso apetite por tecnologia e assistência material ocidental, negociações que levam a amizades.

Solidariedade étnica ou religiosa é outra causa poderosa, como no caso de Jonathan Pollard, um judeu americano que se sentiu obrigado a cooperar com Israel por sua etnia. Esta causa é também vista com certa frequência nos laços entre chineses americanos e a República Popular da China, ao menos aos olhos da China.

Os impactos da solidariedade étnica ou religiosa como bases para recrutamento de árabes muçulmanos são importantes, mas são muito mais relevantes no que tange a contra-inteligência. A desconfiança racista impede que muitos voluntários da etnia se aproximem dos serviços americanos de inteligência - o que é ainda mais problemático considerando a imensa necessidade por falantes nativos de idiomas do Oriente Médio. Em outras palavras, a ignorância cultural e o racismo nos EUA favorecem a ameaça do fundamentalismo. Na ofensiva uma deficiência similar está presente - em 2003, apenas 22 estudantes americanos se formaram em estudos árabes.

Por fim, houveram muitos casos nos quais a motivação para espionar era a espionagem em si - como no caso de Allen W. Dulles, oficial e diplomata brilhante que buscava a aventura na atividade de inteligência contra o Terceiro Reich, e futuro diretor da CIA. Em outros casos, porém, como no de Ames e Hanssen, esta motivação pode vir acompanhada de arrogância que leva à captura do espião. Ainda assim, o interesse pelo jogo da espionagem e a habilidade são importantes e deves ser buscados também quando operando em organizações fundamentalistas transnacionais.

Concluímos pela relevância da HUMINT, mas também por sua grande modificação desde a era soviética. Suas aplicações serão mais policiais e menos reminescentes das guerras de espiões, e se estenderão a fontes menos tradicionais de informação, como a OSINT. O único fator que permanece constante é o ser humano, com suas forças, complexidades e, felizmente, fraquezas e vulnerabilidades.

The dilemma of open source intelligence: is OSINT really intelligence?

Arthur S. Hulnick

O sistema americano de inteligência sempre foi ambivalente sobre material colhido de fontes abertas. Gerentes de inteligência valorizam seu valor, mas seus mecanismos de coleta encolheram com o fim da Guerra Fria. Após o 11 de setembro, a área voltou a crescer.

Em 2004, sob o DNI, um novo escritório foi criado para analisar fontes abertas, o OSC. Os usuários não se mostraram tão entusiasmados quanto os criadores do novo sistema. Pesquisas mostraram que os usuários têm menos paciência e interesse para ler relatórios de inteligência de fontes abertas.

Ainda assim a OSINT era bem vista pelos oficiais de inteligência, e para oficiais de caso comparar a OSINT com o que suas fontes secretas lhes dão é muito valioso.

A OSINT costumava ser obtida por meio de publicações físicas, por vezes obtidas por assinatura regular. Em geral, OSINT compõe 80 por cento da inteligência disponível ao analista, o que pode não ser verdade quanto a sociedades mais fechadas. OSINT também não é tão útil para lidar com problemas transnacionais, embora indique o que outros países estão fazendo a respeito.

No setor privado surgiram uma série de serviços de análise de OSINT para clientes pagantes por assinatura. O *Department of Homeland Security* faz a mesma análise, e a disponibiliza ao público. Nesse sentido a OSINT é a principal ferramenta de inteligência no setor privado, incluindo informações financeiras e sobre competidores. Usa-se também a "inteligência cinzenta", de informações menos disponíveis, escondidas e encontradas em arquivos públicos econômicos, compilando os produtos finais de acordo com a requisição dos usuários finais, incluindo também recomendações de decisão - o que nunca existe em relatórios de inteligência governamental.

Apesar das reservas que usuários têm quanto à OSINT, ela chega a muitas publicações nacionais, estudos, boletins e estimativas. É parte, portanto, da mistura de fontes que analistas utilizam rotineiramente.

No contexto de alerta estratégico, a OSINT foi capaz de perceber a morte de Konstantin Chernenko antes que fosse noticiada, interpretando a programação musical da Rádio Moscou. Música marcial era uma indicação de que um golpe militar havia se iniciado. Hoje o alerta antecipado foi facilitado pelos serviços de radiodifusão de 24 horas, de forma que seria muito difícil não perceber um evento de qualquer significância política. Este sistema, naturalmente, não poderia identificar ameaças pequenas transnacionais, mas viu facilmente como a reação global ao 11 de setembro se desdobrou.

OSINT é uma boa base para a análise posterior, mas o que torna esta análise especial é a inteligência humana e outras fontes sensíveis.

Esta situação não mudou quando os materiais de OSINT mudaram. Muito do que se observa é propaganda e retórica, mas há ocasionais vazamentos úteis mesmo em regimes de mídia controlada.

Trata-se de uma ferramenta útil, ainda que os usuários prefiram fontes sensíveis. Sua redução, então, pode talvez ser explicada pela diminuição da necessidade de entender o que saía das sociedades comunistas fechadas, especiamente em mídia regional de menor relevância, que deixou de ser monitorada, reduzindo o pessoal e recursos dedicados à OSINT.

Um certo número de oficiais se dedicou a evitar o desaparecimento da OSINT, e no ato de 2004 um escritório foi criado, ainda que tenha sido uma tentativa falha. A análise foi obrigada a depender do setor privado para a coleta e processamento de OSINT.

A proliferação de fontes expandiu o mundo da OSINT de forma que há simplesmente material demais, e se utilizam formas de "mineração de dados" automatizada para organizar as bases de dados. Os oficiais contemporâneos entendem tecnologia e nela são capazes, uma mudança generacional. Outra mudança é aproliferação de sistemas de reconhecimento comercial, como o Google Earth. Estes sistemas não são de resolução ou tempo comparável aos sistemas sensíveis, mas ainda assim atraíram atenção e são usados como outros sistemas de OSINT.

Ainda que as fontes sejam abertas, há razões para tratar algumas delas como sensíveis, e proteger os relatórios finalizados, porque decisões são extrapoladas a partir destes relatórios. Outra questão é o *copyright*, e o fato de que OSINT também serve para reconhecer algo que os adversários querem esconder.

Mesmo considerando o baixíssimo custo de coleta de OSINT, há certos contras no mundo da inteligência ed fonte aberta, especialmente que pode incluir desinformação e falsidades em abundância. Fontes humanas mentem ou dizem mais do que sabem, imagens são ambíguas e interceptações sofrem de má tradução - a OSINT traz seus próprios problemas. Por isso analistas sempre estão buscando a pepita de ouro comparando múltiplas fontes, mas ela quase nunca aparece.

A paciência e habilidade são necessárias para encontrar a interpretação mais confiável. Nada é mais politizado ou parcial do que a blogosfera, e separar o joio do trigo é uma habilidade crucial.

Desinformação é um problema mais perigoso, envolvendo pequenas verdades em histórias falsas. Normalmente a desinformação é facilmente reconhecida por analistas de inteligência, mas não necessariamente pelos usuários.

Pode haver também o uso de esteganografia, ou o envio de mensagens secretas escondidas na mídia aberta. Esta técnica não é nova. Por fim, enquanto poucos países podem ter satélites espiões, todos utilizam imagens comerciais, inclusive para encontrar alvos e espionar sistemas militares.

Há aspectos importantes na contra-inteligência da OSINT. Os EUA disponibilizam um grande volume de informações, mesmo com seu sistema de controle de segredos nacionais, e cidadãos americanos podem requisitar qualquer informação abaixo de certo nível de segredo de acordo com o *Freedom of Information Act*.

A obtenção de OSINT por adversários pode ocorrer mesmo a partir das publicações abertas da própria CIA, em centenas de artigos sobre estudos de inteligência. Já há algum tempo, porém, Langley controla quais destes artigos podem de fato ser abertos ao público. O comitê de revisão negava certo conteúdo porque acreditava que confirmaria operações da CIA que

não eram abertamente reconhecidas, mas certas vezes mesmo a ira do comitê não levava à censura.

Aprender sobre a CIA não é mais difícil, e há uma abundância de artigos precisos, ainda que o segredo de fontes e métodos seja bem mantido. O Congresso publica também estudos públicos que incluem questões de segurança e inteligência. O governo Bush tentou, sem sucesso, restringir a circulação deste tipo de material, criando então outras categorias, como "sensível" (para material não secreto, mas alegadamente sensível).

OSINT é, claramente, inteligência. Steele acredita que poderia mesmo substituir certas fontes sensíveis, ainda que seus números sejam difíceis de defender. A OSINT tem sido bem vista com frequência por oficiais de inteligêjcia desde a abertura do Open Source Center.

A OSINT de fato fornece informação, sobre adversários, que estes adversários podem não querer que tenhamos. Bem interpretada, pode ser tão esclarecedora quanto uma gente bem informado ou uma imagem nítida. O que importa, no final, é a habilidade de entregar bons julgamentos aos tomadores de decisão - e se a OSINT é capaz de ajudar a fazê-lo, ela vale o custo e o esforço de sua análise.

Artificial intelligence on the battlefield: implications for deterrence and surprise

Zachary Davis

A inteligência artificial avançou sobre o campo da segurança nacional dos EUA a uma grande velocidade, por sua percepção como uma tecnologia revolucionária, sua absorção rápida pela economia, e as ambições de potenciais adversários.

1 AI, Big Data e Machine Learning

Até o momento a comunidade de segurança nacional não tem uma linguagem comum para discutir as novas tecnologias. O termo "inteligência artificial" é usado para discutir uma miríade de fenômenos, assim como o genérico "*cyber*".

Na maioria das aplicações, AI trata de algoritmos de reconhecimento de padrões, que são "treinados" para associá-los a resultados desejados, incluindo nisto o processamento de texto e a inferência. É um imenso salto no reconhecimento de informação "enterrada", desde que se saiba qual a informação que se busca.

AI geral tenta recriar funções do cérebro humano. AI específica, embora muito significativa, está também muito distante de conseguir replicar a razão humana.

AI específica, porém, já está presente, com grandes aplicações nas ciências, até mudando padrões metodológicos antigos. No mercado, potencializou ferramentas de análise e outras áreas ricas em dados. Nesses casos, porém, é mais uma ferramenta de apoio e multiplicação de força do que uma tecnologia revolucionária. O aumento da interconectividade ilustrado pela IOT dá ainda outra oportunidade à revelação de *insights* escondidos pela AI.

2 Aplicações militares e efeitos táticos e estratégicos

Como muitas tecnologias, a AI é carregada de potencial militar latente. Entre 2018 e 2019 os EUA iniciaram diversos comitês e ordens executivas sobre desenvolvimento e liderança em AI.

Para aplicações militares com análogos civis, a análise apoiada por AI já está em uso, mas são distintas daquelas de combate - que têm impactos táticos e estratégicos. Efeitos táticos são advindos de sistemas de armas e organização, e definimos efeitos estratégicos como aqueles capazes de causar a mudança do balanço de poder.

3 Aplicações táticas

O processamento dos grandes volumes de dados envolvidos em operações militares é um nicho natural para a AI. O Projeto Maven, cuja missão inicial era localizar soldados do Estado Islâmico, teve implicações vastas envolvendo volumes colossais de dados heterogêneos que só podem ser

explorados com o auxílio de AI.

O processamento veloz se traduz em duas vantagens militares - agilidade e alcance. A AI torna possível analisar condições de batalha dinâmicas em tempo real e atacar de forma otimizada e com menos riscos.

3.1 Veículos onipresentes e oniscientes

A nova geração de veículos autônomos é de alta prioridade para aplicações militares da AI, assim como a guiagem de plataformas espaciais e submarinas - permitindo não apenas a navegação, mas formações complexas.

O gerenciamento integrado de batalha, comando, controle, comunicações e inteligência (BMC3I) é peça chave para encontrar e atacar baterias de mísseis, e portanto pode ser fundamental para enfrentar elementos das estratégias de negação de área (A2AD) da Rússia e China. BMC3I guiada por AI pode ajudar a guiar e coordenar esforços envolvendo plataformas múltiplas.

3.2 Modelos e simulações

A AI aumenta o poder de simulações e ferramentas de estudo de emprego de armas nucleares e convencionais. Modelos de AI podem confirmar a confiabilidade do arsenal nuclear sem depender de testes nucleares, e o uso de modelos já é uma parte fundamental do design de quase todos os maiores sistemas de armas.

3.3 Coleta e análise de inteligência

Com a abundância de fluxos de inteligência sendo coletados, a comunidade de inteligência tem o desafio da sobrecarga de dados. Este é um problema que pode ser enfrentado com redes neurais analisando conjuntos multimodais de dados buscando evidências de atividades específicas. É também possível utilizar o *machine learning* para combinar dados financeiros de fonte aberta com outras formas de inteligência buscando transferências ilícitas.

4 Aplicações estratégicas

4.1 Reconhecimento e ISR

Identificação de objetos é um ponto natural para o auxílio da AI. A *National Geospatial-Intelligence Agency* liderou a aplicação da AI para necessidades militares e de inteligência, mas identificação é apenas o início - inteligência, vigilância e reconhecimento (ISR) são a chave para informação situacional, que se torna cada vez mais crítica.

4.2 Guiagem de precisão

A guiagem por AI torna possível localizar e atacar uma variedade de alvos estratégicos, como porta-aviões, mísseis móveis ou armas nucleares. Esta capacidade e percepções sobre sua existência poderiam romper a estabilidade da dissuasão - especialmente na existência de um ataque antiforças acompanhado da capacidade de abater qualquer retaliação remanescente, podendo erodir preceitos de dissuasão baseados na vulnerabilidade mútua.

4.3 Defesa antimíssil

Avanços em guiagem e navegação por AI poderiam melhorar possibilidades para um grande número de sistemas de defesa estratégica e tática contra mísseis balísticos. A convergência de capacidades ofensivas e defensivas poderia, porém, reacender medos de um ataque-surpresa, e assim erodir a estabilidade estratégica.

4.4 Cyber-AI

Como um domínio inerentemente digital, o "ciberespaço" atrai aplicações de AI, como nos algoritmos de mídia social. A disponibilidade de imensas quantidades de dados atrai sondagem, mapeamento e penetração por AI de sistemas de computadores, incluindo a descoberta de vulnerabilidades, identidades, relacionamentos e outras informações valiosas. De forma ofensiva, a AI poderia localizar indivíduos específicos para coleta, disrupção e desinformação. Ataques cibernéticos à estrutura de comando e controle poderiam ser catastróficos. Como capacidade ofensiva, a AI poderia também detectar estas intrusões e anomalias debilitantes em sistemas civis e militares.

5 Consequências em potencial

5.1 AI oponente

Não é possível ter os benefícios da AI e negá-los ao oponente. Os sistemas de negação de área (A2AD) russos e chineses, por exemplo, podem reduzir a confiança de aliados americanos nos sistemas dos EUA, e serem enfrentados com AI; mas mesmo a *percepção* do favorecimento da capacidade de primeiro ataque pode levar ao mau cálculo e à corrida armamentista. Quaisquer medidas devem levar a contramedidas que anulem vantagens iniciais.

5.2 Fragilidade de dados

Sistemas de AI são vulneráveis a *inputs* falhos de dados, levando a decisões incorretas e injustas. A inteligência artificial pode, pois, agravar o problema do "lixo adentro, lixo afora", especialmente quando os dados não são curados antes de sua análise. Mesmos sistemas modernos como o Projeto Maven são facilmente enganados por dados confusos ou falhos. Com campanhas de engano e desinformação, estas falhas seriam ainda mais amplificadas, e mesmo quando os dados são sólidos a AI ainda "alucina" com objetos que não existem. Acidentalmente acertar os alvos incorretos poderia ter consequências estratégicas muito sérias.

5.3 Manipulação de dados

O enfrentamento a muitos sistemas de AI pode ser simples. A manipulação de dados fornece muitas oportunidades de engano, e corromper dados de formas calculadas pode levar a pesadelos logísticos, má comunicação, confusão e erros devastadores. O problema da "caixa preta" da AI também significa que seria difícil perceber a manipulação de dados.

5.4 Perda de qualidade

Para o bom gerenciamento de crises, nem sempre a decisão e execução rápida são o melhor caminho. A própria Crise dos Mísseis foi vista por conselheiros como um caminho sem saída à ação militar antes de sua solução diplomática. As vantagens de campo de batalha poderiam reduzir o tempo disponível à diplomacia para evitar a guerra e mesmo a confrontação nuclear - afinal, em sua forma atual, sistemas de AI de análise do espaço de batalha não incluem qualquer consideração a esforços diplomáticos, violando o princípio clausewitzeano da continuação da política.

5.5 Sistemas de sistemas de sistemas

Sistemas de AI operam na base de *software* customizado para cada propósito. Não há um grande mecanismo para integrar sistemas operando em diferentes plataformas. Para empregar o ISR multi-domínio, é necessário integrar todo tipo

de sensores, armas e comunicações muito diferentes, operados por agências, comandos e empresas diferentes, com diferentes autoridades, acessos e procedimentos. Aliados teriam ainda outros supersistemas diferentes.

5.6 Alertas estratégicos requerem mais do que dados

A solução do desafio do alerta estratégico por meio de plataformas informadas por AI requer um sistema holístico de análise de ameaças que não se desenvolverá naturalmente, requerindo imensos esforços, e ainda que as novas técnicas sejam úteis, analistas precisarão ainda fazer julgamentos baseados em informação incompleta ou pouco confiável.

5.7 Imprevisibilidade

A integração e operação conjunta de sistemas de AI levará a resultados imprevistos que podem ter consequências estratégicas. A interação entre diferentes sistemas pode ser incerta, levando a resultados desconhecidos, mesmo inexplicáveis, como a seleção dos alvos incorretos. Também não se pode prever como a AI convergirá com outras tecnologias, e que surpresas estratégicas podem estar envolvidas.

5.8 Envolvidos

Os envolvidos no processo de tomada de decisão estão ficando muito numerosos, especialmente no que diz respeito à autoridade de tomada de decisão e hierarquias organizacionais. Com diversos sistemas de AI lendo o mesmo campo de batalha, cada um conectado a sua própria cadeia de comando, a *coordenação entre os humanos* envolvidos na decisão sobre um tema extremamente dinâmico e envolvendo dezenas de atores, como empresas, aliados, adversários, agências e culturas organizacionais se torna mais difícil. Cada humano envolvido influenciará como a AI contribui para objetivos separados e comuns.

5.9 Manipulação da percepção pública

O uso de AI em mídias eletrônicas para manipular percepções públicas pode afetar a estabilidade estratégica, afetando também como os líderes reagem e decisões sobre escalação e pacificação de conflitos.

5.10 Aproximações insuficientes

Decisões de guerra e paz não podem depender inteiramente de análises preditivas. Há diferenças fundamentais na forma como se usam dados para propósitos científicos, econômicos, logísticos e na *previsão do comportamento humano*. As previsões dos sistemas de AI em relação ao resultado de conflitos não são aceitáveis, ao menos nas margens de erro envolvendo questões de guerra e paz - e um otimismo excessivo em predições mágicas poderia levar a catástrofes. Não se pode esquecer que a imprevisibilidade humana está nos dados **e** na tomada de decisão, com amplas margens de erro.

5.11 Parcerias público-privadas

Parcerias público-privadas determinam o futuro da AI, mas a guerra permanece responsabilidade do Estado. Inteligência artificial é acessada e utilizada além dos controles governamentais, e governos utilizam a *expertise* civil para desenvolver AI de uso militar. Competição entre países para buscar talento civil na nova tecnologia pode levar a crises estratégicas de contra-inteligência, propriedade intelectual e respeito por normas internacionais.

5.12 Conflitos de interesse

Na prática, isso significa que muitos países usarão os mesmos especialistas, empresas e cadeias de suprimento para apoiar seus esforços militares em AI. Esta dinâmica já é evidente nos mercados digitais, onde grandes companhias acomodam práticas chinesas enquanto expressam oposição a projetos como o Maven - o governo americano, porém, não tem escolha além de depender do setor privado para desenvolver e implementar estratégias de AI, o que pode ter efeitos estratégicos caso prejudique a habilidade de competir por talento e capacidade.

6 Alterações no cálculo fundamental da dissuasão

6.1 Mudança de percepções

No topo da lista de aplicações estratégicas da AI está a ameaça de ataque surpresa. A possibilidade de encontrar e atacar alvos móveis reacende medos relativos ao primeiro-ataque incapacitante. Ainda que a lógica da dissuasão não se modifique, a mera percepção sobre sua mudança pode levar a uma variedade de contramedidas.

As contribuições da AI não substituem cálculos políticos - o ataque de Pearl Harbor foi um resultado de má interpretação do cálculo de risco do governo japonês, pois os EUA reconheciam a capacidade de Tokyo de lançar um ataque transpacífico. A responsabilidade permanece nos líderes - a possibilidade de um ataque desarmador ainda envolve riscos gigantescos. Ela ainda assim traz consigo um dilema clássico de segurança, que trará contramedidas daqueles ameaçados.

6.2 Perda da vulnerabilidade mútua

A combinação de excelente ISR com um escudo eficaz poderia tornar mais tentador um ataque desarmador, decapitador ou cegador. Esta revisão da lógica da dissuasão poderia ser muito desestabilizante, visto que a vulnerabilidade compartilhada e retaliação assegurada são pontos centrais da teoria da destruição mútua assegurada - daí a afirmação de Putin em março de 2018 de que suas novas armas eram imunes a qualquer sistema de defesa. Evitando as *percepções* sobre as capacidades antimíssil dos EUA, Putin engajou-se num esforço para preservar a MAD.

6.3 Alterações regionais

Plataformas de ISR apoiadas por AI podem afetar a estabilidade regional. Aliados dos EUA estão avançando suas próprias capacidades no assuntos. Inicialmente, as capacidades do ocidente poderão fornecer opções para enfrentar os sistemas A2AD chineses e russos.

Em adição a benefícios táticos, o co-desenvolvimento de ISR multidomínio permite colaboração para enfrentar diretamente ameaças à segurança de aliados americanos na Ásia e Europa. O fortalecimento da dissuasão regional e dissuasão nuclear extrarregional reduz a motivação para assumir riscos e apoia interesses mais amplos. Aplicações que apoiem estes objetivos serão benéficas à estabilidade estratégica.

6.4 Benefícios da competição

A competição global em AI já começou - há uma corrida armamentista em curso. Quaisquer vantagens podem ter vida curta conforme contramedidas e riscos aumentam. Estes não são problemas técnicos, mas modificadores da natureza

da guerra. No momento o cálculo da dissuasão permanece estável.

7 Riscos de consequências imprevistas

É possível especular sobre como os desenvolvimentos em AI mudarão a guerra e a estabilidade estratégica, mas as interações entre tecnologias poderão produzir duplos desconhecidos que não se pode prever, mas os principais riscos podem ser assim descritos:

- Dados distorcidos podem levar sistemas de AI a tomar ações não intencionais, e dados podem ser distorcidos intencionalmente.
- AI comete erros com uma frequência que pode ser inaceitável para decisões estratégicas.
- A convergência de AI e do domínio cibernético pode trazer consequências imprevisíveis à estabilidade estratégica, como em ataques cibernéticos à NC3 apoiados por AI.
- Um ritmo de batalha acelerado pelo ISR multidomínio pode impedir esforços diplomáticos.
- Interações entre sistemas de AI de países diferentes podem produzir cálculos incorretos.
- Convergências com outras tecnologias, como computação quântica ou EMPs, podem confundir ou distorcer as instruções.
- A guiagem a alvos estratégicos como submarinos seria capaz de destruir a santidade da retaliação assegurada, e produziria efeitos muito desestabilizadores.

8 O desafio maior

Mudanças na lógica da dissuasão e estabilidade regional não são novas nem necessariamente prejudiciais. Aplicações que apoiem forças nucleares aumentando capacidades de infraestrutura e logística reforçam a dissuasão aumentando a credibilidade das forças retaliatórias.

AI tática também pode apoiar a dissuasão estratégica, especialmente conforme a letalidade e agilidade do nível tático produz resultados que podem escalar ao nível estratégico. Os EUA e seus aliados ainda mantém superioridade convencional, e a AI pode estender estas vantagens e derrotar a A2AD russa e chinesa - e estes podem escolher uma escalação estratégica ao invés de concessões.

Para que as aplicações militares de AI avancem objetivos de segurança nacional, elas precisam ser integradas a uma estratégia mais ampla, que necessariamente reforce a dissuasão estratégica nos níveis regional e estratégico.

Intelligence reform: balancing democracy and effectiveness

Thomas C. Bruneau, Steven C. Boraz

O analista de inteligência estratégica não tem tempo para conduzir pesquisas e testar hipóteses alternativas - o usuário que requisitá-lo quase certamente precisará de respostas imediatas. Por isso é necessário que a experiência, a pesquisa e o pensamento sejam passados à crise - e é aqui que o treinamento e a experiência são mais importantes.

A análise de inteligência é a atividade mais intelectualmente difícil e sofisticada de toda a comunidade de inteligência, sendo necessário ir além do que parece ocorrer e buscar o significado de dados ambíguos, inconsistentes, incompletos e contraditórios.

Dados inconclusivos são parte comum da análise de inteligência. Os tomadores de decisão precisam ser capazes de ver dados objetivamente e fazer julgamentos sem evidência conclusiva. Conectar os pontos não é fácil quando não se sabe se os pontos existem ou se devem ser conectados.

O propósito é tentar entender o que ocorre no mundo, discernindo fatos pertinentes de um fluxo infinito de informação. A essência da análise é informação e *insight*, derivada de conhecimento de caso preexistente, com o objetivo de alertar sobre crises, identificar ameaças, monitorar situações dinâmicas, esclarecer problemas e detectar tendências, ajudando o tomador de decisão a considerar opções e resultados alternativos.

1 Fontes

O trigo do analista é uma mistura de todo tipo de informação, incluindo muita informação amplamente disponível (OSINT), bem como HUMINT, SIGINT, IMINT e MASINT. O volume é imenso, a alimentação é rápida e há sempre o ruído de informação contraditória ou imprecisa, bem como a desinformação intencional.

O caráter "de múltiplas fontes" reflete o fato de que raramente uma única fonte será completa o suficiente, e as fontes precisam ser complementadas e verificadas ao máximo. Abaixo dos grandes grupos jihadistas operam pequenas células, cujas operações só podem ser identificadas utilizando todo o conjunto de informação coletada para encontrar os planos de poucos indivíduos.

Ter múltiplas fontes é o ideal, não a regra, e mesmo múltiplas fontes podem enganar. A diferença entre a escrita de inteligência e a escrita acadêmica é que o analista de inteligência escreve antes de se sentir pronto para fazê-lo. O material precisa ser completo, com ou sem o tempo ideal.

2 Dados crus e relatórios finais

A análise gera o produto final, mas o processo é um ciclo - a análise identifica lacunas, que pedem mais coleta, que pede mais análise. Os pro-

blemas enfrentados pelos usuários finais definem os requerimentos da coleta.

Antes da análise, certo processamento pode ser necessário nos dados brutos, como em decodificação e tradução de textos, e interpretação de imagens. Apenas depois de uma pré-verificação dos dados brutos eles se tornam objetos de inteligência. O pessoal envolvido no processamento pode ser visto como um conjunto de analistas, mas seu trabalho não é a produção de produtos finais de inteligência.

O termo "inteligência final" se refere a qualquer produto que tenha completado o rigoroso processo de correlação e verificação de múltiplas fontes, bem como passado por um processo de revisão. Se dá em diversas formas, e analistas são chamados para produzir algumas e todas.

Inteligência atual lida com eventos cotidianos e indicações de tendências. Os relatórios buscam significados, alertas e consequências de curto prazo, e são frequentes em forças-tarefa dedicadas a crises específicas.

Inteligência estimativa parte do que se sabe e busca o desconhecido, ou mesmo o incognoscível. Ela provém guias estratégicos para políticas de três a cinco anos no futuro, sugerindo padrões alternativos e produzindo análises informadas da possibilidade de certos resultados.

Inteligência básica compila dados de referência na forma de monografias (biográficos, geográficos, militares, econômicos), estudos, mapas, ordens de batalha e publicações.

Outros tipos de inteligência final incluem inteligência de alerta, inteligência para apoio operacional, focada na condução de operações específicas, e inteligência científica e técnica, que reportam avanços técnicos e características de sistemas estrangeiros incluindo armamentos. Nenhum destes produtos finais, porém, conclui o processo - sua produção é contínua envolvendo disseminação, *feedback* e outras partes de um processo dinâmico. O salto do analista na direção do desconhecido é constante - utilizar o julgamento e a experiência específica para desafiar os limites da incerteza.

3 Abundância de informação

Durante a Guerra Fria, o problema era frequentemente a falta de informação, que era essencialmente secreta e de difícil obtenção. No século XXI o desafio está na abundância de informação aberta, um ruído que deve ser superado. Dados se multiplicam, e sua seleção e validação se tornam cada vez mais trabalhosas.

Os analistas, assim, precisam cavar mais fundo para encontrar melhores informações para os usuários. Recipientes de análise que já são bem informados precisam de relatórios particularmente bons. Até certo ponto, servem como seus próprios analistas - eles não precisam de lugares-comuns, mas de *insights* únicos relativos a problemas já bem compreendidos pelos usuários. Ademais, o analista precisa seguir o mantra da neutralidade e objetividade num esforço constante. Parcialidade sempre aparece, e o custo pago é em credibilidade.

4 Primazia da escrita

Apresentações orais podem ser requisitadas, mas a maior habilidade do analista é sua escrita e pensamento claros. Enquanto acadêmicos escrevem para outros acadêmicos, analistas escrevem para leigos em potencial que não tem tempo para um estudo detalhado. O analista, portanto, precisa ser a ponte entre o generalista e o especialista.

Além disso, para atingir os níveis mais altos, o relatório precisa ser conciso. Uma página ou nada; três minutos ou nenhum. Não apenas escrever

para ser compreendido, mas escrever de forma que a ambiguidade seja impossível. Um dos produtos mais efetivos pode ser um comentário de duas frases, seguido por uma atualização de dois parágrafos.

5 Expectativas

Demandas e expectativas sobre o analista aumentam conforme tomadores de decisão não têm tempo para ler ou contemplar, e precisam de ajuda para lidar com os fluxos de informação. O número de usuários cresce. O que é escrito compete por atenção de múltiplas fontes. A chave não é inundar o usuário de informação, mas ser ágil, relevante e valioso, indo além do que já se sabe sobre um assunto já bem explorado pela mídia.

6 Neutralidade

A prática tem se afastado dos métodos tradicionais de se afastar da política do tomador de decisão e mesmo do coletor de informação. Trabalhar em colaboração permite que o analista perceba de qual informação o tomador de decisão precisa, e coletores têm uma ideia melhor do que coletar. Hoje analistas sentam lado a lado com coletores de HUMINT.

Dar ao usuário o que ele quer sem se molhar em sua política é quase impossível. É necessário iluminar alternativas sem sugerir qual deve ser tomada, e a colaboração aumenta o risco de politização da inteligência. O centro da atividade ainda é, porém, dar a verdade ao poder.

Carmen Medina não defende a neutralidade, mas integridade, definida como uma ética profissional específica acompanhada de honestidade intelectual. É importante também perceber que os usuários *sabem* o que querem fazer. A inteligência é o argumento, não a razão. Ainda que os usuários "selecionem" alternativas que recebem da inteligência, é importante que o analista não "selecione" as alternativas que demonstra. A perda de credibilidade é fatal à carreira de análise.

7 Reformas

A imensa falha de inteligência que não foi capaz de prever os ataques de 11 de setembro foi atribuída a alguns fatores: a ênfase na inteligência atual, a falha em reconhecer a atração da religião politizada, a desconsideração das proclamações de Bin Laden e de cooperação entre sunitas e xiitas, e a incapacidade de relacionar eventos na Ásia, no Oriente Médio e na Malásia e Indonésia, sendo a comunidade de inteligência organizada regionalmente.

O consenso é que os analistas haviam se tornados aversos ao risco, evitando falhas ao invés de imaginar surpresas. Inteligência mais imaginativa, porém, sempre encontra obstáculos:

Clientite, ou a tendência a se apaixonar pelo país que se estuda, é bem conhecida. *Espelhamento* é a assunção que outros fariam como você, especialmente quando acompanhado de etnocentrismo. *Mindset* é a tendência a avaliar informação nova de acordo com uma hipótese existente. *Groupthink* é a inclinação a reforçar interpretações com outros chegando às mesmas conclusões, o que pode levar a confiança exagerada. *Análise linear* presume uma projeção sequencial na qual cada evento flui logicamente ao próximo, e não permite o resultado inesperado. A análise linear leva a a uma lagarta diferente, mas para chegar à borboleta é necessária imaginação.

A comunidade de inteligência não acreditava que um ator racional enviaria mísseis a Cuba, e seu erro corrigido mostrou que se deve ser cético frente ao modelo do "ator racional". O tomador de decisão não viu a ação como irra-

cional, e é importante sair da mente "ocidental" para perceber motivos e políticas de líderes estrangeiros. A conclusão de que Hussein tinha armas de destruição em massa foi uma tempestade perfeita de *mindset*, *groupthink* e análise linear.

8 Padrões

Análise tem muito a ver com o reconhecimento de padrões. Tomadores de decisão insistem que querem projeções de longo prazo, mas sua atenção sempre se volta ao aqui e agora. O fato de que eventos globais são reportados pela mídia constantemente contribui para uma situação de crise perpétua, que precisa de respostas imediatas a tudo. O fato é que usuários precisam de inteligência atual e de longo prazo, e a falta de uma ou outra torna o conjunto de produtos incompleto.

9 Riscos ocupacionais

O erro é parte comum da atividade de inteligência. Falhas de inteligência não são apenas inevitáveis, são naturais. Não importa quão incompleto um julgamento possa ser, ele é esperado e precisa ser feito. Não há reorganização capaz de reparar erros de inteligência, porque o problema é a incerteza em si. Este é um custo intrínseco à atividade. Frequentemente se acerta, porém, e constantemente a inteligência prova seu valor - melhor produzida por analistas que deixam seus preconceitos na porta.

Os problemas acima continuarão existindo, mas novos esforços de reorganização e treinamento são sempre bem vindos. O treinamento continua ao longo da carreira de um analista, e a profissionalização enfatiza o uso de múltiplas hipóteses e interpretações alternativas.

Personalidade e temperamento são também importantes, sendo necessário trabalhar com prazos curtos. É necessário mergulhar em montes de dados e conceitualizar conhecimento substantivo a partir deles, contribuindo substancialmente à segurança nacional numa profissão fascinante.