UNIVERSIDADE ESTADUAL DE CAMPINAS
INSTITUTO DE GEOCIÊNCIAS

ÉRICO SANT'ANNA PERRELLA

FORA DO CONTROLE: O AMBIENTE INFORMACIONAL NOS MANUAIS MILITARES DO DEPARTAMENTO DE DEFESA DOS EUA

CAMPINAS
2022

ÉRICO SANT'ANNA PERRELLA

FORA DO CONTROLE: O AMBIENTE INFORMACIONAL DOS MANUAIS MILITARES DO DEPARTAMENTO DE DEFESA DOS EUA

DISSERTAÇÃO APRESENTADA AO INSTITUTO DE GEOCIÊNCIAS DA UNIVERSIDADE ESTADUAL DE CAMPINAS PARA OBTENÇÃO DO TÍTULO DE MESTRE EM POLÍTICA CIENTÍFICA E TECNOLÓGICA

ORIENTADOR: PROF. DR. MARKO SYNESIO ALVES MONTEIRO

ESTE EXEMPLAR CORRESPONDE À VERSÃO FINAL DA DISSERTAÇÃO DEFENDIDA PELO ALUNO ÉRICO SANT'ANNA PERRELLA E ORIENTADA PELO PROF. DR. MARKO SYNESIO ALVES MONTEIRO

CAMPINAS

2022

Ficha catalográfica
Universidade Estadual de Campinas
Biblioteca do Instituto de Geociências
Marta dos Santos - CRB 8/5892

P426f

Perrella, Érico Sant'Anna, 1991-
Fora de controle : o ambiente informacional dos manuais militares do Departamento de Defesa dos EUA / Érico Sant'Anna Perrella. – Campinas, SP : [s.n.], 2022.

Orientador: Marko Synesio Alves Monteiro.
Dissertação (mestrado) – Universidade Estadual de Campinas, Instituto de Geociências.

1. Estados Unidos. Department of Defense. 2. Informação. 3. Cibernética. 4. Inteligência militar. 5. Etnologia. I. Monteiro, Marko Synesio Alves, 1975-. II. Universidade Estadual de Campinas. Instituto de Geociências. III. Título.

Informações para Biblioteca Digital

Título em outro idioma: Out of control : the informational environment in the military manuals from the US Department of Defense
Palavras-chave em inglês:
Department of defense
Information
Cybernetics
Military intelligence
Ethnology
Área de concentração: Política Científica e Tecnológica
Titulação: Mestre em Política Científica e Tecnológica
Banca examinadora:
Marko Synesio Alves Monteiro [Orientador]
Alcides Eduardo dos Reis Peron
Anna Catarina Morawska Vianna
Data de defesa: 30-06-2022
Programa de Pós-Graduação: Política Científica e Tecnológica

Identificação e informações acadêmicas do(a) aluno(a)
- ORCID do autor: https://orcid.org/0000-0002-7073-6481
- Currículo Lattes do autor: http://lattes.cnpq.br/2802651822952257

UNIVERSIDADE ESTADUAL DE CAMPINAS
INSTITUTO DE GEOCIÊNCIAS

AUTOR: Érico Sant'Anna Perrella

FORA DE CONTROLE: O AMBIENTE INFORMACIONAL DOS MANUAIS MILITARES DO DEPARTAMENTO DE DEFESA DOS EUA

ORIENTADOR: Prof. Dr. Marko Synesio Alves Monteiro

Aprovado em: 30 / 06 / 2022

EXAMINADORES:

Prof. Dr. Marko Synesio Alves Monteiro - Presidente

Prof. Dr. Alcides Eduardo dos Reis Peron

Profª. Drª. Anna Catarina Morawska Vianna

A Ata de Defesa assinada pelos membros da Comissão Examinadora consta no processo de vida acadêmica do aluno.

Campinas, 30 de junho de 2022.

DEDICATÓRIA

Dedico esta dissertação aos meus avós Marinalva, Manoel, Francesco e Giuseppina. Suas ações em meio aos tempos e eventos turbulentos do Século XX mostram que é possível e necessário ter esperança no futuro.

AGRADECIMENTOS

Esta dissertação não seria possível sem o suporte e carinho dos meus pais Miguel e Cileda, do meu irmão Gabriel e da minha companheira de vida Clarissa. Se o mundo acadêmico fosse menos individualista, Clarissa inclusive seria oficialmente co-autora deste trabalho, já que muitos fios, ideias e palavras expressos aqui se originaram conjuntamente por entre nossos corpos.

Não podem faltar agradecimentos aos meus avós, Marinalva, Manoel, Francesco e Giuseppina e aos meus tios Zenon, Cilda, Calixto, Felice, Rosa e Antônio. Todos os meus amigos sintam-se contemplados também, assim como os gatinhos Chiba, Ameixa e Nenê, sem vocês nada seria possível.

Ao meu orientador Marko, agradeço por toda a paciência e rigor.

Aos meus companheiros e professores da pós-graduação agradeço pelo quanto aprendi com vocês, especialmente sobre disciplinas e áreas diferentes da minha.

Aos funcionários do Instituto de Geociências da UNICAMP pela prestatividade, paciência e eficiência.

À CAPES, por viabilizar o financiamento para a pesquisa.

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Código de Financiamento 001.

EPÍGRAFE

Gonna lay down my burden,
Down by the riverside,
Gonna lay down my sword and shield,
Down by the riverside,
Ain't gonna study war no more.
Study war no more.
Canto spiritual negro estadunidense

Until the philosophy
Which hold one race superior
And another, inferior
Is finally and permanently
Discredited and abandoned
Everywhere is war
Me say war
That until there are no longer
First class and second class citizens of any nation
Until the color of a man's skin
Is of no more significance than the color of his eyes
Me say war
That until the basic human rights
Are equally guaranteed to all, without regard to race
Dis a war
That until that day
The dream of lasting peace
World citizenship
Rule of international morality
Will remain but a fleeting illusion to be pursued
But never attained
Now everywhere is war
Bob Marley and the Wailers, War

RESUMO

O trabalho segue etnograficamente como se constitui e opera o “ambiente informacional”, conceito utilizado extensivamente em manuais militares estadunidenses recentes. Definido no Dicionário de Termos Militares do Departamento de Defesa (DoD) dos EUA como “o agregado de indivíduos, organizações e sistemas que coletam, processam, disseminam e agem baseados em informação”, o ambiente informacional tem o potencial de abarcar todo o mundo, tal qual o mapa da fábula de Borges, que de tão detalhado acaba por ter o tamanho e complexidade igual ao território mapeado. Relacionado a um “ambiente de segurança”, o termo foi criado pelo DoD para lidar com os desafios trazidos pela utilização de tecnologias digitais por “adversários” das forças de segurança dos EUA. O termo sugere uma integração entre os ambientes físicos e digitais, civis e militares e cria uma lógica de legitimação e clamor pela atuação sistemática e permanente das forças de segurança estadunidenses também no ambiente online.

Inspirado por Clastres e sua proposta de antropologia contra o estado, assim como pelos zapatistas - que declaram ter aprendido tudo que sabem sobre guerrilha a partir do estudo dos manuais militares dos EUA e da OTAN, busco olhar para alguns dos mecanismos de operação da inteligência militar no Departamento de Defesa dos EUA, analisando como os manuais militares fazem fazer “segurança”, ou seja, como os manuais participam de uma articulação entre enunciados e ações. São analisados em conjunto narrativas, registros históricos e tecnologias que participam dessa tentativa estadunidense de estabilização de um “ambiente de segurança” e de um “ambiente informacional”, assim como tecnologias e padrões de comportamento das forças de segurança dos EUA, historicamente responsáveis por uma série de violências contra as democracias, os direitos humanos e a justiça social.

palavras-chave: informação; ambiente informacional; ambiente de segurança; military intelligence; departamento de defesa; etnografia documental.

ABSTRACT

The work ethnographically follows how the “informational environment” - a concept used extensively in recent US military manuals - is constituted and operated. Defined in the US Department of Defense (DoD) Dictionary of Military Terms as “the aggregate of individuals, organizations, and systems that collect, process, disseminate, and act on information,” the information environment has the potential to encompass the entire world, just like the map in Borges fable, which is so detailed that it ends up having the same size and complexity as the mapped territory. Related to a “security environment”, the term was created by the DoD to address the challenges posed by the use of digital technologies by “adversaries” of US security forces. The term suggests an integration between physical and digital, civil and military environments and creates a logic of legitimation and clamor for the systematic and permanent action of US security forces also in the online environment.

Inspired by Clastres and his proposal of an anthropology against the state, as well as by the Zapatistas - who claim to have learned everything they know about guerrilla warfare from studying US and NATO military manuals, I seek to look at some of the operating mechanisms of the US Department of Defense military intelligence, analyzing how military manuals do “security”, that is, how manuals participate in an articulation between statements and actions. Narratives, historical records and technologies that participate in this US attempt to stabilize a “security environment” and an “informational environment” are analyzed together, as well as technologies and behavior patterns of US security forces, historically responsible for a series of violence against democracies, human rights and social justice.

keywords: information; information environment; security environment; military intelligence; department of defense; document ethnography.

LISTA DE ILUSTRAÇÕES

Imagem 1 - Excerto de um manual de mecânica automobilística: Como resolver problemas na suspensão, amortecedores e direção do carro Volkswagen Kombi (Fonte: Haynes Guide 1600 VW Transporter).....19
Imagem 2 - Momento de nossa prisão no Centro Cultural São Paulo (Fonte: Acervo Próprio).....30
Imagem 3 - Perfil no aplicativo de relacionamentos Tinder do Capitão Botelho, no qual Botelho se passava por socialista (Fonte: El País).....33
Imagem 4 - Tabela com o "fluxo lógico" sobre operações em ambiente informacional (Fonte: DEPARTMENT OF DEFENSE, 2018, p. xi).....58
Imagem 5 - Modelo de ambiente informacional que, segundo o manual JCOIE, privilegia a ideia de controle das transmissões de informação (Fonte: DEPARTMENT OF DEFENSE, 2018).....68
Imagem 6 - Principais *Information Related Capabilities*, como listadas no *DoD Strategy for Operating in the Information Environment* de 2016 (Fonte: GAO Report).....74
Imagem 7 - Diagrama que ilustra o processo de aplicação de IRCs para obter influência sobre humanos e sistemas (Fonte: *DEPARTMENT OF DEFENSE*, 2012, p. I-7).....80
Imagem 8 - Componentes básicos de uma célula de operações de informação, como proposto no manual *JP 3-13 Information Operations*. Notar as várias IRCs mencionadas.....82
Imagem 9 - Estrutura proposta pelo manual JP 3-13 para a coordenação de OI no caso de operações executadas em contexto interagências (em conjunto com órgãos civis do governo dos EUA) (Fonte: DEPARTMENT OF DEFENSE, 2012, p. II-8).....84
Imagem 10 - Diagrama que detalha etapa por etapa o processo de planejamento e acompanhamento inicial de uma operação de informação no DoD (Fonte: DEPARTMENT OF DEFENSE, 2012, p. IV-3).....85
Imagem 11 - Cartum *School Begins* de Louis Dalrymple, publicado na revista Puck de 25 de janeiro de 1899.....106
Imagem 12 - Diagramas representando um sistema comum (1) e um sistema cibernético (2) (Fonte: elaboração própria).....123
Imagem 13 - O ciclo de inteligência. Notar como cada subsistema recebe como entrada a saída do anterior (Fonte: INTERAGENCY OPSEC SUPPORT STAFF, 2000).....127

LISTA DE ABREVIATURAS E SIGLAS

ABIN: Agência Brasileira de Inteligência

AI: Ambiente Informacional

AMAN: Academia Militar Agulhas Negras

CIA: *Central Intelligence Agency*

C2: *Command and Control*

C2W: *Command and Control Warfare*

CNO: *Computer Network Operations*

CIE: Centro de Inteligência do Exército

DEIC: Departamento de Investigações Criminais

DOPS: Departamento de Ordem Pública e Social

DOI-CODI: Departamento de Operações de Informação - Centro de Operações de Defesa Interna

DOD: *Department of Defense*

DOJ: *Department of Justice*

ESCT: Estudos Sociais da Ciência e da Tecnologia

EW: *Electronic Warfare*

EMSO: *Electro Magnetic Spectrum Operations*

ELN: Exército de Libertação Nacional

EZLN: Exército Zapatista de Libertação Nacional

EPR: Exército Popular Revolucionário

EUA: Estados Unidos da América

ESNI: Escola Superior Nacional de Informações

ESG: Escola Superior de Guerra

EDA: Escola das Américas

FOIA: *Freedom of Information Act*

FARC: Forças Armadas Revolucionárias de Colômbia

FHC: Fernando Henrique Cardoso

FMI: Fundo Monetário Internacional

FM: *Field Manual*

GLO: Garantia da Lei e da Ordem

GSI: Gabinete de Segurança Institucional

IO: *Information Operations*

IE: *Information Environment*

IRC: *Information Related Capabilities*

JCOIE: *Joint Concept for Operating in the Information Environment*

JC: *Joint Concept*

JCS: *Joint Chiefs of Staff*

MILDEC: *Military Deception*

NEP: Novo Exército Popular

NSA: *National Security Agency*

OAB: Ordem dos Advogados do Brasil

OPSEC: *Operational Security*

ORI: Outros requisitos de inteligência

OI: Operações de Informação

PSYOPS: *Psychological Operations*

PRI: Partido Republicano Institucional

RPI: Requisitos prioritários de inteligência

SNI: Serviço Nacional de Informações

SISBIN: Sistema Brasileiro de Inteligência

US: *United States*

SUMÁRIO

INTRODUÇÃO - Informação e controle político-militar na contemporaneidade: a criação de um ambiente informacional…… 15
Manuais militares como material de trabalho……... 17
O encontro etnográfico com manuais militares…… 20
Etnografías de documentos: entre o público e o secreto……...21
Composições material-semióticas e imaginários sociotécnicos……26
Um encontro forçado com a "inteligência": sangrado para dentro do campo…….. 30
Apresentação da dissertação……..34
CAPÍTULO 1 - O inimigo tipo Phineas Fisher e o aparato sociotécnico ambiente informacional……...39
A ciberinimiga……...39
Circunscrevendo o inimigo digital no ambiente informacional……42
Bases militares, embaixadas e fortalezas digitais subterrâneas: a comunidade de inteligência e seus frequentadores civis e militares…….45
A doutrina militar estadunidense e a importância do *Joint Chiefs of Staff* do Departamento de Defesa……48
O Departamento de Defesa……... 51
Command and control e os OODA *loops*: a forma de organização do Departamento de Defesa ……...53
O problema-solução do ambiente informacional…… 57
Ações derivadas do problema-solução que define o ambiente informacional: *Information Related Capabilities*……..……...61
Um ambiente em construção: as ligações entre *information operations* e o *information environment*……...62
CAPÍTULO 2 - *Information related capabilities*: da guerra fria aos anos 90……70
As principais IRCs…… 70
Como utilizar IRCs: O *Information and Influence Framework* (IIF)..... 77
Quem executa operações de informação: a célula de OI…….. 81
Como são planejadas e executadas operações de OI: a coordenação interagências e a imaginação do inimigo como etapas cruciais……85
Antes das operações de informação: operações de influência e as estratégias de deterrência e contrainsurgência…….. 90

A doutrina de contra-insurgência e as operações de influência…… 93
CAPÍTULO 3 - A origem da noção de guerra como um problema cibernético: inteligência, informação e controle durante a primeira metade do século XX nos EUA ……101
A experiência colonial, novas tecnologias e o nascimento da inteligência militar estadunidense…….....……102
A instabilidade da primeira metade do século XX como catalisadora da atividade de inteligência…….. 109
Inimigos informacionais, a análise de sistemas e a cibernética…….…….....115
A nova era das organizações cibernéticas……... 125
CONCLUSÃO…….. 131
REFERÊNCIAS…… 141

INTRODUÇÃO - Informação e controle político-militar na contemporaneidade: a criação de um ambiente informacional

Na primeira semana de setembro de 2016, após dias de intensas manifestações convocadas através do Facebook contra o novo governo de Michel Temer, minha vida se cruzaria com a inteligência do Exército Brasileiro. Conforme apuração da Agência Pública[1] e da Ponte Jornalismo[2], o hoje Major do Exército William Pina Botelho — que, durante pelo menos dois anos (2014-2016), trabalhou como agente infiltrado acompanhando as atividades de movimentos políticos de esquerda na capital do estado de São Paulo — utilizando a identidade falsa de Balta Nunes, compareceu às manifestações dos dias anteriores e se infiltrou em grupos de Whatsapp, Telegram e Facebook, criados pelos manifestantes para organizarem-se durante os atos. Infelizmente, eu era um dos muitos que participavam desses grupos de chat. No dia 4 de setembro, dia em que se pensava que ocorreria a maior das manifestações, foram combinados através dos grupos online diversos pontos de encontro. Dirigi-me a um dos pontos por volta das 14h, uma hora antes do horário marcado para o ato. Ao chegar ao Centro Cultural São Paulo, encontrei-me com outras vinte e uma pessoas, entre as quais eu sabia o nome de cinco, todas conhecidas nos dias anteriores, na rua e na internet. Enquanto nos preparavámos para começar a caminhar em direção ao ato, notamos que estávamos sendo sobrevoados por um helicóptero da polícia. Fomos então encurralados e detidos por quarenta homens e mulheres do Batalhão de Ações Especiais da Polícia Militar de São Paulo, com vestes camufladas cinza e armaduras anti-distúrbio, que pularam as muretas e cercas do local, apontando fuzis e escopetas para nossas cabeças.

Esse encontro equivocado e desastroso com a inteligência militar brasileira foi o acontecimento que me empurrou para uma espécie de "pré-campo", uma porta de entrada para a realização da pesquisa que gestou esta dissertação, cujo tema são as relações entre informação e controle político-militar na contemporaneidade. Como veremos, é impossível falar sobre essas relações sem evocar certas práticas idealizadas e realizadas pelas forças de segurança, partes dos Estados modernos responsáveis pela manutenção da lei e da ordem e, portanto, da estabilidade política. Como recorte deste tema, escolhi estudar o "ambiente informacional" (AI), conceito cunhado pelo Departamento de Defesa dos EUA para pautar

---

[1] Disponível em: https://apublica.org/vigilancia/infiltrados/botelho-o-espiao-que-ninguem-amava/. Acesso em: jul. 2021.

[2] Disponível em: https://ponte.org/infiltrado-do-tinder-que-espionava-manifestantes-e-oficial-do-exercito/. Acesso em: jul. 2021.

sua atuação no presente e futuro próximo. O AI é definido como o agregado de pessoas e sistemas que coletam, processam e disseminam informação. Como veremos, o DoD estipula que sua missão principal neste novo ambiente é a influência sobre comportamentos, crenças e regras que orientam a tomada de decisão de pessoas ou máquinas. Inspirado por minha experiência e por essas intrigantes definições relacionadas ao “ambiente informacional" — que unificam pessoas e máquinas como alvos a serem influenciados — proponho a seguinte questão de pesquisa: como é constituído o conceito de “ambiente informacional” dos militares da inteligência dos EUA? Para perseguir tal questão, realizei uma etnografia que teve como material-base uma série de documentos militares, em especial, manuais.

O trabalho se mostra pertinente, uma vez que o governos dos EUA e suas forças de segurança têm imensa influência na doutrina militar dos países ocidentais, com os procedimentos e formas de organização estadunidenses sendo replicados no interior de cada polícia e força armada de países como Colômbia, México e Brasil. Um trabalho que busca descrever a operação da inteligência militar dos EUA pode servir, por exemplo, para a realização de futuros estudos comparativos entre as operações dos EUA e dos países latinos, ou mesmo futuros projetos de pesquisa que busquem inventariar os equipamentos físicos utilizados para cada uma das atividades de inteligência, associando-os às práticas, de modo que tais análises possam ser utilizadas para conceber políticas públicas destinadas ao monitoramento e à supervisão da atividade de inteligência. Os dados desta dissertação também podem ser utilizados para compor estudos futuros que analisam como se articula geopoliticamente a relação entre militares brasileiros e estadunidenses, assim como as intenções de cada uma das partes dessa relação.

O trabalho demonstra que o processo de profissionalização da atividade de inteligência dentro do aparato militar dos EUA culmina na recente proposta do Departamento de Defesa, a qual visa a instituição de um “ambiente informacional”. Para a “operação em ambiente informacional”, o DoD propõe que todas as unidades militares dominem as atividades de inteligência, denominadas “operações de informação”, tornando-se capazes de, através destas, realizar operações militares para influenciar comportamentos de indivíduos, organizações e sistemas. Tal desenvolvimento marca o ápice da importância e da profissionalização tanto da atividade de inteligência quanto do próprio conceito de informação no interior do aparato de segurança estadunidense. O trabalho também apresenta como resultado o fato de que é necessária uma estrutura gigante, complexa e custosa para a operação das atuais necessidades de inteligência em “ambiente informacional”, o que exige

uma intensa colaboração entre iniciativa privada, militares e governo civil para executar o novo esforço de guerra permanente e informatizado.

Os manuais de doutrina, assim como a teoria de sistemas, a cibernética e a teoria dos jogos são alguns dos instrumentos principais utilizados pelos militares para organizar e operar o dia a dia de suas atividades, ou seja, para continuamente profissionalizarem-se, inclusive de maneira científica. Ainda sobre os manuais, o trabalho também mostrou como esse material atua na formatação dos tipos inimigos a serem combatidos pelos militares, já que as preocupações com as capacidades imaginadas pelos militares como sendo capacidades inimigas são centrais na determinação das técnicas e procedimentos que devem ser criados internamente para que as forças de segurança sejam capazes de combater efetivamente todos os tipos de inimigos previstos. Finalmente, o trabalho também mostra como, pelo menos ao longo do século XX, boa parte das preocupações dos setores de inteligência militar se centraram no combate ferrenho a qualquer iniciativa comunista pelo mundo inteiro, com o comando civil das forças militares compartilhando e fomentando essa convicção anticomunista.

Manuais militares como material de trabalho

O ambiente informacional é definido oficialmente pelo DoD como:

> The information environment is the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information. This environment consists of three interrelated dimensions, which continuously interact with individuals, organizations, and systems. These dimensions are known as physical, informational, and cognitive. The physical dimension is composed of command and control systems, key decision makers, and supporting infrastructure that enable individuals and organizations to create effects. The informational dimension specifies where and how information is collected, processed, stored, disseminated, and protected. The cognitive dimension encompasses the minds of those who transmit, receive, and respond to or act on information. (JOINT CHIEFS OF STAFF, 2012, p. vii)

Para saber mais sobre cada um dos componentes desse ambiente, utilizei como materiais principais de pesquisa os manuais que compõem a doutrina militar para a "operação em ambiente informacional". Também foram utilizadas falas de militares em fóruns públicos de discussão, assim como documentos internos do Departamento de Defesa, tais como diretivas que definem as funções do departamento e documentos de estratégia que delineiam quais devem ser os focos de ação do departamento nos próximos anos. Trabalhos de historiadoras e historiadores militares também foram amplamente utilizados, principalmente

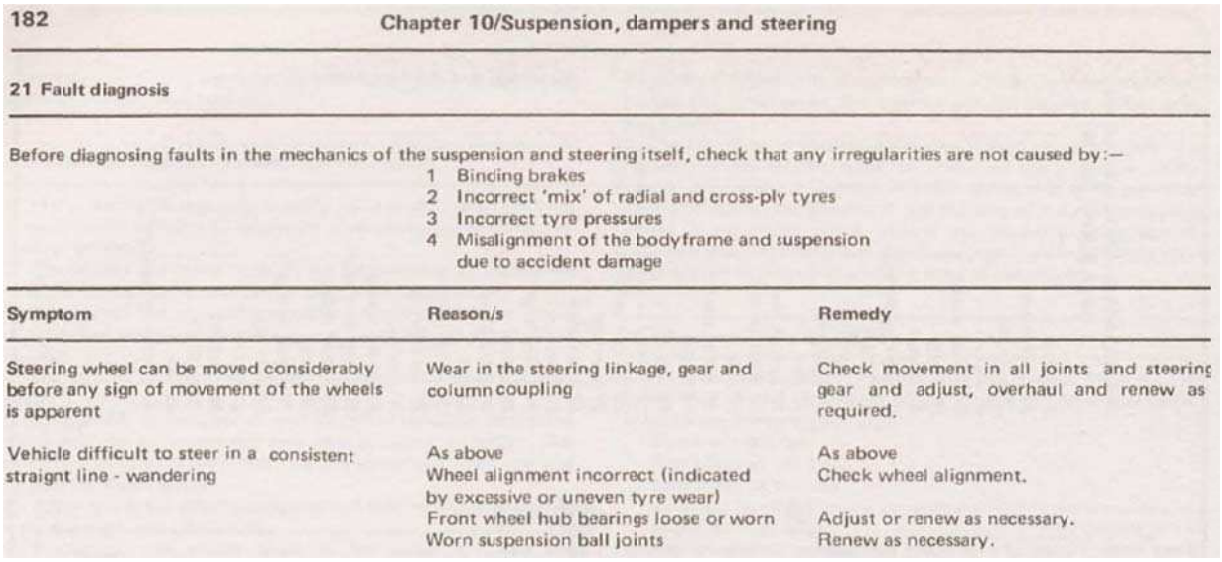
para contextualizar em ações e fatos históricos a utilização de determinados conceitos ou técnicas por parte dos militares estadunidenses.

Manuais, assim como os arquivos e repositórios dos quais fazem parte, são codificações físicas de um *ethos* e de uma *práxis*. É justamente por isso que esses materiais servem à análise antropológica, sociológica e histórica como fontes de pesquisa, de modo que muito pode se descobrir sobre uma organização através dos documentos criados com a intenção de auxiliar o funcionamento dessa própria organização. Esses documentos, que detalham o que se espera do cotidiano de uma determinada função interna, podem ser continuamente consultados — não apenas durante a formação dos membros da organização. Segundo o site da Biblioteca do Congresso dos EUA sobre os manuais do Exército estadunidense:

> Of interest to military historians, curators, military enthusiasts, re-enactors and collectors, army manuals can be used to trace the evolution of the Army's doctrine, organizational structure, equipment, uniforms, and weapons. They are also helpful in terms of the care, maintenance and preservation of military artifacts.
>
> Army manuals include publications on historic U. S. military vehicles, including military motorcycles, jeeps, military trucks, scout cars, tanks, amphibians, and aircraft. Subjects of the manuals also include radio, cooking, language dictionaries and phrase books. (CUFFIA, 2022).

Nesse aspecto, os documentos e manuais analisados se assemelham a manuais técnicos como "guias de serviço"[3] de mecânica automobilística, que contêm instruções sobre como funcionam as partes do veículo e mostram como identificar falhas e como realizar os consertos (Imagem 7). Como nos lembra a descrição citada acima da Biblioteca do Congresso, os manuais associam objetos e palavras às práticas e, nessa condição, servem como guias para a execução de uma atividade complexa, como no caso deste trabalho, a atividade de inteligência.

[3] Do inglês *service manuals*, uma categoria de literatura técnica direcionada a mecânicos.



182 Chapter 10/Suspension, dampers and steering

21 Fault diagnosis

Before diagnosing faults in the mechanics of the suspension and steering itself, check that any irregularities are not caused by:—
1 Binding brakes
2 Incorrect 'mix' of radial and cross-ply tyres
3 Incorrect tyre pressures
4 Misalignment of the bodyframe and suspension due to accident damage

Symptom	Reason/s	Remedy
Steering wheel can be moved considerably before any sign of movement of the wheels is apparent	Wear in the steering linkage, gear and column coupling	Check movement in all joints and steering gear and adjust, overhaul and renew as required.
Vehicle difficult to steer in a consistent straight line - wandering	As above Wheel alignment incorrect (indicated by excessive or uneven tyre wear) Front wheel hub bearings loose or worn Worn suspension ball joints	As above Check wheel alignment. Adjust or renew as necessary. Renew as necessary.

Imagem 1 - Excerto de um manual de mecânica automobilística: Como resolver problemas na suspensão, amortecedores e direção do carro Volkswagen Kombi (Fonte: Haynes Guide 1600 VW Transporter)

Documentos como os manuais militares podem ser analisados para além de seu conteúdo. É possível, por exemplo, se perguntar sobre sua forma, quais as suas esferas de circulação, como eles são criados, armazenados e modificados, a quem se destinam, quando ficam ultrapassados e são abandonados, ou o que acontece quando eles circulam fora de suas esferas previstas de circulação. Neste trabalho, no entanto, foco a atenção no conteúdo e no contexto político dos manuais, buscando entender como esses articulam enunciação e ação[4], assim como um etnógrafo interroga e conversa com um interlocutor humano.

Estruturalmente, os manuais analisados normalmente possuem uma primeira seção que contém um resumo de todo o documento, assim como algumas páginas contendo as justificativas para a existência de tal documento — por exemplo, situando o documento como parte da execução de uma estratégia militar estadunidense de longo prazo, como é o caso da DoD *Strategy for Operating in the Informational Environment,* de 2016. Na primeira seção também encontra-se um sumário com as mudanças realizadas nessa versão específica do documento, assim como que órgão realizou a elaboração do manual. As seções seguintes explicam em detalhes e com abundância de exemplos os principais conceitos apresentados no manual, seguido pela apresentação das autoridades e responsabilidades relacionadas à operacionalização dos conceitos apresentados pelas pessoas e equipes envolvidas, assim como

[4] "To Levy (2001, 23), documents 'are, quite simply, talking things.' Invoking Latour's notion of delegation, Levy continues: 'They are bits of the material world — clay, stone, animal skin, plant fiber, sand — that we've imbued with the ability to speak.'" (HANDBOOK STS AULA MARKO, p. 61)

são nessa etapa levantadas algumas considerações legais relacionadas ao tema do documento. São então apresentados de maneira sistematizada e detalhada os procedimentos burocráticos necessários para a execução oficial da operação, como as formas de avaliar o andamento das atividades, ou as formas específicas de coordenar as ações entre agências diferentes. Finalmente, os manuais têm um glossário e apêndices contendo referências e compilados de regulações internas do departamento e leis pertinentes.

Os principais materiais utilizados nesta dissertação são os manuais oficiais públicos do DoD denominados *JP 3-13 Information Operations* (JP 3-13), e o *Joint Concept for Operating in the Information Environment* (JCOIE). O primeiro teve sua última versão publicada em 2014, e o último foi publicado no ano de 2018. O *Department of Defense Dictionary for Military and Associated Terms* também foi utilizado extensivamente na pesquisa e constitui um dos principais materiais analisados, justamente por ser um glossário oficial de termos utilizados pelo DoD, compilado constantemente pelo próprio DoD. Como a definição dos termos "informação", "inteligência" e "segurança" e a interligação entre eles se alteraram com o tempo dentro desses documentos, foram consultadas várias revisões dos documentos — as mais antigas delas datando dos anos 50. Foram também utilizadas na análise do contexto histórico, historiografias militares, assim como análises de manuais tornados públicos do DoD e da CIA utilizados no período da Guerra Fria.

O encontro etnográfico com manuais militares

Este trabalho é posicionado dentro de uma chave interdisciplinar de análise de políticas científicas e tecnológicas, dialogando com campos como estudos sociais da ciência e da tecnologia, antropologia da ciência e da tecnologia, antropologia da guerra, e também tendo como referências teórico-metodológicas teorias críticas à ciência e à tecnologia propostas por filósofas feministas. Como método de pesquisa, utilizei a etnografia. Dado o caráter técnico dos materiais com os quais trabalhei, a saber, prioritariamente manuais militares, mas também dicionários militares e as implicações tecnocientíficas do termo "informação" — componente básico do meu objeto de pesquisa —, procurei nas etnografias da ciência e da tecnologia um direcionamento.

A partir da década de 1980, o encontro entre estudos sociais da ciência e da tecnologia com a etnografia fez com que a produção de conhecimento no "núcleo duro" da ciência, o laboratório, passasse a ser considerada como fonte de preocupação e análise (MONTEIRO, 2012, p. 139). Concomitantemente, a antropologia passou a se interessar por

temas ligados à ciência e à tecnologia, ampliando o alcance da etnografia no que concerne ao campo onde a produção científica ocorre. Para o antropólogo Marko Monteiro, práticas tecnocientíficas não produzem apenas materialidades, mas também saberes, poderes e significados (2012, p. 147). Sendo assim, a potência da etnografia como método de pesquisa está em permitir uma maior visibilidade das complexas inter-relações entre sistemas sociais e sistemas técnicos, ou seja, relações que são "sociotécnicas".

Monteiro também aponta os possíveis impactos positivos, frutos de etnografias que se preocupam com tal fazer sociotécnico, uma vez que essas etnografias são "formas não só de pensar a realidade, mas também de intervir na construção de novas tecnologias" (2012, p. 148). Para o antropólogo, cada vez mais se firmam no horizonte possibilidades concretas de que cientistas trabalhem junto a etnógrafos da ciência para atuarem como agentes de formulação de políticas públicas sobre ciência e tecnologia. Acredito também que, ao abordar etnograficamente a produção de conhecimento, tecnologias e técnicas[5] militares, possamos avançar no estabelecimento de diálogo e de alianças capazes de gerar transformações importantes e urgentes no modo como o militarismo e a sociedade civil (incluindo nós, cientistas) se relacionam. Afinal, uma das grandes promessas da etnografia sempre foi a de potencializar nossa capacidade de aprender com as diferenças (ROHDEN, MONTEIRO, 2019).

Etnografias de documentos: entre o público e o secreto

> O efeito da narração sobre a ação que ela narra – efeito que passa pela ficção, "pelo falso e pelo verdadeiro, pela história e pelo romance" – é precisamente o enigma que poder-se-ia explorar. (FAYE, 2009, p. 10).

A pesquisa antropológica de instituições, como as militares, apresenta uma série de desafios, a começar por como concretamente é possível se aproximar desses entes. Os documentos figuram como uma porta de entrada muito interessante, como podemos ver nos trabalhos de Richard Harper e Katherine Verdery, antropólogos que estudam organizações sigilosas através de seus documentos. Nesta seção apresentarei brevemente esses trabalhos, além de discorrer sobre a questão do sigilo para a pesquisa etnográfica.

[5] Algumas etnografias clássicas também foram fonte de inspiração, em especial com relação aos modos de descrição das técnicas aprendidas no processo de contato com o "outro". É interessante notar que a tradição antropológica como um todo sempre preocupou-se tanto com o pensamento racional – comparando-o com o pensamento mágico, como no caso de Evans-Pritchard – quanto com a produção e circulação de artefatos técnicos – como no Kula, descrito por Malinowski (ROHDEN, MONTEIRO, 2019, p. 1).

Harper é autor de um estudo sobre o Fundo Monetário Internacional (FMI), que é considerado um marco na etnografia documental (2009). Harper propõe estudar a "carreira" de um documento, a qual seria composta de anotações etnográficas relativas ao ciclo de vida dos documentos, associando os conteúdos, usuários, mídias e reações aos documentos e uns aos outros, e, assim, criando uma teia de relações que seria útil para analisar o que — e como — fazem as organizações. Harper é influenciado pela teoria ator-rede latouriana e sua metodologia se inspira no campo dos Estudos Sociais de Ciência e Tecnologia (ESCT), com destaque para a utilização de Harper do conceito de antropologia simétrica. Através desse conceito, os chamados praticantes do campo de ESCT propõem que a antropologia abandone voluntariamente as grandes divisões natureza-cultura, ciência-política, humano-não humano, primitivo-civilizado, em prol de uma abordagem simétrica que estude de maneira integrada e considere a igualdade de importância das diversas facetas e processos que compõem os problemas sociais. Nessa perspectiva, considerar não humanos como atores, ou seja, como detentores de agência, significa investigar o que esses não humanos fazem fazer.

Através da relação humano-objeto, os documentos são considerados como não humanos que fazem fazer coisas: Harper mostra que, no interior do FMI, as ações e tecnologias previstas de serem tomadas e utilizadas quando um documento chega a seu usuário variam imensamente dependendo da posição e função desse usuário dentro do Fundo. O conjunto das diferentes ações que podem ser tomadas (e das tecnologias que podem ser usadas para executar essas ações) como respostas ao conteúdo de um documento ou à simples presença do documento em um lugar específico, compõem uma parcela significativa do trabalho da organização. Harper retrata metaforicamente o próprio FMI como uma máquina de processamento de informações, tendo os documentos como insumo principal, a energia vital da burocracia. Através da análise dos documentos como objetos centrais, seu estudo permite criar e testar hipóteses sobre como cada setor do FMI entende sua função e missão, e como esses setores interagem uns com os outros e com os atores externos à organização, como os governos dos países que se relacionam com o FMI.

Verdery, antropóloga romena e estadunidense, foca seu trabalho na análise de documentos contidos nos arquivos do aparato de segurança romeno e também investiga o que esses documentos fazem fazer. Nesse aspecto, a autora ressalta que os documentos podem revelar o "trabalho conceitual" por trás deles, ou, em outras palavras, quais epistemologias estão relacionadas com seu uso, confecção e circulação. Assim como outros pesquisadores como Hull (2012), Stoler (2010) e Harper (2009), Verdery (2014) propõe uma análise que crie

uma ponte entre os documentos e as práticas e formas organizacionais. Em seus estudos nos arquivos da antiga polícia secreta comunista *Securitate*, Verdery pergunta para os documentos questões como:

> - Como foram formados os agentes que confeccionaram determinado documento?
> - É possível observar faccionalismos internos na organização através da análise dos documentos?
> - Como mudam com o tempo as relações entre essa organização e as outras com as quais ela interage?
> - Como muda a organização e o organograma interno com o tempo?
> - Há rotatividade de funcionários internamente à organização? Há rotatividade de funcionários entre organizações? Como são os salários e perspectivas de carreiras dos funcionários?
> - Qual o mandato da organização? Esse mandato muda com o tempo?
> - Que tecnologias são utilizadas para a geração dos documentos e que tecnologias são previstas para o entendimento pleno do conteúdo dos documentos?
> - Que efeitos imprevisíveis podem acontecer quando documentos circulam por onde não "deveriam"?

Através dessas questões, a autora cria um contexto que servirá para entender onde a organização se insere e atua. Enquanto são levantadas as respostas para as perguntas acima, a autora foca nas tendências, recorrências e dissonâncias encontradas na análise desses documentos. Verdery analisa os documentos integradamente sob os eixos de conteúdo, forma e efeito, ligando as tecnologias materiais de produção e circulação de documentos — as intenções por trás da própria existência dos materiais e escolhas de tecnologia — às consequências práticas que causam os documentos. Como o trabalho de Verdery é principalmente sobre a utilização de informação pelos aparatos de segurança dos países comunistas do leste europeu e se utiliza dos documentos como insumo básico para uma pesquisa de cunho antropológico sobre o conceito de segurança, ele servirá como referência metodológica principal para este trabalho.

Verdery, assim como Harper faz com o FMI, também descreve o aparato de segurança comunista como uma máquina de processamento de informação, mas, dessa vez, uma máquina responsável por categorizar as pessoas em inimigos ou não. Somente por essa razão haveria a existência dessa instituição e, nesse sentido, portanto, os funcionários e agentes da segurança incorporariam a própria noção de ordem e seriam os responsáveis por excelência por garantir — inclusive preventivamente — que nenhum inimigo atrapalhe a paz do Estado. O trabalho de Verdery descreve que boa parte dos oficiais comunistas têm a sensação de estarem o tempo todo engajados em uma guerra permanente, que envolveria conspirações constantes contra o partido comunista ou contra a visão de sociedade dos oficiais comunistas. Tal sentimento de ansiedade — beirando o medo e o desespero — teria grande impacto na escolha das tecnologias utilizadas pelo aparato de segurança, como computadores, arquivos de papel, escutas telefônicas, gravadores, microfones e chaves criptográficas, escolhidos a fim de manter o maior grau de controle informacional possível sobre os alvos. A ansiedade exibida pela coleta frenética e sem limites de dados acaba gerando vários outros efeitos, como a necessidade do sigilo e da compartimentação de informação como meios de preservar a identidade dos agentes e informantes — criando, entre outras coisas, impunidade para atos ilegais dos informantes e agentes de segurança.

A ansiedade e o medo sentidos pelos agentes, somados à impunidade garantida pelo segredo, também poderia levar o "público" à conclusão que os agentes de segurança são instáveis e não confiáveis. Uma interação desse tipo, entre ansiosos, medrosos e desconfiados, teria tendência a gerar situações de conflito, desentendimento ou mesmo de mais ansiedade e medo. Verdery escreve sobre o leste europeu pré-queda do muro de Berlim, mas muito de sua análise antropológica parece ser pertinente para descrever alguns aspectos das forças de segurança de países "ocidentais", como Brasil, Colômbia, México ou os EUA de 2021. Sem o comunismo autoritário e farsesco que caracterizava parte do pensamento da *Securitate* romena estudada por Verdery, muitos dos comportamentos das forças de segurança ocidentais se assemelham aos dos serviços secretos do bloco comunista da europa oriental: o zelo absoluto pela ordem, com a corporificação da lei e do Estado; a ansiedade e o medo; a utilização da violência política; a obsessão pelo controle dos fluxos de informações; e a manutenção de amplos arquivos de espionagem indiscriminada sobre todos os cidadãos.

Um ponto importante a ser considerado com relação aos documentos que compuseram minha pesquisa — e outras que se propõem a estudar documentos militares e estatais —, é que parte das práticas que analisei são sigilosas e potencialmente ilegais, o que

torna o estudo dos órgãos de inteligência mais trabalhoso. Os aparatos de segurança não divulgam como monitoram adversários políticos ou como é decidido quem é suspeito e quem não é[6]. No entanto, em governos supostamente democráticos, o funcionamento das forças de segurança precisa ter o mínimo de supervisão da sociedade civil e o governo precisa de um nível mínimo de transparência sobre suas operações por uma questão de organização interna. Nos EUA, o Departamento de Defesa publica uma série de resoluções, manuais e diretivas que tem o duplo objetivo de servir como guias para os funcionários do DoD saberem quais são as políticas oficiais do Departamento e também servir para que a sociedade civil saiba como estão organizadas suas forças de segurança. Mesmo nesses documentos "públicos" nem tudo é público e muitos manuais consultados para essa dissertação continham anexos, seções ou documentos complementares secretos.

Para citar dois exemplos: O manual de inteligência da CIA, *Human Resource Exploitation*[7], utilizado no treinamento de forças latino-americanas, fala sobre duas semanas de um treino prático secreto de interrogatório a ser realizado em conjunto no país dos treinados, implicando que haveria, como parte do curso, um treino em que efetivamente os instrutores interrogariam presos ao lado de autoridades latino-americanas. Não é possível saber mais detalhes, somente os envolvidos e seus superiores terão acesso a essa informação. No documento *DoD Manual 5240-01: Procedures for governing the conduct of DoD intelligence activities*[8], que supostamente contém as linhas mestras para a condução de atividades de inteligência em todas as agências e contratados do DoD, é citado um anexo sigiloso (DoD 5240.1-R) que contém provisões que impactam várias seções do documento público, por exemplo, a seção que determina em que casos um estrangeiro pode ser espionado eletronicamente e como.

Por sorte, o estudo do secreto e do sigilo é um desafio comum no fazer antropológico. Evans-Pritchard estava interessado em sociedades secretas entre os Azande do Sudão, organizações subterrâneas e populares entre os jovens plebeus de ambos os sexos que foram desprezadas pelos nobres zande, condenadas por missionários religiosos e proibidas em 1919 pela administração colonial britânica. O antropólogo admitiu a dificuldade em aprender sobre as sociedades secretas, mas, através de conversas e depois de se juntar a uma associação e participar de algumas assembleias, afirmou que não era impossível (GONZÁLEZ, 2012, p.

[6] Os manuais da Escola das Américas são uma exceção, pois falam abertamente sobre o uso de violência para fins políticos e também por que foram tornados públicos após muitos anos de batalhas legais entre o governo dos EUA e grupos de ativistas.
[7] Tornado público em 1997. O trecho citado localiza-se na página B-2.
[8] Versão de agosto de 2016.

22). Além desse exemplo óbvio, podemos pensar o trabalho antropológico permeado pelo segredo de maneira mais geral, uma vez que muitas informações produzidas em conversas, entrevistas e observações participantes são da ordem da confissão, do segredo e da fofoca. Sinto-me, portanto, tranquilo em buscar inspiração na antropologia para lidar com o problema das partes faltantes.

Composições material-semióticas e imaginários sociotécnicos

Somando-se à intenção de, como sugerido pelas etnografias descritas acima, acompanhar o que os manuais "fazem fazer", nas primeiras aproximações com o campo pude perceber alguns atributos que, ao longo da pesquisa, se mostrariam centrais para a observação e análise realizadas. Por um lado, ao folhear digitalmente os manuais, pude apreender a complexidade existente ali, composta de redes de relações que perpassam instituições, equipamentos, pessoas, conceitos, instruções escritas e partes faltantes. Tal mistura mostrou-se cada vez mais interdependente, com cada esfera ou dimensão se constituindo mutuamente na relação com as outras. Por outro lado, chamou-me a atenção o modo pelo qual os manuais estão intrinsecamente associados às dimensões imaginativas da realidade, dependendo disso tanto para delimitar definições conceituais quanto para formular práticas, sendo que tal predisposição à imaginação aparece de modo distribuído entre a complexa rede de relações que emerge a partir da leitura dos manuais. Para trabalhar esses dois aspectos, baseei-me nos conceitos de composições material-semióticas e de imaginário sociotécnico, os quais apresentarei a seguir. Por fim, nesta seção, exponho um comentário teórico-metodológico sobre as implicações dos meus próprios interesses e de minha trajetória no modo como realizei a pesquisa aqui apresentada.

Procurei observar meu objeto — o ambiente informacional — e os materiais aos quais recorri para tatear seus rastros — os manuais que o operacionalizam — a partir da noção de "composições material-semióticas", cunhada pela filósofa da ciência Donna Haraway (1995). Esse termo se refere a uma "entidade desajeitada" e tem como intenção "enfatizar o objeto de conhecimento como um eixo ativo, gerador de significado" (Ibid., p. 40). Desse modo, os objetos científicos considerados enquanto "ator material-semiótico" nunca estariam presentes imediatamente em nossas análises, sendo sempre — e a cada vez — apresentados de formas múltiplas, nunca em uma "determinação final ou única do que pode contar como conhecimento objetivo numa conjuntura histórica específica" (Ibid., p. 40). Além disso, ao

unir os termos “material” e “semiótico” em uma palavra hifenizada, o que Haraway propõe é que consideremos esses dois aspectos como indivisos e mutuamente constituintes.

Durante esta dissertação me deparei com um conjunto de palavras concatenadas em documentos militares. Porém, Haraway nos alerta que palavras não só são palavras, elas são práticas material-semióticas pelas quais tanto objetos da atenção quanto sujeitos do conhecimento são mutuamente constituídos (HARAWAY, 2018, p. 218). Aqui, um ponto de atenção deve ser levantado: o objeto e materiais com os quais lidei têm como objetivos primeiros o controle e a demarcação de fronteiras de pensamento (um conceito) e de ações (estruturas de operações). Ao considerá-los como “composições material-semióticas”, busquei justamente escapar das armadilhas de estabilização do real e atentar às oscilações que emergem “desde dentro” das fronteiras, uma vez que aquilo que estas contêm — de modo sempre provisório — permanece gerativo, “produtor de significados e de corpos” (HARAWAY, 1995, p. 41). As leituras e descrições que realizei foram balizadas pela busca dessa oscilação fronteiriça e da capacidade gerativa do meu objeto e materiais, buscando enfocar como os significados e corpos, as composições e práticas “material-semióticas”, colapsam os domínios técnicos, orgânicos, políticos, econômicos, oníricos/imaginativos e textuais (HARAWAY, 2018, p. 12).

Gostaria agora de abordar o segundo aspecto observado nos manuais, o domínio “onírico/imaginativo” que participa das composições e práticas “material-semióticas”. O termo “imaginários sociotécnicos” é comumente utilizado nos estudos sociais da ciência e da tecnologia para descrever tal domínio, definindo-o como “visões de futuros desejáveis mantidas coletivamente, estabilizadas institucionalmente e publicamente performadas, incentivadas por compreensões compartilhadas de formas de ordem e vida social alcançáveis por e apoiadoras de avanços na ciência e tecnologia” (JASANOFF apud SILVA, 2020). Para que tais visões de futuro sejam configuradas, tanto presente quanto passado são acionados através dos imaginários sociotécnicos, que servem como lentes para interpretar e produzir fenômenos. Assim, horizontes de possibilidades são estabelecidos através da criação e adoção de tecnologias, mas também através de inspirações e retroalimentações estéticas, afetivas e sociais (SILVA, 2020).

Através dessa definição de “imaginário sociotécnico” podemos afirmar a condição constituinte de tal domínio da realidade para a produção da inovação, ou seja, para a criação e acomodação de novas tecnologias e técnicas. Porém, em sua etnografia junto a cientistas e engenheiros, Marisol Marini demonstra como tal dimensão imaginativa muitas vezes é

completamente suprimida dos registros da produção científica e tecnológica (2021, p. 2). A antropóloga pesquisou, junto a uma rede de dispositivos de assistência circulatória, uma tecnologia conhecida como “corações artificiais”, cujo propósito é diminuir o alto índice de mortes em decorrência da insuficiência cardíaca. Ao acompanhar a produção de tal tecnologia, Marini notou que, durante a prática de pesquisa dos cientistas e engenheiros, emergiram diversas situações nas quais imaginavam-se corpos “sem corações”. Tal “esforço imaginativo projetivo” estava atrelado a um engajamento material e também a negociações entre diversos atores e entidades (MARINI, 2021, p. 3).

Para Marini, o processo criativo está inscrito no fazer manual, caracterizando-se como uma imaginação corporificada e distribuída entre diversos atores. Imaginários sociotécnicos estão, desse modo, diretamente atrelados às práticas, não sendo uma atividade puramente mental ou cognitiva nos termos comumente empregados — os quais restringem tal processo ao cérebro —, mas, sim, referidos a uma cognição expandida que “se mistura despudoradamente com o corpo e o mundo na conduta de suas operações” (MARINI, 2021, p. 11). No caso de Marini, que pôde acompanhar uma "ciência em ação", as ocorrências e campo analisadas que trouxeram um vislumbre dos imaginários sociotécnicos em práticas corporificadas foram imprevistos, e intercorrências e atuações acidentais compuseram os experimentos e as produções de protótipos. Tal situação é impossível no caso da minha pesquisa, uma vez que os manuais que compuseram meu trabalho de campo são a consolidação material de uma “ciência [militar] em ação”, ou seja, acompanhar etnograficamente o momento exato de sua produção já não é mais possível, nem acredito que seria, dada a impenetrabilidade que as instituições militares se auto-impõem.

Porém, foi importante para a análise levar em conta tal associação entre imaginário e práticas corporificadas destacada por Marini, uma vez que os manuais são, em última instância, uma tentativa de controle de práticas corporificadas, muitas vezes realizadas com as mãos (“manuais”), executadas por pessoas associadas a instituições militares, civis, acadêmicas e empresariais. Olhar para tais práticas codificadas em manuais é, portanto, olhar para o caráter imaginativo oculto nesses aparatos técnicos. E, como veremos, é possível desdobrar esse caráter imaginativo em múltiplas dimensões, por exemplo: as imaginações que foram necessárias para formalizar o conteúdo do manual, em especial, a imaginação de uma entidade chamada “inimigo”; as imaginações difusas que são necessárias para executar as operações descritas no manual; o horizonte de possibilidades imediato, ou seja, o futuro imaginário que a execução de tais operações acarreta; o imaginário sociotécnico necessário

para a criação de um “ambiente informacional”. Procurei descrever, ao longo dos capítulos, as práticas implícitas nos manuais, tendo como pano de fundo a ligação entre essas e os imaginários sociotécnicos, que foram, na medida do possível, melhor delimitadas na conclusão.

Por fim, gostaria de destacar que a descrição que realizo, fruto da observação etnográfica, não se pretende de forma alguma ser neutra: é uma descrição densa e crítica, que carrega consigo as marcas do meu próprio modo de habitar o mundo. Dessa forma, procurei ancorar tal descrição em um “saber localizado”, ou seja, a partir de uma “objetividade corporificada” capaz de estabelecer uma relação com meu objeto de pesquisa que não colapse nem obscureça os princípios políticos, éticos e epistemológicos aos quais me vinculo (HARAWAY, 1995). Esta etnografia é a expressão de um encontro estranhado com militares da inteligência dos EUA. As afetações que foram produzidas durante esse encontro são marcadas pelas histórias que nós dois carregamos. Apresentarei a minha história de forma resumida na próxima seção, quando narrarei como se deu minha entrada — forçada — em uma espécie de “pré-campo” que me levou a conduzir esta pesquisa. Já a história deles, o coração desta dissertação, será apresentada a partir de uma objetividade corporificada ao longo de todo o texto.

Um encontro forçado com a "inteligência": sangrado para dentro do campo

Imagem 2 - Momento de nossa prisão no Centro Cultural São Paulo (Fonte: Acervo Próprio).

Resumindo a longa história que se segue ao momento de minha prisão, vinte e um de nós fomos presos e levados ao Departamento de Investigações Criminais (DEIC) — antigo Departamento de Ordem Pública e Social (DOPS), um dos principais órgãos de tortura durante o regime político anterior brasileiro. Ficamos presos lá por um dia, sem acesso a advogados e sem nenhuma acusação formal. Um dos presos foi separado dos outros durante nosso translado em um ônibus da polícia até o DEIC: o já mencionado Capitão do Exército William Pina Botelho, identificado posteriormente através dos esforços do site *Ponte Jornalismo* e do jornal *El País*[9]. Através das informações obtidas ao se infiltrar com sua identidade de esquerda, "Balta Nunes", nos grupos de comunicação criados nas manifestações dos dias anteriores, William Pina, o comando do Exército e a polícia — cooperando no momento por meio de uma Operação de Garantia da Lei e da Ordem[10] — acreditavam ter

[9] Disponível em: https://brasil.elpais.com/brasil/2016/09/09/politica/1473452777_631937.html. Acesso em: jul. 2021.

[10] Segundo o site do Ministério da Defesa: "Realizadas exclusivamente por ordem expressa da Presidência da República, as missões de Garantia da Lei e da Ordem (GLO) ocorrem nos casos em que há o esgotamento das forças tradicionais de segurança pública, em graves situações de perturbação da ordem. Reguladas pela Constituição Federal, em seu artigo 142, pela Lei Complementar 97, de 1999, e pelo Decreto 3897, de 2001, as operações de GLO concedem provisoriamente aos militares a faculdade de atuar com poder de polícia até o restabelecimento da normalidade. Nessas ações, as Forças Armadas agem de forma episódica, em área restrita e por tempo limitado, com o objetivo de preservar a ordem pública, a integridade da população e garantir o funcionamento regular das instituições." Disponível em: https://www.gov.br/defesa/pt-br/assuntos/exercicios-e-operacoes/garantia-da-lei-e-da-ordem. Acesso em: jul. 2021.

pego os líderes dos black blocs, supostamente os responsáveis pelos confrontos com a polícia nos atos dos dias anteriores.

Do lado de fora do DEIC, minha companheira Clarissa foi a primeira a chegar à vigília de familiares que se seguiria pela madrugada. Ao perguntar sobre nós na portaria fechada, dois policiais perguntam se Clarissa já havia assistido àquele filme em que terroristas escondem uma bomba na cidade e os policiais são obrigados a torturar os terroristas para obterem a localização da bomba. Depois dizem a ela que nós estávamos bem, mas que não sairíamos do jeito que entramos. Passam-se alguns minutos e Clarissa recebe no celular uma requisição de amizade no Facebook de um sujeito chamado Balta Nunes. Balta manda mensagens para Clarissa, falando que na esquerda não havia mulheres bonitas como ela e a chama para tomar uma cerveja.

Após intervenção do ex-senador Eduardo Suplicy, do ouvidor civil das polícias Júlio César Fernandes Neves, do deputado Paulo Teixeira e do vereador Nabil Bonduki, pudemos ter acesso a advogados e fomos então acusados de formação de quadrilha com intenção de no futuro cometer depredações e enfrentar a polícia. Como a maioria de nós não se conhecia e não havia conosco nada ilegal nem perigoso, essa argumentação não se sustentou e, durante audiência de custódia no dia seguinte, todos tivemos a prisão relaxada. Isso não impediu o DEIC de conduzir um inquérito policial sobre o caso, o que resultou em uma denúncia do Ministério Público e uma série de julgamentos na primeira instância, segunda instância, Justiça Militar e Conselho Nacional do Ministério Público. Durante esse processo descobrimos que a Operação de Garantia da Lei e da Ordem (GLO) foi decretada pelo presidente Michel Temer e assinada por ele, pelo ministro da justiça Alexandre de Moraes e pelo ministro do Gabinete de Segurança Institucional (GSI), General Sérgio Etchegoyen[11]. Tal GLO teria como pretexto garantir a segurança da passagem da tocha paralímpica por São Paulo e serviria de escudo legal para o Exército infiltrar o Capitão Botelho nos nossos grupos de WhatsApp.

Durante meses fui monitorado pela polícia após esse episódio. Nosso julgamento envolveu mobilização intensa de movimentos sociais e resultou em absolvição em primeira e segunda instância[12]. Nem o Exército nem a Polícia Militar apresentaram qualquer prova que pudesse nos ligar a atos de violência ou ao planejamento de tais atos. A infiltração ocorrera

[11] A família Etchegoyen é uma das mais tradicionais famílias militares do Brasil. Os membros atuais são ácidos críticos das Comissões da Verdade. O tio e o pai do General Sergio Etchegoyen aparecem na lista de torturadores e facilitadores da tortura.

[12] O promotor do MP-SP recorreu da decisão da absolvição em primeira instância.

sem a autorização da Justiça, ainda que sob o manto da GLO, complicando as forças de segurança que, diante da própria ação ilegal, negaram que as informações coletadas nos grupos de chat online teriam sido usadas em nossa prisão. Além disso, negaram a própria infiltração do Capitão Botelho, que foi transferido de São Paulo para Manaus. Sabemos, no entanto, que não havia outra forma de termos sido presos que não tivesse envolvido a infiltração do agente Botelho nesses grupos de chat. No passado, e talvez ainda no presente, a "comunidade de informações"[13] denominava "sangrar" a interceptação de comunicações. Fomos "sangrados", mas dessa vez não através de nossas linhas telefônicas, como era costumeiro durante o regime militar, mas pelos nossos canais de comunicação digitais.

A investigação do jornal *El País* revelou que Botelho é autor de artigos acadêmicos sobre inteligência, coleta de informações e terrorismo, sendo lotado no Centro de Inteligência do Exército. Botelho vivia em um apartamento na Av. Brigadeiro Luiz Antonio, cedido a ele pessoalmente por um general chamado Manoel Morata. Morata, influente em sua carreira no setor de informações e então presidente do Círculo Militar, quando capitão, durante as décadas de 70 e 80, trabalhou no antigo Destacamento de Operações de Informação — Centro de Operações de Defesa Interna (DOI-CODI), órgão ligado ao Exército, famoso por seu patrono Brilhante Ustra e responsável à época por monitorar os subversivos, principalmente o crescente movimento sindical e o nascente Partido dos Trabalhadores (GODOY, 2015). Do repertório da repressão também foi sacado outro modus operandi de Botelho em nosso encontro: descobrimos, após investigação minuciosa e análise de mensagens trocadas por meio dos aplicativos, que o Capitão sistematicamente assediava as garotas dos movimentos monitorados por eles, como no caso das mensagens recebidas por Clarissa do lado de fora do DEIC. Botelho mantinha um perfil no aplicativo de relacionamentos Tinder com o nome de Balta Nunes, onde se passava por socialista. São vários os casos documentados da utilização por Botelho dessa combinação de monitoramento

[13] "Comunidade de informações", ou "comunidade de informações e segurança" era o nome dado ao conjunto de pessoas, grupos e instituições que formavam o aparato de repressão e espionagem política durante o regime militar: "A comunidade contava com os serviços secretos das três Forças — Exército (CIE), Marinha (CENIMAR), Aeronáutica (CISA) —, o SNI, uma parte da Polícia Federal, a Comissão Geral de Investigações (CGI), as Divisões de Segurança que estavam presentes em todos os Ministérios – DSI, ASI, as delegacias estaduais de Ordem Política e Social (DOPS), as segundas seções das unidades militares e, finalmente, com os serviços de informações das polícias militares. (...) A própria expressão – "comunidade de informações", remete ao auxílio mútuo entre os integrantes da comunidade, que deveriam incorporar um sentimento de lealdade, colaboração e corporativismo. (...) Havia [também] a possibilidade de qualquer pessoa, mesmo de fora do governo, de integrar as "Comunidades Complementares de Informações". (ANDRADE, 2014, p. 65).

político e assédio de cunho sexual. No jargão da comunidade de informações, essa técnica também tem nome: “paquera”.

Imagem 3 - Perfil no aplicativo de relacionamentos Tinder do Capitão Botelho, no qual Botelho se passava por socialista (Fonte: El País)

Comecei minha busca pesquisando então sobre como os militares realizavam operações como a que fui vítima, envolvendo um agente disfarçado monitorando grupos de chat online. Essa busca sobre a relação entre atividade de inteligência e informação digital me levou a uma imersão na literatura sobre essas seções do aparato militar, caracterizadas como “fazedoras oficiais de inimigos”, ou seja, como órgãos responsáveis pela identificação e monitoramento de potenciais adversários do Estado. O entrelaçamento entre tecnologias digitais e política que a espionagem cibernética traz à tona me fascinou, levando-me a me debruçar sobre os modos como os órgãos de inteligência produzem internamente seus adversários.

Apresentação da dissertação

Esta dissertação segue um caminho não linear que parte de meu encontro com o setor de inteligência do Exército Brasileiro, fato que despertou em mim uma paranoia e uma curiosidade intensa sobre o funcionamento desse tipo de órgão. A imersão no campo me levou então à trajetória que sigo neste trabalho: a curiosidade sobre o "ambiente informacional", sobre a ciberespionagem, em geral, e sobre quais preocupações rondam a mente dos militares estadunidenses de inteligência, levou-me ao conceito de "operações de informação" — tipos de operação definidas pela doutrina militar dos EUA como operações militares baseadas no conceito de informação. Após entender um pouco mais sobre essas operações, senti a necessidade de entender ainda mais sobre as origens históricas da própria relação entre militares e informação, que, como veremos, é uma relação estreita e cada vez mais forte ao longo dos séculos XX e XXI. Durante toda a dissertação, realizei uma descrição analítica dos documentos que compõem meus materiais de pesquisa, tentando ao máximo utilizar os termos nativos para explicar cada conceito e relação, e inserindo esses termos em análises políticas sobre as suas condições — materiais e conceituais — de existência.

Uma vez que minha vida, assim como a de meus amigos e familiares, foi afetada por preocupações práticas e técnicas ligadas à inteligência militar, inclusive muitas delas convergentes com as descritas neste trabalho, decidi que enfrentaria tais preocupações. Esta dissertação consiste em uma pesquisa acadêmica que não se refere somente à situação vivida por mim, mas a outras que já aconteceram e acontecem com tantos de nós: este trabalho é um contra-inventário de palavras, um contra-thesaurus, destinado a funcionar como um manual para a leitura dos manuais para aqueles que desejam reagir e aprender a lutar. Tentei criar um guia, parcial e localizado — a partir de minha experiência —, para o modo de pensar e agir dos setores de inteligência, mostrando casos concretos de sua atuação, a fim de abrir possibilidades para estudos futuros destinados à contenção legal e extralegal das atividades desses órgãos e de seus comandantes civis, tão responsáveis pelas barbaridades históricas como os próprios militares.

Esta dissertação está dividida em três capítulos, sendo eles: capítulo 1 - O inimigo tipo Phineas Fisher e o ambiente informacional; capítulo 2 - *Information Related Capabilities*: da guerra fria aos anos 90; e capítulo 3 - A origem da noção de guerra como um problema cibernético: inteligência, informação e controle durante a primeira metade do século XX nos EUA.

No primeiro capítulo sigo a minha trajetória de pesquisa, me aproximando do conceito de "ambiente informacional" e desenredando-o a partir de alguns fios. No início deste percurso, me deparo com as lógicas de funcionamento do Departamento de Defesa e da doutrina militar, que ecoam por toda a chamada Comunidade de Inteligência. Após uma breve descrição de quem são e como vivem os militares e trabalhadores civis que compõem o DoD e a CI, exponho como, nos últimos anos, o Departamento de Defesa dos EUA busca institucionalizar a ciberespionagem como uma das atividades básicas a serem realizadas pelas forças de segurança estadunidenses no contexto do que eles chamam de "ambiente informacional", definido no manual *Joint Concept for Operating in the Informational Environment* (JCOIE). Para o DoD, o AI é definido como o agregado de indivíduos, organizações e sistemas que processam informação e é composto por três dimensões interconectadas: cognitiva, física e informacional. O aumento vertiginoso da importância da informação e das tecnologias da informação no decorrer dos anos 90 faz com que o AI transcenda e determine o curso do chamado "ambiente de segurança" — conjunto de possibilidades e ações que podem afetar os interesses nacionais e a política externa dos EUA. Novas ameaças, principalmente provenientes de movimentos que buscam contestar as normas internacionais ou desafiar o status quo político, levam o DoD a preconizar a criação em todas as suas unidades militares de capacidades relacionadas a operações militares, baseadas, por sua vez, em informação — as chamadas *Information-Related Capabilities* (IRCs) —, de modo que essas unidades possam responder efetivamente às condições contemporâneas decorrentes da instituição de um "ambiente informacional". Neste momento, realizei uma discussão baseada em termos nativos do modelo teórico-epistemológico por trás do AI. Na parte final do capítulo, traço, através das versões antigas de manuais e de fontes históricas oficiais, uma genealogia do termo AI. Tal genealogia indica que para o DoD as "operações em ambiente informacional" seriam o que anteriormente eram as chamadas "operações de informação", tipo de operação realizada há décadas pelos militares estadunidenses, desenvolvida e consolidada em manuais desde meados dos anos 90.

No capítulo 2, através da análise descritiva do manual de doutrina *JP 3-13 Information Operations,* emitido pelo *Joint Chiefs of Staff* do Departamento de Defesa, o trabalho explora quais são as principais *Information-Related Capabilities* (IRCs) — ações associadas à execução de fato das OI — e como elas são integradas através do *Information Influence Framework* (IIF) com a finalidade de alterar "comportamentos", "crenças" e "regras" de indivíduos, organizações e sistemas, objetivo de toda operação de informação.

Tais tipos de suboperações que compõem as OI são, por exemplo, as “operações psicológicas”, a “enganação militar”, as “operações no ciberespaço”, as “operações em espectro eletromagnético” e as “relações civis militares”, que são utilizadas integradamente de modo a realizarem operações ofensivas de “projeção de informação” e/ou defensivas, visando a “proteção de informação”. Após compilar as definições das principais IRCs e descrever o IIF, o trabalho descreve como a doutrina prevê a formação da “célula de OI” — formada por profissionais versados em cada uma das IRCs, assim como representantes de empresas e do governo civil — como unidade básica para a execução de uma operação de informação. Segui, então, o processo de concepção de uma operação de informação no DoD, acompanhando cada um dos passos burocráticos necessários, desde a requisição da operação por autoridade civil ou militar superior, até o planejamento da operação e sua execução, passando também por uma descrição breve de como é avaliado o sucesso ou falha de uma operação de informação. Nas seções finais do capítulo, busquei entender os antecedentes históricos das operações de informação, sendo remetido à estratégia de deterrência e aos teóricos da coerção no contexto da Guerra Fria e às operações de influência e contra-insurgência realizadas pelo Departamento de Defesa e pela CIA entre os anos 60 e 90, no Vietnã, e por toda a América Latina, incluindo o Brasil.

O capítulo 3 trata de uma genealogia da inteligência militar estadunidense, complementando a contextualização sobre os tipos de preocupações, atividades e técnicas historicamente associados à comunidade de inteligência. Segui os primeiros passos da atividade de inteligência no Departamento de Guerra (antecessor do Departamento de Defesa), desde a instituição da primeira seção dedicada à coleta de “informações militares”, em 1889, passando pela experiência colonial dos EUA nas Filipinas e pela Guerra de Fronteiras EUA-México como experiências pioneiras e inovadoras relacionadas à atividade de inteligência. Nessas experiências foram utilizados pela primeira vez interceptações de rádio e telégrafos, agentes informantes, veículos automotores, aviões e câmeras aéreas, assim como computadores. Em seguida, descrevi como a experiência dos EUA na Primeira Guerra Mundial consolida a atividade de inteligência como uma das principais atividades realizadas pelas forças militares, tanto devido às necessidades de inteligência da frente de batalha europeia quanto devido às necessidades no front interno, com os EUA imersos em intensa agitação política sindical e racial — principalmente de orientação esquerdista — o que aterroriza a classe política e engaja a comunidade de inteligência em uma extensa caçada aos indivíduos e grupos contestadores da ordem. A experiência dos EUA na Segunda Guerra

Mundial consolida a já estreita aliança Estado-Mercado-Ciência, colocando o governo dos EUA e o Departamento de Guerra como principais coordenadores de um esforço científico e industrial. Esse esforço resultou na geração de tecnologias que seriam essenciais para o modo de vida contemporâneo, como as tecnologias digitais, os radares e sonares, assim como a teoria cibernética e de sistemas, que teriam imensa influência na organização do aparato de segurança estadunidense no período da Guerra Fria, marcado pela computadorização e cibernetização da organização e da operação do Departamento de Defesa e da comunidade de inteligência sob Robert McNamara.

Na conclusão, discorro sobre algumas das minhas percepções e surpresas que prevaleceram ao final do trabalho. Em primeiro lugar, abordo a relação de alteridade que acabei criando com meus interlocutores militares, o que me fez, por exemplo, parar de imaginar a totalidade da instituição militar como formada por pessoas "pouco inteligentes", "ignorantes" ou "brutas", como pensava de modo preconceituoso ao início do trabalho. O trabalho revela um raciocínio epistemológico complexo por trás do conceito de "ambiente informacional" e das "operações de informação". Esse raciocínio, porém, em nenhum momento reivindica um mundo melhor, ou mesmo a paz, para fundamentar a arbitrariedade do aparato de segurança, o que acende uma luz vermelha nas ciências sociais, já que os militares utilizam-se de conceitos muito semelhantes aos conceitos, por exemplo, de dissolução sujeito-objeto ou de não separação entre humanos e não-humanos, assim como teorias da ciência política embasam, por exemplo, a ideia de "coerção" ou de "uso gradual da força" utilizada pelos militares. Tal situação clama pela inclusão do "saber localizado" no fazer científico como forma de aumentar o exercício da responsabilidade na ciência e na academia.

Outra conclusão importante da pesquisa se relaciona a como a homogeneização da linguagem e os manuais atuam como instrumentos simultaneamente destinados a formatar uma comunidade (no caso, os militares e a comunidade de inteligência); a auxiliar na operação do dia a dia dos aparatos militares (como repositórios de lógicas, termos e relações que podem e são consultados de maneira constante); e a atuar na cristalização do processo de profissionalização da própria atividade militar. Nesse sentido, a pesquisa mostra a importância de um órgão como o *Joint Chiefs of Staff* do Departamento de Defesa, que atua de modo a materialmente garantir a sobrevivência e a continuidade do próprio aparato militar estadunidense como instituição ligada a uma comunidade. A interação histórica entre o Departamento de Defesa, a ideia de informação e as tecnologias de informação também

evidencia que essas últimas tiveram papel fundamental no processo de profissionalização da atividade militar ao longo dos séculos XX e XXI.

Outro resultado da análise que também rompeu alguns de meus preconceitos se relaciona com o fato de que os militares nunca atuam sozinhos. Nas situações analisadas neste trabalho, verificou-se que quase sempre foi necessária uma cooperação intensa entre o poder civil e os militares, além da indústria e da academia, para a realização dos diversos atos horrendos que as forças militares dos EUA protagonizaram nos últimos cem anos, como nos casos das Filipinas, Vietnã e América Latina, ou mesmo no caso das operações de informação da atualidade, que burocraticamente precisam de múltiplas aprovações e interações com o poder civil.

Por fim, a última conclusão que o trabalho apresenta se relaciona com o imaginário sociotécnico por trás da formatação da contemporânea figura de inimigo do DoD. Tal inimigo constitui-se como um inimigo complexo e múltiplo, contestador da ordem e do status quo político, versado em todas as tecnologias de última geração e anonimizado pela ação da internet, podendo inclusive hoje ser um aliado. Tal configuração de inimigo estimula um sentimento de paranoia permanente que fomenta o Departamento de Defesa e a comunidade de inteligência a cada vez mais aumentarem seus escopos de ação e suas capacidades tecnológicas. Nesse sentido, o “ambiente informacional” faz parte de uma ecologia caótica que caracteriza o modo de vida dos funcionários da inteligência militar.

CAPÍTULO 1 - O inimigo tipo Phineas Fisher e o aparato sociotécnico ambiente informacional

Neste capítulo apresento com mais detalhes o conceito de ambiente informacional, apresentando antes uma breve descrição das principais preocupações dos militares relacionadas à informação. Também são explicitados os principais atores deste trabalho, os militares estadunidenses e sua "comunidade de inteligência", assim como algumas de suas principais instituições — o Departamento de Defesa dos EUA e o *Joint Chiefs of Staff* — e formas de organização. Tais formas de organização envolvem, por exemplo, a utilização de manuais de doutrina, assim como de conceitos ligados à teoria de sistemas e a cibernética como orientadores da operação do dia a dia das forças de segurança estadunidenses. O final do capítulo discute o modelo conceitual por trás da ideia de ambiente informacional e explora as relações históricas entre ambiente informacional e as chamadas operações de informação, operações militares realizadas pelas forças militares dos EUA que visam influenciar o comportamento de pessoas, organizações e sistemas.

A ciberinimiga

> *Ésta es mi palabra sencilla que busca tocar el corazón de la gente simple y humilde, pero también digna y rebelde. Ésta es mi palabra sencilla para contar de mis hackeos, y para invitar a otras personas a que hackeen con alegre rebeldía.*
>
> *Hackeé un banco. Lo hice para dar una inyección de liquidez, pero esta vez desde abajo y a la gente simple y humilde que resiste y se rebela contra las injusticias en todo el mundo.*
>
> *Pero no fui yo sola quien lo hizo. El movimiento del software libre, la comunidad del powershell ofensivo, el proyecto metasploit y la comunidad hacker en general son las que posibilitaron este hackeo. La comunidad de exploit, in hizo posible convertir la intrusión en las computadoras de un banco en efectivo y bitcoin. Los proyectos Tor, Qubes y Whonix, junto a las y los criptógrafos y activistas que defienden la privacidad y el anonimato, son mis nahuales, es decir, mis protectores [1]. Me acompañan cada noche y hacen posible que siga en libertad.*

Assim a hacker Phineas Fisher nos convida a adentrar seu "Guia *Do-it-Yourself* para roubar bancos", um manual detalhado sobre os modos de pensar e agir utilizados por ela para roubar o Banco Nacional das Ilhas Cayman, em 2019[14]. Após justificar sua ação "Robin Hood" cibernética como uma "injeção de liquidez vinda de baixo e destinada à gente humilde e rebelde" e afirmar que sua força se encontra no movimento do software livre e no

[14] O manual foi publicado de maneira anônima no site Pastebin (https://pastebin.com/), utilizado frequentemente por hackers para a publicação de comunicados e de dados vazados.

movimento *cypherpunk*[15], Phineas nos apresenta nas seções seguintes seus motivos políticos para a realização das "expropriações", assim como uma metodologia relativamente precisa para a execução de um roubo como o realizado por ela. O guia é ao mesmo tempo passo a passo e panfleto de propaganda e tem o objetivo expresso de se constituir não só como um manual técnico de expropriação, mas também como um guia ideológico do porquê realizar tal ato.

Phineas argumenta que, para aqueles que rejeitam o sistema capitalista e acreditam que a riqueza das classes altas foi fruto de roubo do esforço vital dos trabalhadores, o roubo online de bancos constitui uma alternativa viável para o financiamento da revolta contra o capitalismo e dos novos modos de vida anticapitalistas. Phineas estimula suas leitoras a conhecerem os livros que influenciaram sua visão de mundo, escritos principalmente por autoras e autores anarquistas e decoloniais como bell hooks, David Bollier, Noam Chomsky, Ocalan Abdullah, Silvia Federici, Howard Zinn e Eduardo Galeano.

A segunda parte do texto versa sobre o método técnico utilizado por Phineas para o roubo. Phineas apresenta os novíssimos softwares Tor, Qubes e Whonix, utilizados para garantir a anonimidade total no processo de hacking. Através dessas ferramentas, cada pacote de informação que caracteriza o tráfego de internet proveniente do computador do hacker será criptografado e embaralhado com o tráfego de outros milhares de usuários, passando por vinte ou trinta países aleatórios antes de chegar ao destino real — fazendo com que uma investigação judicial e/ou policial sobre determinada atividade online seja muito difícil, já que essa envolveria dezenas de infraestruturas privadas de internet e jurisdições legais diferentes. Em seguida (após a configuração de uma máquina de trabalho anonimizada para a aspirante à hacker), Phineas apresenta a ferramenta Metasploit, que consiste num banco de dados open-source, listando bugs[16] e vulnerabilidades em todo o tipo de software comercial. Nesse repositório alguns bugs contém malwares[17] associados e prontos para serem rodados contra um alvo — os chamados exploits — e outros bugs são apenas descritos teoricamente. O que Phineas sugere fazer é escolher algum produto de software muito utilizado no sistema

[15] O movimento cypherpunk se baseia na rebeldia punk transplantada para o ambiente da internet. Alguns famosos cypherpunks são Julian Assange, Jacob Appelbaum, Edward Snowden e Chelsea Manning (ASSANGE *et al.*, 2012)

[16] Bugs são erros e falhas em código computacionais.

[17] Malwares são softwares maliciosos criados para serem capazes de dar ao hacker a possibilidade do controle remoto do computador da vítima.

bancário, como o firewall corporativo SonicWall[18], da Dell. Checa-se, então, se existem bugs novos reportados pela comunidade nesse software.

Como sempre existem novos bugs, basta escolher um e, utilizando o conhecimento disponível a um programador experiente, criar seu próprio exploit que utilize o bug escolhido como uma porta de entrada não autorizada para a injeção de código malicioso no computador do inimigo. Em seguida, Phineas utiliza o software Zmap — utilizado para escanear rapidamente todos os endereços de Internet existentes, em busca de certas características em seus servidores — para buscar servidores que usem o SonicWall e que contenham a palavra "banco" na assinaturas de seus certificados digitais de segurança HTTPS[19]. Nesse ponto, obtém-se uma lista de alvos, provavelmente bancos, que rodam SonicWall e que seriam imediatamente passíveis de ser invadidos pelo código preparado para o hacking. O código utilizado por Phineas para burlar o SonicWall e entrar no Banco Nacional das Ilhas Cayman tem cerca de trinta linhas[20] e também é publicado no manual como exemplo.

Uma vez invadido o sistema do banco, a hacker monta (utilizando uma ferramenta interna do Windows, a chamada "linha de comando"[21]) um sistema de espionagem que monitora o trabalho de várias seções do banco, até que, depois de vários anos de monitoramento, Phineas consegue obter as credenciais necessárias para a realização de remessas internacionais e, assim, inicia uma operação consistente na remessa de pequenas quantias para si, no meio de fluxos maiores de operações bancárias internacionais. Segundo a autora do guia, sua operação de expropriação só acabou, pois, durante uma das transferências, ela cometeu um erro burocrático, alertando os responsáveis pela área internacional do banco.

Na seção final do texto, Phineas dá instruções sobre como utilizar contas off-shore para distribuir o dinheiro roubado, de modo a dificultar a sua recuperação por governos; dá detalhes do funcionamento do sistema internacional de transações bancárias SWIFT; e, por fim, oferece seu e-mail e diz que está disposta a ajudar financeiramente outras pessoas interessadas em realizar ações como a dela. Nos anos anteriores à publicação desse guia,

---

[18] O SonicWall é um software firewall, responsável por filtrar como um servidor corporativo conversa com a internet. Firewalls são barreiras digitais destinadas a barrar tráfego de rede proveniente de computadores desconhecidos e/ou não autorizados.

[19] HTTPS é um protocolo de comunicação entre computadores utilizado para que dois ou mais computadores estabeleçam comunicação segura e criptografada entre si, impedindo que terceiros possam enxergar facilmente o conteúdo da "conversa".

[20] Para uma base comparativa, um software comercial contemporâneo como o Mozilla Firefox ou o Microsoft Word tem por volta de um a dois milhões de linhas de código.

[21] Powershell é o nome oficial da linha de comando do Windows.

Fisher já havia publicado outros dois manuais semelhantes, um direcionado a mostrar como ela realizou uma invasão no sistema da polícia catalã, e outro para estimular invasões semelhantes às que ela realizou na empresa de ciberespionagem Gamma Group. Para provar que as ações realmente ocorreram, em cada um dos ataques a hacker vazou também um grande pacote de informações internas provenientes de meses ou anos de monitoramento de seus adversários.

Circunscrevendo o inimigo digital no ambiente informacional

Phineas Fisher mostra um perfil abertamente de esquerda, mas seu método e lógica, que contestam a legitimidade das barreiras digitais delimitadoras das fronteiras computacionais dos bancos, empresas, em geral, ou departamentos de polícia e tribunais, poderiam facilmente ser apropriados por grupos fundamentalistas religiosos, supremacistas brancos revoltados com o *big government*, simples criminosos digitais, programadores entediados, além de, é claro, serviços estatais e privados de espionagem. Historiadores dos militares, como Martin van Creveld (2015), Peter Galison (1994) e Manuel de Landa (1991), entre outros, mostram como uma certa imaginação da persona do inimigo, assim como as supostas capacidades técnicas deste, historicamente guiam o mandato e o escopo das ações dos serviços de segurança. Isso faz com que ocorra uma espécie de corrida armamentista permanente entre os militares e seus oponentes, que constantemente utilizam novas tecnologias como formas de enfrentar ou evadir a lei, resvalando na constante atualização do aparato militar.

Neste capítulo, argumento que o conceito de "ambiente informacional", que apresentarei a seguir, foi desenvolvido pelas forças de segurança dos EUA exatamente para lidar com uma situação do tipo *Phineas Fisher*. No sumário do documento do Departamento de Defesa que define o termo encontramos, por exemplo, uma passagem que versa sobre os desafios sociais enfrentados pelas forças de segurança dos EUA relacionados à informação e às tecnologias de informação:

> The security environment is the set of global conditions, circumstances, and influences that will affect the employment of the U.S. military and includes the sum of all operational environments (OE). The Joint Force will face two interrelated challenges in the future security environment. The first is contested norms in which powerful actors, dissatisfied with the status quo, will capitalize on changes in communication and changes in socio-cultural contexts to contest norms governing international behavior. The second challenge is persistent disorder in which weak states are incapable of maintaining domestic order in the face of crisis. Information pervades the security environment, enabling people to see more, share more, create more, and organize faster than ever before. Information technology has significantly enhanced human interaction around the globe and elevated the importance of information as an instrument of power wielded by individuals and societies in politics, economics, and warfare. Advances in information technology have significantly changed the generation of, transmission of, reception of, and reaction to information. These advances have increased the speed and range of information, diffused power over information, and shifted socio-cultural norms. (p.vi)

O trecho acima nos leva direto ao jargão militar e explica um pouco sobre a ecologia do Departamento de Defesa, justificando o porquê da instituição de um "ambiente" informacional. O trecho prega que o "ambiente de segurança" — formado por quaisquer atos e circunstâncias que possam afetar a ideia de segurança corrente nas forças militares estadunidenses — agora se encontra fortemente ligado ao "ambiente informacional", pois esse último seria o cenário onde se desenrolam alguns dos principais desafios contemporâneos das forças de segurança. A ligação entre "ambiente de segurança" e "ambiente informacional" implica o estabelecimento do último como um importante "local" dos acontecimentos e esforços militares, justificando a construção de linguagem que insere o "ambiente informacional" entre os "ambientes operacionais"[22] das forças de segurança. Através dessa lógica, o Departamento de Defesa estende o seu mandato para a execução da "segurança" e da "defesa" também no "ambiente informacional". Em tal novo ambiente, a informação em si e as tecnologias de informação são centrais: segundo o DoD, como a informação agora é considerada um "instrumento de poder", utilizado por sociedades e indivíduos para confrontos nos âmbitos político, econômico e militar, as forças militares estadunidenses devem imediatamente se preparar para atuar também nesse novo ambiente operacional.

Na passagem citada também vemos claramente expressa a questão de que mudanças no status quo e a "contestação de normas" são algumas das principais preocupações do DoD e de seus chefes políticos civis. Como veremos, tais preocupações — utilização de novas tecnologias por adversários e possíveis mudanças nas "normas socioculturais" — têm fortes raízes históricas e acompanham há pelo menos um século as ações do Departamento de

[22] "The joint force commander's operational environment is the composite of the conditions, circumstances, and influences that affect employment of capabilities and bear on the decisions of the commander (encompassing physical areas and factors of the air, land, maritime, and space domains) as well as the information environment (which includes cyberspace)." (DEPARTMENT OF DEFENSE, 2012, p. viii) (JP 3-13).

Defesa nos EUA e em todo o mundo. Se enfrentar um inimigo sofisticado como Phineas Fisher agora é uma das tarefas das forças militares, como exatamente proceder em termos de ações possíveis contra tal adversário? Para os militares estadunidenses, veremos que a resposta seria "através da atividade de inteligência militar", ou, mais especificamente, através de "operações em ambiente informacional", atividades ligadas histórica e materialmente à inteligência militar, como detalhado no capítulo 2. As seções de inteligência militar[23] são os órgãos responsáveis pela operação dentro das forças de segurança estatais das tarefas relacionadas a "coletar informações sobre o inimigo e sobre o ambiente de batalha para o comandante" (FINNEGAN; DANYSH, 2015, p. 3), por isso a sua importância no caso, por exemplo, de um inimigo que mascara aleatoriamente seu tráfego hacker entre o tráfego de outros usuários, ocultando sua identidade em uma trilha complexa e não trivial de caminhos online, e, além disso, agindo com finalidades políticas.

É justamente o trabalho da inteligência militar desenvolver e operacionalizar métodos de identificação e neutralização de tal ameaça complexa. Para isso, as seções de inteligência desenvolveram uma série de subdisciplinas que executam cada uma das funções relacionadas à identificação, monitoramento e neutralização de inimigos; essas disciplinas são chamadas hoje pelo DoD de *Information Related Capabilities* (IRCs) e são capacidades chave que, segundo a estratégia atual do DoD, devem ser colocadas em prática em todas as forças de segurança estadunidenses, como maneira de responder aos desafios no ambiente informacional e no ambiente de segurança.

Para que possamos nos aproximar mais do conceito de "ambiente informacional", proponho observar com mais atenção o aparato sociotécnico que compoẽm esse emaranhado de termos, pessoas, técnicas e tecnologias. Antes de navegarmos com mais detalhes pelos termos e relações nativas que caracterizam o ambiente informacional e as operações militares neste, precisamos fazer uma escala nos arredores do rio Potomac, nas divisas dos estados de Maryland e Virgínia, a fim de conhecermos um pouco mais sobre as pessoas e organizações que formam o Departamento de Defesa e a mais ampla comunidade de inteligência — organização interagências que inclui o DoD como membro coordenador e que executa de fato as funções de inteligência para o governo dos EUA. A próxima seção é dedicada, portanto, a apresentar como vivem atualmente os militares do setor de inteligência e suas principais organizações.

[23] As seções de inteligência militar dos serviços de segurança estatais são também conhecidas como serviços de espionagem ou polícias secretas.

Bases militares, embaixadas e fortalezas digitais subterrâneas: a comunidade de inteligência e seus frequentadores civis e militares

Os militares que operam no ambiente informacional, pessoas que integram o objeto de estudo deste trabalho, se distribuem espacialmente por todo os EUA, compondo o que é oficialmente chamado pelo governo dos EUA de "comunidade de inteligência" (CI). Essa comunidade é formada hoje por dezoito agências:

> - Two independent agencies—the Office of the Director of National Intelligence (ODNI) and the Central Intelligence Agency (CIA);
> - Nine Department of Defense elements—the Defense Intelligence Agency (DIA), the National Security Agency (NSA), the National Geospatial-Intelligence Agency (NGA), the National Reconnaissance Office (NRO), and intelligence elements of the five DoD services; the Army, Navy, Marine Corps, Air Force, and Space Force;
> - Seven elements of other departments and agencies—the Department of Energy's Office of Intelligence and Counterintelligence; the Department of Homeland Security's Office of Intelligence and Analysis and U.S. Coast Guard Intelligence; the Department of Justice's Federal Bureau of Investigation and the Drug Enforcement Agency's Office of National Security Intelligence; the Department of State's Bureau of Intelligence and Research; and the Department of the Treasury's Office of Intelligence and Analysis (OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE, 2022).

Estima-se que a comunidade de inteligência dos EUA emprega hoje cerca de 850 mil pessoas (PRIEST; ARKIN, 2011), a maioria delas através de empresas privadas que prestam serviços ao governos dos EUA, as chamadas *government contractors*[24]. Três tipos de locais são centrais para a existência da comunidade de inteligência: as bases militares dos EUA, assim como suas embaixadas, são os locais de onde se opera a política externa e de segurança dos Estados Unidos no estrangeiro; no interior dos EUA, grandes escritórios subterrâneos sem janelas servem hoje como locais de trabalho da CI, além de serem locais onde a infraestrutura de comunicações e computação da CI e do setor de defesa se encontram fisicamente (SNOWDEN, 2019, p. 95). Exemplos desse último tipo de construção, os escritórios-servidores subterrâneos, são os *National Cryptologic Centers* que a *National Security Agency* mantém em Utah, no Havaí, no Texas e na Geórgia (P/K, 2019), que servem ao mesmo tempo como gigantescos centros de interceptação de comunicações e sedes administrativas da NSA. Nessa classificação de construções também se incluem as sedes da

CIA em Washington DC, edificações com vários andares subterrâneos ligados entre si por redes de túneis (SNOWDEN, 2019, p. 95).

[24] Exemplos de grandes *contractors* são Lockheed Martin, Northrop Grumman, ManTech, Boeing, Analytic Services Inc e Humana (THE TOP 10 FEDERAL DEFENSE CONTRACTORS, 2021).

Além das bases, embaixadas e escritórios-servidores espalhados pelos EUA e pelo mundo, um local é particularmente importante para o convívio dos membros e para a operação da CI, pela proximidade do local com os centros de poder e decisões civis do governo dos EUA. Washington DC, capital dos EUA, se situa no encontro dos estados de Maryland e Virgínia, a 115 metros de elevação do mar e a cerca de 35 quilômetros de distância do Oceano Atlântico. A região tem clima subtropical úmido e temperaturas que variam dos 7 aos 33 graus Celsius, contando com uma malha urbana de cerca de 30 km de raio, porém se estendendo na direção leste por mais 50 km até a cidade de Baltimore. O distrito de Washington DC concentra a maior parte das agências e departamentos do governo federal dos EUA, assim como as sedes das maiores empresas *contractors* do governo, o que torna essa região uma área de extrema importância para a operação do dia a dia do governo dos EUA. Segundo um levantamento recente, moram nessa região aproximadamente 5.7 milhões de pessoas, sendo 375 mil delas empregadas diretamente pelo governo federal dos EUA, entre as quais cerca de 70 mil são empregadas pelo Departamento de Defesa (U.S. BUREAU OF LABOR STATISTICS; FEDERAL RESERVE BANK OF ST. LOUIS, 2022). Nos arredores de DC, encontramos ainda mais 80 mil empregados diretos do DoD no estado da Virgínia e mais 40 mil no estado de Maryland (FEDERAL CIVILIAN EMPLOYMENT, 2022). Tal concentração de funcionários federais faz com que essa região tenha alguns dos maiores preços de aluguel e custos de vida dos EUA (ANDREWS, 2021). A maior parte do que se passa nos materiais analisados nesta dissertação foi decidido ou elaborado nos arredores de DC, por membros civis do governo envolvidos na CI (como funcionários em cargos comissionados no DoD) ou membros militares que a integram.

Através de pesquisas na plataforma Glassdoor[25] utilizando as palavras chave "military intelligence" e "intelligence specialist", é possível navegar por diversas vagas de emprego para a área, assim como relatos de salários e condições de trabalho postados online publicamente por funcionários da CI. Os salários variam de aproximadamente U$ 50 mil anuais, no caso de soldados especialistas em inteligência do Exército trabalhando em cargos iniciantes ou subalternos, a cerca de U$ 100-130 mil anuais para especialistas de caráter mais técnico nas áreas de invasão de computadores ou criptologia[26] na NSA, e U$ 190 mil anuais para gerentes e líderes sêniores de áreas internas da inteligência militar no DoD.

[25]Site que reúne vagas de empregos. Saiba mais em: https://www.glassdoor.com.br/. Acesso em: maio 2022.
[26] Criptologistas são especialistas na criação e quebra de códigos.

O ingresso e o "crescimento" na atividade de inteligência se dá principalmente através de três maneiras:

A primeira é através do serviço militar e posterior ingresso nas escolas de formação superior das forças armadas dos EUA — localizadas por todo o território e responsáveis pela formação de pessoal especializado para cada subárea das forças militares. Através da combinação de ensino profissional militar, experiência e tempo de serviço, é possível progredir na carreira militar tornando-se um oficial e, eventualmente, um comandante em alguma unidade das forças armadas, no próprio Departamento de Defesa ou em outros setores do governo federal.

Outra forma de ingresso na atividade da inteligência militar é a utilizada por Snowden (SNOWDEN, 2019, p. 91): ser contratado por uma empresa *contractor* para prestar serviços ao governo como um militar, porém, como um funcionário privado. Nesse caso, os funcionários podem ter formações técnicas tradicionais universitárias, que serão complementadas por cursos de formação interna em cada agência, a qual sediará de fato seus trabalhos. Tal opção pode ser verificada pela quantidade de vagas disponibilizadas pelas diversas *contractors* do setor de defesa e pelas diversas agências de inteligência militar que compõem a CI nas plataformas de busca de emprego online, como a já citada Glassdoor.

A terceira forma de se juntar a CI é através de um apontamento político para o exercício de cargo comissionado na administração federal. Essa via de entrada ocorre no âmbito da política partidária, das administrações e dos congressistas eleitos, e funciona como uma maneira de o executivo, o judiciário e o legislativo civis exercerem o controle e o monitoramento político — relacionado à sociedade civil — da atividade de inteligência.

As primeiras duas opções — uma carreira nas forças armadas ou uma contratação pela iniciativa privada — são majoritariamente as formas de entrada e de progressão no setor de inteligência, com apenas uma minoria de especialistas em inteligência sendo provenientes de cargos de natureza política, apesar de alguns desses cargos, como o de Secretário da Defesa ou o de Diretor de Inteligência Nacional, serem cargos civis muito importantes a ponto de poderem ajudar a mudar os rumos do aparato de segurança estadunidense.

A doutrina militar estadunidense e a importância do *Joint Chiefs of Staff* do Departamento de Defesa

No começo desta pesquisa, procurando estudar sobre a prática da ciberespionagem militar, comecei a frequentar certos espaços online voltados principalmente ao público militar

estadunidense, como seminários e conferências online[27], podcasts[28], sites de notícias[29], canais do YouTube[30] e bibliotecas digitais[31]. Não sendo um militar[32], tive que, em primeiro lugar, me acostumar à linguagem, repleta de termos e lógicas desconhecidos para mim. Utilizando inicialmente o método de notar recorrências e divergências nos discursos e narrativas, ao buscar por "ambiente informacional", me deparei com a recorrência de três outros termos: "doutrina", "operações de informação" e "operações no ciberespaço", que se mostraram muito importantes ao longo da pesquisa e serviram como âncoras para a realização desta dissertação. Assim, para seguirmos traçando o conceito de "ambiente informacional", proponho analisarmos nesta sessão o termo-vizinho "doutrina", uma vez que, como veremos, é através da doutrina que se estabelece um léxico comum capaz de dar corpo às ações propostas pelos termos "operações de informação" e "operações no ciberespaço", que serão analisados em detalhes no próximo capítulo.

Ao monitorar esses ambientes públicos online destinados a frequentadores castrenses, noto que em boa parte das vezes que oficiais estadunidenses falam sobre a execução de ciberoperações por parte das forças militares, quase sempre eles se referem à "doutrina" como algo orientador para suas falas seguintes. Buscando descobrir sobre o que é essa doutrina, encontro em um podcast da Escola Militar de West Point uma fala do Diretor de Doutrina do Exército dos EUA, Coronel Rich Creed:

---

[27] Por exemplo a CyCon, da OTAN, seminários do *Center for Strategic and International Studies* (CSIS), do *Royal United Services Institute* (RUSI) e do *Army Cyber Institute da West Point Academy*, todos disponíveis no YouTube (https://www.youtube.com/).

[28] Por exemplo o *War on the Rocks Podcast*, o *Irregular Warfare Podcast*, o *Modern War Institute at West Point Podcast*, *U.S. Army Heritage and Education Center Military History Lectures Podcast* e o *Combined Arms Doctrine Directorate (CADD) Podcast*, todos disponíveis na plataforma Google Podcasts (https://podcasts.google.com/). Acesso em: maio 2022.

[29] Sites como o The WarZone (https://www.thedrive.com/the-war-zone), DefesaNet (https://www.defesanet.com.br/), DefenseOne (https://www.defenseone.com/), DefenseTech (https://www.military.com/defensetech) e BreakingDefense (https://breakingdefense.com/). Acesso em: maio 2022.

[30] Como CovertCabal (https://www.youtube.com/c/CovertCabal), Battle Order (https://www.youtube.com/c/BattleOrder), Task and Purpose (https://www.youtube.com/c/Taskandpurpose) e o Binkov Battlegrounds (https://www.youtube.com/c/BinkovsBattlegrounds). Acesso em: maio 2022.

[31] Principalmente a biblioteca digital de Doutrina Militar do think tank alemão *Berlin Information Center for Transatlantic Security* (https://www.bits.de/NRANEU/others/doctrine.htm), do *Joint Chiefs of Staff* do Departamente de Defesa (https://www.jcs.mil/library/), a Homeland Security Digital Library (https://www.hsdl.org/c/), a biblioteca digital do *Congressional Research Service* dos EUA (https://crsreports.congress.gov/) e a biblioteca digital do *Project on Government Secrecy* da *Federation of American Scientists* (https://sgp.fas.org/). Acesso em: maio de 2022.

[32] Além de pesquisador, minha profissão é a de programador de computadores e robôs.

> Every profession, and the US Army is a profession, has a unique body of knowledge. Our body of professional knowledge is our doctrine, (...) [it] establishes the language of our profession and it fits in a larger body of army knowledge. For the army this larger body includes regulation pamphlets which address the administration of the army; training publications which address some specific training tasks and procedures; we have technical manuals, which address some specific equipment related topics - how we do maintenance and operate equipment and so forth; and we have finally the doctrine, which addresses the conduct of operations. Doctrine really gets to how the army operates. (URBAN WARFARE PROJECT, 2021, 3:00).

A partir das palavras do Coronel Creed, concluo que meu interesse repousa nas práticas organizacionais — o que Creed chama de operações — da inteligência militar estadunidense, uma vez que são essas práticas que de forma geral povoam os manuais sobre os quais me debrucei como porta de entrada etnográfica. Pesquisando sobre quais documentos e materiais em que poderia obter para a realização de uma pesquisa sobre que relações e lógicas emergem das práticas relacionadas à informação no setor de inteligência do governo dos EUA, descobri que, no Departamento de Defesa dos EUA, órgão responsável segundo eles mesmos por "providenciar as forças necessárias para deter a guerra e garantir a segurança nacional" (OUR STORY, [*s. d.*]), existe um importante comitê chamado *Joint Chiefs of Staff* (JCS), que, entre outras coisas, é responsável pela publicação da doutrina militar oficial, destinada a ser seguida por todas as agências e forças subordinadas ao DoD[33].

O *Joint Chiefs of Staff* é chefiado pelos oficiais mais graduados das forças militares estadunidenses — apontados pelo Presidente dos EUA e confirmados pelo Senado — e tem a missão de supervisionar o presente e planejar o futuro das *Joint Forces*[34] (ABOUT THE JOINT CHIEFS OF STAFF, 2016). O comitê é operacionalizado por um *staff* burocrático permanente, formado por alguns dos melhores alunos provenientes das escolas de formação militar, e é organizado em seções internas, cada uma responsável por supervisionar a operação de um ramo militar considerado essencial para a defesa dos EUA. Sendo formado por grandes especialistas em assuntos militares, o JCS também tem as funções de assessorar o presidente e o Conselho de Segurança Nacional[35] em assuntos de segurança interna e externa,

---

[33] A doutrina militar de inteligência do DoD é seguida como padrão de doutrina da CI, já que o JCS possui, como veremos, um órgão padronizador de termos, técnicas e procedimentos, sendo este órgão muito importante e influente na comunidade militar e de segurança dos EUA como um todo.

[34] Conjunto de todas as forças militares, o que inclui exército, marinha, guarda costeira, forças espaciais, marines e aeronáutica, além das diversas agências sob o controle do DoD, conforme veremos na próxima seção. Durante a pesquisa não consegui achar uma lista oficial contendo todas as agências. Uma lista compilada por usuários da Wikipédia pode ser vista em: LIST OF U.S. DEPARTMENT OF DEFENSE AGENCIES (2022), a qual lista pelo menos 50 agências. Uma lista de websites ligados ao DoD, presente no próprio website do DoD, mostra algumas centenas de unidades internas (DOD WEBSITES, [*s. d.*]).

[35] O Conselho de Segurança Nacional é um conselho composto por indicados do Presidente dos EUA que atuam como assessores e operadores das políticas de segurança estipuladas por ele. Os conselheiros de segurança nacional atuam em um ambiente interagência como emissários do poder civil.

além de consolidar uma doutrina única — a chamada *Joint Doctrine* — para todas as *Joint Forces* sob seu comando. O JCS mantém uma biblioteca digital que contém todos os milhares de documentos definidores da doutrina atual das forças militares estadunidenses. Essa biblioteca digital é a fonte da maioria dos documentos oficiais que analiso neste trabalho[36].

Navegando pela biblioteca, encontrei um livro que se tornaria um companheiro durante todo o percurso da pesquisa: o *Dicionário de Termos Militares e Associados* (DTMA), também publicado pelo JCS. O diciońario é atualizado constantemente por uma equipe fixa[37], como parte de um esforço do JCS em homogeneizar os termos e conceitos contidos nos milhares de manuais que definem a doutrina de cada subsetor do aparato militar estadunidense. Cada verbete do dicionário contém uma breve definição e uma seção que indica qual documento da biblioteca é a fonte mais apropriada para ser consultada a fim de saber mais sobre o verbete. O verbete de "doutrina conjunta", por exemplo, mostra a seguinte definição oficial, que confirma o que ouvimos do Coronel Creed:

> joint doctrine — Fundamental principles that guide the employment of United States military forces in coordinated action toward a common objective and may include terms, tactics, techniques, and procedures. See also Chairman of the Joint Chiefs of Staff instruction; Chairman of the Joint Chiefs of Staff manual; doctrine; joint publication; joint test publication; multinational doctrine. (CJCSI 5120.02) (JOINT CHIEF OF STAFFS, 2022, p. 123).

A doutrina militar, ou seja, os "termos, táticas, técnicas e procedimentos" encontrados em documentos oficiais e falas de militares em fóruns públicos, se solidifica materialmente em manuais que, assim como o dicionário supracitado, buscam homogeneizar não somente o conhecimento que deve circular, mas também como esse conhecimento deve ser compartilhado e colocado em prática. Assim, escolhi os manuais de doutrina do Departamento de Defesa como materiais fundamentais de pesquisa. Sugiro, agora, aprofundarmo-nos um pouco no que consiste hoje o Departamento de Defesa, a fim de que, nas seções seguintes, possamos caminhar de maneira mais informada para uma análise de suas atividades, especificamente no setor de ciberespionagem, utilizando "ambiente informacional" como eixo para tal investigação e os manuais como materialização sociotécnica desse conceito amplo e abrangente.

---

[36] A biblioteca pode ser consultada em: https://www.jcs.mil/Doctrine/. Acesso em: maio 2022.

[37] A *Joint Education and Doctrine Division* (JEE), subunidade do gabinete do *Chairman of the Joint Chiefs of Staff* (CJCS), segundo a Instrução do DoD 5025.12 (DOD, 2020) e a Instrução do *Chairman of the Joint Chiefs of Staff* 5705.01G (CJCS, 2020).

O Departamento de Defesa

Como alguns dos números apresentados nas seções acima mostram, o Departamento de Defesa dos Estados Unidos da América é uma das maiores e mais importantes organizações militares do mundo, empregando somente de maneira direta cerca de 1.3 milhões de pessoas (ACTIVE DUTY U.S. DEPARTMENT OF DEFENSE PERSONNEL NUMBERS FROM 1995 TO 2020, 2020), com um orçamento de U$ 728 bilhões em 2022 (HADLEY, 2022). Fazem parte de seu organograma todos os ramos das forças armadas dos EUA[38], assim como uma série de agências[39] que executam atividades ligadas à manutenção da segurança nacional estadunidense.

Segundo a diretiva do DoD 5100.01, que estabelece o mandato oficial do DoD, os objetivos do departamento são:

> a. Support and defend the Constitution of the United States against all enemies, foreign and domestic.
> b. Ensure, by timely and effective military action, the security of the United States, its possessions, and areas vital to its interest.
> c. Uphold and advance the national policies and interests of the United States. (DEPARTMENT OF DEFENSE, 2020, p. 1-2).

Procurando destrinchar essa definição interna de missão geral, procurei no dicionário militar por algumas das palavras-chave utilizadas na descrição acima, achando as definições de “national security” e “security” apropriadas — curiosamente não encontrando, porém, a definição de “defesa”:

[38] Os chamados “serviços” militares sob o DoD são o *US Army* (Exército), o *US Marine Corps* (conhecidos como os Marines), a *US Navy* (Marinha), a *US Air Force* (Força Aérea), a *US Space Force* (Força Espacial) e a *US Coast Guard*. Os “Comandos” são unidades militares responsáveis por coordenar em certas jurisdições o trabalho conjunto das agências e serviços do DoD, e são esses o *Africa Command*, *Central Command*, *Cyber Command*, *European Command*, *Indo-Pacific Command*, *Northern Command*, *Southern Command*, *Space Command*, *Special Operations Command*, *Strategic Command* e o *Transportation Command*.

[39] As principais agências, chamadas de *combat support agencies* são: *Defense Contract Management Agency*, *Defense Health Agency*, *Defense Information Systems Agency*, *Defense Intelligence Agency*, *Defense Logistics Agency*, *Defense Threat Reduction Agency*, *National Geospatial Intelligence Agency* e a *National Security Agency* entre outras menores como a famosa *Defense Advanced Projects Research Agency* (DARPA).

> national security — A collective term encompassing both national defense and foreign relations of the United States with the purpose of gaining: a. A military or defense advantage over any foreign nation or group of nations; b. A favorable foreign relations position; or c. A defense posture capable of successfully resisting hostile or destructive action from within or without, overt or covert. See also security. (JP 1) (JOINT CHIEFS OF STAFF OF THE DEPARTMENT OF DEFENSE, 2022, p. 162).
>
> security — 1. Measures taken by a military unit, activity, or installation to protect itself against all acts designed to, or which may, impair its effectiveness. (JP 3-10) 2. A condition that results from the establishment and maintenance of protective measures that ensure a state of inviolability from hostile acts or influences. (JP 3-10) 3. With respect to classified matter, the condition that prevents unauthorized persons from having access to official information that is safeguarded in the interests of national security. See also national security. (JP 2-0) (JOINT CHIEFS OF STAFF OF THE DEPARTMENT OF DEFENSE, 2022, p. 122).

Confesso que, ao ler essas definições em conjunto com a missão oficial do departamento, fiquei impressionado com a forma pouco sutil com que o DoD define amplamente seu escopo, de modo que, ao mesmo tempo:

> 1) o DoD se coloca como uma força de defesa dos EUA contra inimigos externos e internos;
> 2) o DoD se coloca como guarda costas dos empresários dos EUA no exterior, o que implica em uma atividade intensa fora dos EUA (e o que exigiria ou a assinatura de diversos tratados internacionais ou, então, o trabalho clandestino);
> 3) o trabalho do DoD se dá principalmente contra o que eles chamam de atos “hostis” que possam de qualquer forma ameaçar as forças de segurança e os interesses dos EUA, o que implica num gigantesco escopo de operação;
> 4) a segurança é vista como uma atividade destinada também a proteger a informação de atos e influências hostis, o que implica a utilização do segredo e da compartimentação de informação como ferramenta de trabalho.

A linguagem, tanto da missão quanto dos verbetes, é bem generalista e não entra em detalhes, mas serve como ponto de partida para a discussão e serve, além disso, para uma definição de escopo de trabalho que poderia abranger qualquer coisa considerada “ameaça”, desde estudantes panfletando contra o Exército e a política de defesa, até grupos de

criminosos online russos que atentassem contra clientes bancários estadunidenses. Como temos visto desde o início do capítulo, o "inimigo", inclusive interno, figura como centro do trabalho do DoD. Reagir ao que o comando civil e militar determina como inimigo é missão do Departamento e de seus milhões de funcionários.

Command and control e os OODA *loops*: a forma de organização do Departamento de Defesa

Uma organização gigante e burocrática como o Departamento de Defesa tem de adotar maneiras para a realização de sua gestão interna. A doutrina e os manuais são alguns desses instrumentos técnicos utilizados para a padronização da ação organizacional. Outros instrumentos importantíssimos para a operação do dia a dia do Departamento de Defesa são os conceitos — e práticas associadas — de "Comando e controle" e de *"Observ-Orient-Decide-Act loops"*, ambos de inspiração cibernética.

Como relatado com mais detalhes no capítulo 3, a partir dos anos 60, sob a gestão de Robert McNamara, o Departamento de Defesa passa a adotar a teoria de sistemas — e suas ciências filhas: cibernética, análise de sistemas, teoria do controle e teoria dos jogos — como forma essencial de conceber a organização do aparato militar estadunidense. A partir da teoria de sistemas, um sistema é abstraído como uma máquina que recebe estímulos, realiza operações de processamento com esses estímulos de entrada (*inputs*) como parâmetros principais e gera respostas (também chamadas de dados de saída ou *outputs*). A teoria cibernética e sua irmã, teoria do controle, preveem que pode ser calculado um valor chamado "erro" a partir de uma comparação das saídas efetivas de um sistema com saídas ideais previstas pelo "administrador de sistema". Com a diferença entre as saídas efetivas e as saídas ideais projetadas em mãos, seria possível pensar que mudanças precisam ser realizadas na etapa de processamento de estímulos da máquina, de modo que a saída do sistema se aproxime mais da saída ideal. É denominado "controle" tal processo de ajuste do sistema, realizado através do cálculo do "erro" e da tomada que ações que processem de forma mais adequada os estímulos de entrada fornecidos ao sistema. Sistemas que calculam seu próprio erro e contêm mecanismos de auto ajuste interno para aproximarem-se automaticamente das respostas ou saídas desejadas são denominados "sistemas cibernéticos".

O Departamento de Defesa passa então a ser conceitualizado como uma máquina ou sistema cibernético que recebe como estímulos os dados relacionados ao "ambiente de segurança" e realiza operações em seus "ambientes operacionais", de modo a gerar como

resultado um “ambiente de segurança” estavelmente favorável aos interesses nacionais e à poĺitica externa dos EUA[40]. A análise de sistemas pode ser utilizada para quebrar esse sistema grande, complexo e ambicioso, compartimentando objetivos em subsistemas menores, dedicados cada um a receber certos dados do “ambiente de segurança” e a realizar certas operações em determinados “ambientes operacionais”, de modo que cada subsistema realize objetivos menores e mais simples. Um dos trabalhos mais árduos do DoD é a constante interligação entre os subsistemas, seus dados de entrada e seus resultados, que, somados, resultam no sistema complexo que representa a operação cotidiana do departamento. Para a avaliação quantitativa e como método de “controle” — ajuste das operações de processamento do sistema visando a melhoria dos resultados — a teoria dos jogos fornece as ferramentas para a simulação de situações que envolvem o comportamento humano, simulações essas que serão utilizadas como balizas a serem testadas contra a realidade para a realização dos ajustes necessários na máquina de segurança que é o DoD.

Os conceitos de “Comando e controle” e de *“Observ-Orient-Decide-Act loops”* derivam diretamente do pensamento ligado às teorias de sistemas, controle e cibernética, que inspiram hoje a organização do DoD. O dicionário do DoD define “Comando e controle” como um sistema que engloba toda a infraestrutura — incluindo procedimentos — necessários para que um comandante militar exerça sua função:

> command and control system — The facilities, equipment, communications, procedures, and personnel essential for a commander to plan, direct, and control operations of assigned and attached forces pursuant to the missions assigned. (JP 6-0) (JOINT CHIEFS OF STAFF, 2022, p. 40).

O elemento de controle se dá através da operacionalização do conceito de *Observ-Orient-Decide-Act Loop*, também conhecido como *OODA Loop*, criado nos anos 60 pelo pesquisador em cibernética e oficial da aeronáutica John Boyd, e subsequentemente adotado pelo DoD como princípio para o ajuste do maquinário interno de segurança (OSINGA, 2006). O conceito institui os quatro passos cíclicos — “observar”, “orientar”, “decidir” e “atuar” — como os passos fundamentais a serem realizados no interior de cada subsistema do DoD e como maneiras genéricas de obter a cada “iteração”[41] do loop melhores resultados de saída. Um comandante ou administrador de uma unidade militar deve utilizar a infraestrutura de

[40] Raciocínio realizado aplicando o conceito de sistema cibernético às definições anteriores sobre a missão do Departamento de Defesa.

[41] Cada “iteração” é uma situação em que o sistema fornece respostas baseado em um conjunto específico de estímulos ou dados de entrada.

comando e controle para a execução dos passos previstos nos OODA loops, de modo a continuamente adquirir novas informações sobre o "ambiente de segurança" e a continuamente tomar decisões e ações no sentido da completude dos objetivos militares.

A operação de fato desse conceito envolve uma ampla necessidade de equipamentos, instituições, técnicas e serviços técnicos — uma parte significativa relacionada ao gerenciamento da informação interna do DoD — que transpassam as fronteiras do Departamento de Defesa e permeiam o resto do governo civil dos EUA, assim como a iniciativa privada, como vimos no caso das carreiras privadas da comunidade de inteligência. Nesse sentido, o Departamento de Defesa constrói historicamente uma forte relação com a indústria de equipamentos militares e armamentos, através não só de amplas compras militares de equipamentos e de tecnologia, mas também através da criação de instituições, como a DARPA (*Defense Advanced Research Projects Agency*), que financiam uma grande rede de empresas desenvolvedoras de protótipos e novas tecnologias, formando o que os militares chamam de base industrial de defesa:

> defense industrial base — The Department of Defense, government, and private sector worldwide industrial complex with capabilities to perform research and development, design, produce, and maintain military weapon systems, subsystems, components, or parts to meet military requirements. Also called DIB. (JP 3-27) (JOINT CHIEFS OF STAFF, 2022, p. 62).

Tal conjugação entre militares, desenvolvimento tecnocientífico e indústria é crucial para o funcionamento do DoD, tanto na forma de prestação de serviços como na forma da produção dos equipamentos e sistemas militares, principalmente desde que passam a crescer e ganhar importância as chamadas Tecnologias da Informação e das Comunicações (TICs), sendo a Primeira Guerra do Golfo um marco para a transição total do DoD em direção a ser uma organização orientada à informação, principalmente na forma de informação digital.

A Operação *Desert Storm* em 1991 contra Saddam Hussein mostra um pouco do por que o DoD decide privilegiar a informação e as TICs como orientadoras da ação castrense dos EUA. Como uma retaliação à invasão de Saddam Hussein ao país vizinho Kuwait, aliado dos EUA, o governo dos EUA conduziu uma ação militar que praticamente destruiu toda a infraestrutura do regime iraquiano, o que levou rapidamente à rendição de Saddam. A operação mostrou ao mundo alguns aspectos inovadores da utilização de tecnologias digitais na guerra. Em primeiro lugar, através de coleta de informações, por meio de sensoriamento remoto por satélite, e através de fontes de inteligência, como interceptações de comunicações, o DoD foi capaz de mapear onde se encontrava toda a infraestrutura de defesa e de

funcionamento do país iraquiano. Foram mapeados usinas elétricas, antenas e cabos de comunicação, poços de petróleo, estradas, prédios com escritórios do governo, quartéis, galpões de depósitos, defesas antiaéreas.

Após a coleta de dados de inteligência, caças estadunidenses conduziram 42 dias de bombardeios contra o Iraque a partir de navios porta-aviões localizados a centenas de quilômetros de distância no Mar Vermelho e no Golfo Pérsico. Os alvos prioritários foram as defesas antiaéreas do governo iraquiano e as instalações de telecomunicações, ambos destruídos rapidamente, possibilitando o colapso de todo o Iraque, praticamente sem possibilidade de resistência. Satélites, radiocomunicação digital, GPS, embaralhadores de frequências[42] e bombas de precisão guiadas computadorizadamente foram algumas das tecnologias e objetos que possibilitaram que a primeira Guerra do Golfo terminasse com baixíssimas mortes das forças dos EUA e uma destruição avassaladora do Iraque.

As campanhas da OTAN na Bósnia (a partir de 1992) e na Iugoslávia (1999), também ocorrem de maneira semelhante: primeiro mapeia-se — por meio dos vários métodos de vigilância digital e inteligência — tropas, infraestruturas e comunicações adversárias e, então, atua-se para destruir as defesas antiaéreas e degradar as formas de comando e controle do inimigo, principalmente suas comunicações; em seguida, campanhas aéreas coordenadas remotamente em tempo real por meio de uma série de equipamentos e armamentos digitais destroem estradas, galpões, quartéis, cidades, de modo a fazer os inimigos renderem-se antes de um engajamento entre tropas lutando no chão. Fundamentais para essas operações foram o conceito de disrupção da cadeia de Comando e Controle inimiga, assim como a manutenção da cadeia de Comando e Controle aliada.

Essas operações militares são conduzidas pelo DoD nos anos 90 e consolidam, através da própria ação militar estadunidense, a percepção de que o controle informacional — nessa época considerado como a habilidade de se comunicar bem enquanto o inimigo se comunica mal — seria essencial para garantir a habilidade das forças de defesa dos EUA de prevalecer em um conflito em que a informação serve como elo que garante a coesão do sistema de Comando e Controle militar.

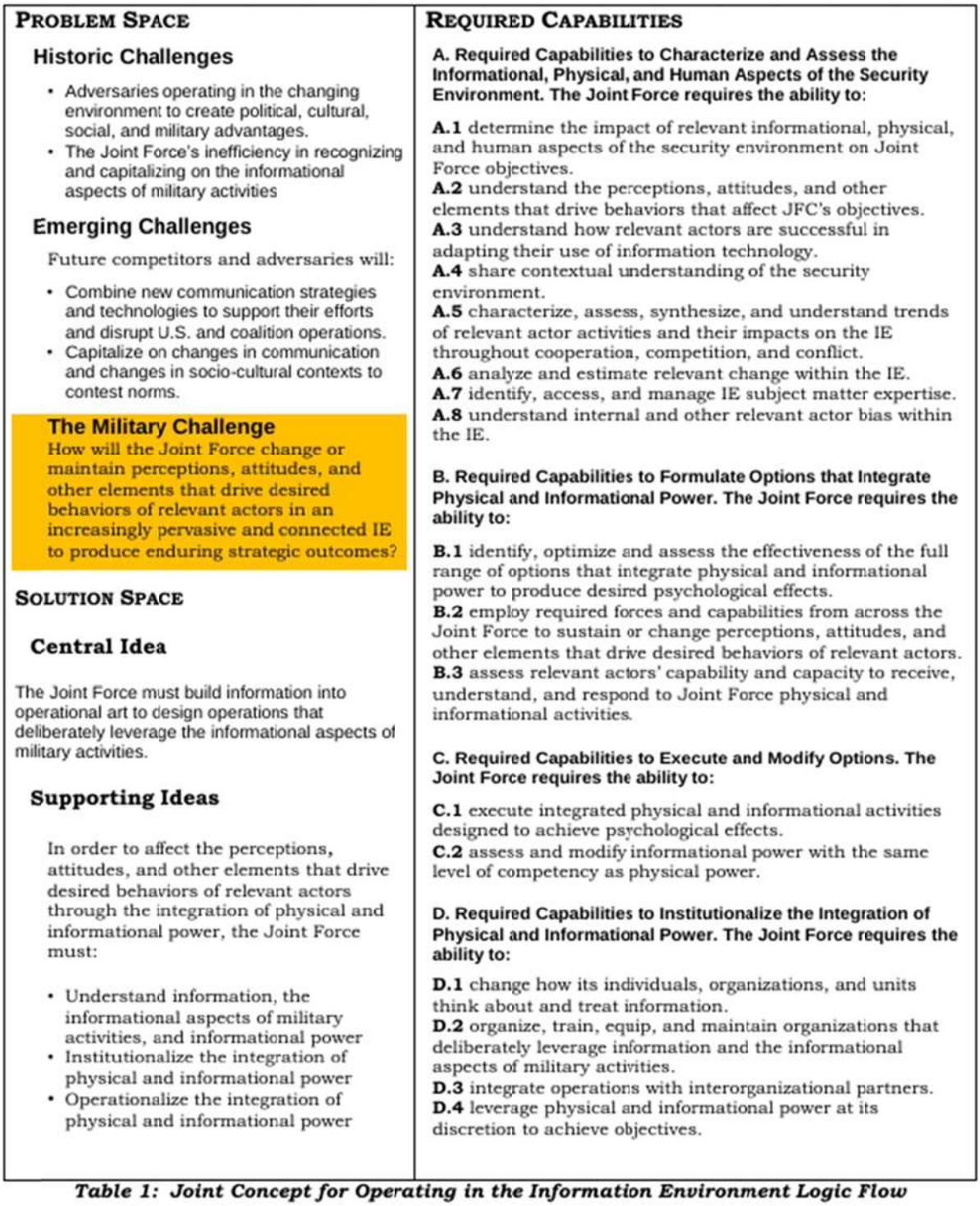
[42] Dispositivos criados para preencher com ruído as frequências utilizadas para a comunicação analógica e digital, cujo objetivo é tornar a comunicação impossível ou muito difícil.

O problema-solução do ambiente informacional

Podemos agora, com um pouco mais de contexto sobre a doutrina, os militares e o Departamento de Defesa, bem como suas formas básicas de organização e o papel geral da informação nessa organização, submergir nos manuais que definem o "ambiente informacional", em busca de entender qual o significado e quais ações efetivamente são previstas pelo termo a partir da perspectiva dos militares — ou da perspectiva doutrinária. É importante ressaltar que os documentos dão maior ênfase às operações em ambiente informacional do que a definições conceituais do que seria o ambiente informacional em si, ou seja, são as operações que definem o ambiente sob a perspectiva militar.

No começo do recente manual *Joint Concept for Operating in the Information Environment* (JCOIE), há um sumário executivo da proposta central do texto, seguido por uma tabela contendo um resumo esquemático do conteúdo do documento (JOINT CHIEFS OF STAFF, 2018, p. xi). A tabela contém o *logic flow*[43] que resume o conceito de operação em ambiente informacional que o DoD tenta colocar em prática, e é dividida verticalmente na metade. Do lado direito, prevendo precedência na leitura, encontram-se duas subdivisões, nomeadas "ESPAÇO PROBLEMA" e "ESPAÇO SOLUÇÃO". Do lado esquerdo, há só uma grande subseção: "CAPACIDADES REQUERIDAS". No lado que corresponde ao espaço problema-solução, os autores expõem a justificativa e a racionalidade por trás do conceito de operação em ambiente informacional. No lado relacionado às capacidades, são expostas ações práticas que precisam ser tomadas no interior do DoD para que o Departamento esteja preparado para prevalecer sobre seus adversários no "ambiente informacional".

[43] Um diagrama contendo fluxos lógicos por trás de um processo ou ideia.



PROBLEM SPACE

Historic Challenges

- Adversaries operating in the changing environment to create political, cultural, social, and military advantages.
- The Joint Force's inefficiency in recognizing and capitalizing on the informational aspects of military activities

Emerging Challenges

Future competitors and adversaries will:

- Combine new communication strategies and technologies to support their efforts and disrupt U.S. and coalition operations.
- Capitalize on changes in communication and changes in socio-cultural contexts to contest norms.

The Military Challenge

How will the Joint Force change or maintain perceptions, attitudes, and other elements that drive desired behaviors of relevant actors in an increasingly pervasive and connected IE to produce enduring strategic outcomes?

SOLUTION SPACE

Central Idea

The Joint Force must build information into operational art to design operations that deliberately leverage the informational aspects of military activities.

Supporting Ideas

In order to affect the perceptions, attitudes, and other elements that drive desired behaviors of relevant actors through the integration of physical and informational power, the Joint Force must:

- Understand information, the informational aspects of military activities, and informational power
- Institutionalize the integration of physical and informational power
- Operationalize the integration of physical and informational power

REQUIRED CAPABILITIES

A. Required Capabilities to Characterize and Assess the Informational, Physical, and Human Aspects of the Security Environment. The Joint Force requires the ability to:

A.1 determine the impact of relevant informational, physical, and human aspects of the security environment on Joint Force objectives.
A.2 understand the perceptions, attitudes, and other elements that drive behaviors that affect JFC's objectives.
A.3 understand how relevant actors are successful in adapting their use of information technology.
A.4 share contextual understanding of the security environment.
A.5 characterize, assess, synthesize, and understand trends of relevant actor activities and their impacts on the IE throughout cooperation, competition, and conflict.
A.6 analyze and estimate relevant change within the IE.
A.7 identify, access, and manage IE subject matter expertise.
A.8 understand internal and other relevant actor bias within the IE.

B. Required Capabilities to Formulate Options that Integrate Physical and Informational Power. The Joint Force requires the ability to:

B.1 identify, optimize and assess the effectiveness of the full range of options that integrate physical and informational power to produce desired psychological effects.
B.2 employ required forces and capabilities from across the Joint Force to sustain or change perceptions, attitudes, and other elements that drive desired behaviors of relevant actors.
B.3 assess relevant actors' capability and capacity to receive, understand, and respond to Joint Force physical and informational activities.

C. Required Capabilities to Execute and Modify Options. The Joint Force requires the ability to:

C.1 execute integrated physical and informational activities designed to achieve psychological effects.
C.2 assess and modify informational power with the same level of competency as physical power.

D. Required Capabilities to Institutionalize the Integration of Physical and Informational Power. The Joint Force requires the ability to:

D.1 change how its individuals, organizations, and units think about and treat information.
D.2 organize, train, equip, and maintain organizations that deliberately leverage information and the informational aspects of military activities.
D.3 integrate operations with interorganizational partners.
D.4 leverage physical and informational power at its discretion to achieve objectives.

Table 1: Joint Concept for Operating in the Information Environment Logic Flow

Imagem 4 - Tabela com o "fluxo lógico" sobre operações em ambiente informacional (Fonte: DEPARTMENT OF DEFENSE, 2018, p. xi)

Na primeira metade da tabela — e do documento JCOIE, já que a tabela resume o próprio documento —, relacionada à justificativa para a operação em ambiente operacional, são listados em ESPAÇO PROBLEMA alguns "desafios históricos" dos militares, um deles

relacionado aos inimigos e outro relacionado a problemas internos das forças de segurança: “adversários que se utilizam de um ambiente dinâmico para obter vantagens políticas, culturais, sociais e militares” são o desafio externo, e “a ineficiência das forças conjuntas em reconhecer e capitalizar os aspectos informacionais das atividades militares” se configura como o desafio interno. Também são listados como “desafios emergentes” as possibilidades que “competidores e adversários futuros combinem novas estratégias de comunicação e tecnologias para dar suporte aos seus esforços e perturbar operações dos EUA e de aliados”. Nas palavras do manual, tais adversários poderiam “capitalizar mudanças comunicacionais e mudanças em contextos socioculturais para o questionamento de normas”.

Em “desafio militar”, há somente uma grande questão, central para a organização militar frente ao novo ambiente informacional: “Como irá a força conjunta mudar ou manter percepções, atitudes e outros elementos que possam definir comportamentos desejados em atores relevantes em um mundo cada vez mais pervasivo e conectado pelo ambiente informacional, de modo a produzir resultados estratégicos duradouros?”. Esse trecho novamente remete o trabalho no ambiente informacional à alteração de comportamentos de pessoas, organizações e sistemas, resumindo e reforçando o apresentado nas seções anteriores deste capítulo sobre as preocupações atuais e o tipo de inimigo que guiaram o processo de instituição de um ambiente informacional pelas forças de segurança dos EUA.

Em ESPAÇO SOLUÇÃO são apresentadas duas ideias que resumem como conceitualmente o DoD pretende efetivamente lidar com os desafios-problemas. A ideia central é que “as forças conjuntas devem transformar informação em arte operacional para projetar operações que deliberadamente alavanquem os aspectos informacionais das atividades militares”. Como “ideia de suporte”, os autores do documento afirmam que “para afetar as percepções, atitudes e outros elementos que definem comportamentos em atores relevantes, através da integração dos poderes físicos e informacionais, a força conjunta precisa: entender informação, os aspectos informacionais das atividades militares e o poder informacional; institucionalizar a integração do poder físico e do poder informacional; operacionalizar a integração do poder físico e informacional.”

Segundo esse manual, assim como outros documentos, a conservação de uma suposta ordem — o que eles denominam segurança, como exemplificado na definição do dicionário militar — é o grande objetivo por trás dessa tentativa de adaptação das forças militares aos novos tempos. Neste trecho, novamente fica implícita a clivagem entre amigos e inimigos, sendo ambos estabelecidos como entidades indefinidas: todos os “atores relevantes”

figuram como potenciais aliados e potenciais adversários. Como o combate ao questionamento de normas e às mudanças sociais fora do controle militar são enfatizados como justificativa para a ação, essas palavras e conceitos atuam como índices cuja função é operar na realidade, interligando palavras impressas e elementos do espaço cognitivo dos usuários desse manual, e criando uma imagem maleável de inimigo que englobaria qualquer indivíduo ou grupo que possa exibir comportamento antissocial ou esteja fora do padrão de bom e certo das forças armadas. Ao assumir como história a utilização, por parte de adversários dos EUA, de um "ambiente dinâmico" para a consolidação de seus próprios objetivos políticos, e como futuro uma previsão de que os adversários combinarão novas tecnologias de comunicação e de informação para o "questionamento de normas", os autores do documento justificam, com base no social e em nome da sociedade, o porquê das forças de seguranças estadunidenses serem detentoras da responsabilidade de guardar a estabilidade política "dos EUA e seus aliados".

A solução proposta para a manutenção da "segurança" no "ambiente informacional" é "transformar informação em arte operacional", de modo a "afetar percepções, atitudes e outros elementos que definem comportamentos em atores relevantes, através da integração dos poderes físicos e informacionais". A informação aparece aqui como algo que se pode usar para afetar a tomada de decisão de pessoas, organizações e sistemas de aliados, assim como de adversários — para dissuadi-los de suas ações ou trazê-los para o campo dos aliados. O ambiente informacional, que nas suas três dimensões (cognitiva, física e informacional) envolve os humanos, as trocas informacionais entre eles, os objetos utilizados para essas trocas e as próprias informações — que podem se relacionar, por exemplo, com a produção material de bens e serviços ou com o gerenciamento da infraestrutura energética de um país — envolveria todo o mundo físico e seria o local onde seriam formados o "conhecimento", o "entendimento", as "crenças", "visões de mundo" e "ações" de indivíduos, grupos, sistemas, comunidades e organizações.

> The IE is comprised of and aggregates numerous social, cultural, cognitive, technical, and physical attributes that act upon and impact knowledge, understanding, beliefs, world views, and, ultimately, actions of an individual, group, system, community, or organization. The IE also includes technical systems and their use of data. The IE directly affects and transcends all OE. (DEPARTMENT OF DEFENSE, 2018, p. 41)

Ações derivadas do problema-solução que define o ambiente informacional: Information Related Capabilities.

A segunda parte da tabela do fluxo lógico de operação em AI lista ações específicas que precisam ser tomadas para garantir que as forças de segurança estejam preparadas para atuar nessa nova esfera. Essas ações são voltadas tanto ao desenvolvimento de capacidades internas ligadas às maneiras como o DoD lida com informação, como para o desenvolvimento de capacidades relacionadas a como o DoD pode atuar no mundo de modo a influenciar os atores relevantes que participam do "ambiente de segurança".

Através da lista de capacidades requeridas - que engloba coisas como "caracterizar, avaliar, sintetizar e entender tendências de atividades de atores relevantes e seus impactos no AI através de cooperação, competição e conflito", "integrar operações com parceiros interorganizacionais" ou "organizar, equipar, treinar e manter organizações que deliberadamente alavanquem informação e os aspectos informacionais das atividades militares", o documento JCOIE apresenta várias ações internas que precisam ser desenvolvidas, ligadas, por exemplo, à racionalização de como os próprios órgãos internos do DoD utilizam informação em seu processo decisório, mas também ligadas ao desenvolvimento de capacidades ofensivas de influenciamento de comportamentos, como, por exemplo, uma operação psicológica de chantagem.

O manual aponta como inevitáveis as transformações que ocasionam os desafios anteriormente descritos e cria um roteiro geral de ações que visam inserir as forças de segurança no papel de controladores da estabilidade social, política, cultural e militar do "ambiente informacional", o que seria realizado através da utilização conjunta de formas de coerção físicas - destinadas à dominação física do corpo - e informacionais - direcionadas à subjugação do processo de tomada de decisão dos adversários. Neste caminho pelo controle das percepções e atitudes, o ambiente informacional transforma a "segurança" em uma questão propriamente de comunicação, tendo a informação - principalmente a digital - no centro das atenções.

Tal movimento pode enunciar algumas possibilidades imensamente distintas. Se as ações destinadas a entender como os atores relevantes se comportam - essenciais para a tomada de ações de influenciamento desses atores - realmente forem realizadas com seriedade e sem preconceito, é possível que se perceba durante esse processo de entendimento do outro que é melhor que as forças de segurança atuem de maneira não violenta e não autoritária, de forma que elas participem como negociadoras políticas em situações de questionamentos à

ordem. Por outro lado, é possível a intensificação de tendências totalitárias dentro dos aparatos de segurança, com a coleta desenfreada de informações sobre tudo e todos, o que estimula o florescimento de um grande complexo empresarial da paranoia, destinado a fornecer a infra estruturas para a nova polícia digital do pensamento. Híbridos entre esses dois extremos também são possíveis, com a utilização de abordagens menos ou mais autoritárias a depender do adversário e da situação.

Até o momento apresentei o nó de relações, ou composições material-semióticas, que foi se desnovelando enquanto fui me aproximando do termo "ambiente informacional". Agora, proponho um movimento em direção à trajetória e contexto pelos quais tal termo veio a ganhar campo dentro das operações militares estadunidenses. Para tanto, retomo as questões utilizadas por Verdery (2014) e Harper (2009) para a análise etnográfica de documentos - levantando as histórias dos principais documentos analisados.

Um ambiente em construção: as ligações entre *information operations* e o *information environment*

Nesta seção realizo uma arqueologia do conceito de ambiente informacional, trazendo à tona o conceito de "operações de informação", o qual exibe um alto grau de convergência com a proposta do DoD de "operações em ambiente informacional". Como veremos nesta seção e mais adiante no trabalho, as operações de informação supõem a execução das chamadas *Information Related Capabilities*, identificadas na seção anterior como parte da "solução" do DoD para a operação em AI.

Segundo os documentos consultados, a tentativa de generalização da aplicação do conceito de AI para todas as agências e contratados pelo DoD dá uma dimensão da crescente importância da informação na perspectiva das operações de segurança. Apesar da utilização de informações ser parte das atividades básicas dos serviços de inteligência desde os primórdios desses órgãos, é somente em meados dos anos 1990 que a questão da informação ganha tal importância que faz com que os militares estadunidenses estabeleçam uma doutrina específica para a utilização integrada de informações em operações militares[44]. Um exemplo é o já apresentado panorama informacional da Primeira Guerra do Golfo e a transição do DoD para uma máquina que privilegia a informação como método de operação.

[44] O termo *operações* é definido no DoD Dictionary como "uma sequência de ações táticas com um objetivo comum ou tema unificador".

Com o lançamento do Manual de Campo *FM 100-6 Information Operations* do Exército, em 1996, e da *Joint Publication 3-13 Information Operations* do DoD, em 1998, *information operations* se tornam uma das esferas básicas de operação das forças de segurança, ao lado das operações aéreas, operações humanitárias, operações de resgate, operações antidrogas ou operações de contra-insurgência. Tal transformação implica a criação de unidades especializadas em operações militares que trabalham especificamente com o conceito de informação como tema central, assim como a integração dessas unidades e esforços no todo das forças de segurança. OI ficam definidas no manual do Exército FM 100-6 de 1996 como:

> continuous military operations within the military information environment that enable, enhance, and protect the friendly force's ability to collect, process, and act on information to achieve an advantage across the full range of military operations; information operations include interacting with the global information environment and exploiting or denying an adversary's information and decision capabilities. (1996, Glossary-7)

O think tank RAND, em um relatório de 2013 financiado e destinado à Marinha[45], faz um levantamento da história da doutrina de OI e relata que essa surge ao mesmo tempo que a ideia de Guerra de Comando e Controle (*Command and Control Warfare*), que, de maneira convergente com a definição de comando e controle atual do dicionário de termos militares, é definida em 1996 como:

> the integrated use of psychological operations (PSYOP), military deception, operations security (OPSEC), electronic warfare (EW), and physical destruction, mutually supported by intelligence, to deny information to, influence, degrade, or destroy adversary C2 capabilities while protecting friendly C2 capabilities against such actions. (CJCSI 3201.01, 1996)

A equipe da RAND comenta que a similaridade das definições de IO e de C2W mostraria um debate interno no DoD sobre como melhor lidar com a questão da informação à época (meados dos anos 90). A RAND declara a vitória do conceito de IO, assim como do conceito mais amplo de *Information Warfare* (IW), que seria um tipo de guerra baseada no controle da informação. Interessante notar que aqui estamos diante da narrativa da RAND — um think tank que atua praticamente como uma subsidiária privada de pesquisas do DoD —- para a origem do termo IO na doutrina militar estadunidense. Também é interessante notar

[45] Acesso em: https://www.jstor.org/stable/10.7249/j.ctt3fh1qp.19?seq=2#metadata_info_tab_contents. Disponível em: maio 2022.

que a definição de IO do Exército de 1996 já menciona um "ambiente informacional" e a definição apresentada de C2W, também de 1996, já contém alguns dos traços que seriam definidores do "ambiente informacional". O DoD tenta generalizá-los com a publicação do JCOIE, em 2018: C2W se trata do uso integrado de "operações psicológicas", "enganação militar", "segurança de operações", "guerra eletrônica", "destruição física" e "inteligência", para negar informações a adversários, assim como para influenciar, degradar ou destruir a capacidade dos adversários de comando e controle (C2).

Ainda segundo o levantamento histórico da RAND, após essa fase inicial de consolidação do termo, no começo dos anos 2000 ocorrem novas mudanças que elevam a prioridade do tema "informação" nos círculos de defesa nos EUA. Em 2001 ocorre o segundo *Quadrennial Defense Review*, estudo promovido pelo gabinete do Secretário de Defesa em conjunto com o *Joint Chiefs of Staff*, com a finalidade de "examinar as condições atuais de segurança nacional a fim de preparar [as forças do DoD] para desafios e oportunidades futuras"[46]. Tal estudo identifica as OI como um entre seis pontos críticos que necessitam de respostas e transformações internas no DoD. Em outubro de 2003, o Secretário de Defesa Donald Rumsfeld publica o *"Information Operations Roadmap"* — que foi classificado como secreto na época —, o qual advoga as OI como competências centrais das forças militares. O documento sugere uma definição de OI que passa a ser adotada como doutrina em todas as forças do DoD:

> The integrated employment of the core capabilities of electronic warfare, computer network operations, psychological operations, military deception, and operations security, in concert with specified supporting and related capabilities, to influence, disrupt, corrupt or usurp adversarial human and automated decision making while protecting our own. (DEPARTMENT OF DEFENSE, 2003, p. 11)

Vemos que, de fato, a definição de 2003 de OI incorpora toda a definição de C2W — que aparentemente nunca chegou a ter doutrina especificamente definida em documento público. Às capacidades que devem ser utilizadas integradamente para a realização de OI, agora também se soma o termo "operações em redes de computadores", que, em conjunto com "operações psicológicas", "enganação militar", entre outras operações, tem a função de "influenciar, interromper, corromper ou usurpar a tomada de decisão do adversário", seja essa realizada de forma humana ou automatizada. Aqui surge uma preocupação até então ausente e que será levada em conta mais tarde quando, em 2018 no JCOIE, o termo "ambiente

[46] Disponível em: https://history.defense.gov/Historical-Sources/Quadrennial-Defense-Review/. Acesso em: maio 2022.

informacional" será definido como formado das já mencionadas três dimensões (cognitiva, física e informacional), integrando pessoas e máquinas como alvos a serem influenciados: a possibilidade da automatização da tomada de decisão em situações militares, tanto por adversários quanto pelo próprio DoD. O termo "operações em redes de computadores", que também aparece pela primeira vez, também dá indícios de novas preocupações à vista, ligadas especificamente à utilização das redes de computadores para a disseminação de informação, assim como para sua proteção. Essa definição de OI será considerada a padrão para a doutrina militar nos EUA até o ano de 2012, quando o DoD publicará a *Joint Publication 3-13 Information Operations*, com uma nova definição de OI aplicável a todo o DoD:

> The integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own. Also called IO. (Approved for incorporation into JP 1-02 with JP 3-13 as the source JP.)

O DoD Dictionary, na versão de janeiro de 2021, mostra que essa definição ainda está vigente. Apesar da atual definição suprimir os termos "guerra eletrônica", "operações em redes de computadores", "operações psicológicas", "enganação militar" e "segurança de operações", assim como "tomada de decisão automatizada", em prol do já apresentado termo "*information-related capabilities*", o DoD Dictionary inclui o seguinte texto após o verbete information operations: "See also electromagnetic warfare; military deception; military information support operations; operations security. (JP 3-13)".

Fica evidente uma variação histórica do termo IO, que caminha para uma versão mais abrangente, discernindo agora adversários e potenciais adversários como alvos e envolvendo as "*information-related capabilities*" (IRC), as quais o DoD Dictionary define como "ferramentas, técnicas ou atividades empregadas em alguma dimensão do ambiente informacional que possam ser utilizadas para criar efeitos e condições operacionalmente desejáveis". Somos então remetidos de volta ao ambiente informacional, e um nó que liga os conceitos de "ambiente informacional" e de "operações de informação" é criado. Os conceitos se aproximam, pois ambos são relacionados à utilização de tecnologias físicas (de destruição física, guerra eletrônica e de operações em redes de computadores) e mentais (operações psicológicas e enganação militar), visando influenciar os comportamentos de adversários e

potenciais adversários (o que pode incluir atuais aliados). A doutrina militar atual agrupa tais atividades sob o termo *Information Related Capabilities* (IRC)[47].

Em 2016, o gabinete do Secretário de Defesa Ash Carter publica um novo *roadmap*, dessa vez intitulado *"DoD Strategy for Operations on Information Environment"*, visando estimular a preparação de todas as agências e contratados do DoD para a operação em ambiente informacional. Na abertura do documento, um texto assinado pelo Secretário relata que, com o advento da internet, a expansão das tecnologias da informação, a ampla disponibilidade de conectividade sem fio e os impactos profundos das redes sociais, atores estatais e não estatais estão utilizando-se do AI para "explorar, interromper e desabilitar sistemas de comando e controle e outras infraestruturas críticas; disseminar propaganda e desinformação; fomentar dissenso interno; recrutar e solicitar financiamento; promover legitimidade para suas ações tirando a legitimidade de outros.". O texto assinado pelo Secretário ressalta que a barreira de entrada para a condução de atividades no AI é baixa, o que estimula e facilita a ação desses atores adversários. Novamente, para os autores desse documento, o objetivo da execução de uma estratégia para a operação em ambiente informacional seria dar ao DoD a habilidade de afetar a tomada de decisão e o comportamento de adversários[48]. A estratégia expressa pelo DoD envolve integrar todo o governo dos EUA, de modo que todos os departamentos e agências que compõem a administração federal tenham os meios para agir de maneira conjunta contra adversários que atentem contra os "interesses nacionais" dos EUA utilizando-se das técnicas descritas pelo Secretário no texto de abertura. O documento *Department of Defense Strategy for Operating in the Information Environment*, estabelece diretamente uma ligação entre as operações em ambiente informacional e as information related capabilities, posicionando as últimas como as maneiras práticas de realizar operação no AI (DEPARTMENT OF DEFENSE, 2016, p.3).

Assim como na história relatada pela RAND, de uma batalha entre os conceitos de IO e C2W, parece haver um movimento em curso no DoD para que as operações em ambiente informacional englobem as agora antigas operações de informações. A disputa entre os conceitos é evidenciada no JCOIE, no qual a argumentação do texto toma rumos surpreendentemente epistemológicos: o texto diversas vezes reforça os fracassos recentes das operações político-militares estadunidenses em face das transformações apresentadas anteriormente. Como parte de um processo de racionalização dessas falhas, os autores

[47] Relatório GAO, p. 6
[48] DoD Strategy for Operation in the Information Environment (DoD, 2016)

propõem que os modelos lógicos e conceituais utilizados para embasar o raciocínio e a ação militar estariam errados até o momento. Falando sobre o modelo lógico que caracteriza o ambiente informacional pré-2018, que como vimos já estava presente na primeira definição de OI de 1996, os autores relatam que ele seria demasiadamente focado na transmissão de informações, com uma excessiva separação entre corpo e mente, entre pensamentos e mente e entre receptor e transmissor, o que privilegiaria a tomada de decisão dentro do DoD no sentido de que o controle da transmissão de informações seria a parte mais importante da conduta de OI (DEPARTMENT OF DEFENSE, 2018, p. 3). O manual JCOIE também declara a inadequação da interpretação corrente até então, a qual separava estritamente aspectos cognitivos, informacionais e físicos do ambiente informacional, representada na Imagem 9 abaixo. A imagem evidencia tanto a separação desses três componentes do AI — representados como nuvens distintas flutuando em uma nuvem maior — quanto o próprio privilégio da ideia de controle informacional — representado na imagem como as setas que interligam as nuvens, que se quebradas separam os elos do AI. Segundo o manual, tal modelo lógico teria sido criado com a finalidade de dar suporte às questões percebidas como mais importantes e urgentes pelos comandante militares de meados dos anos 90: a questão do compartilhamento interno de informações no DoD, a questão da garantia do funcionamento pleno da cadeia de comando e controle e, por fim, a questão da disrupção do fluxo de informações dos inimigos.

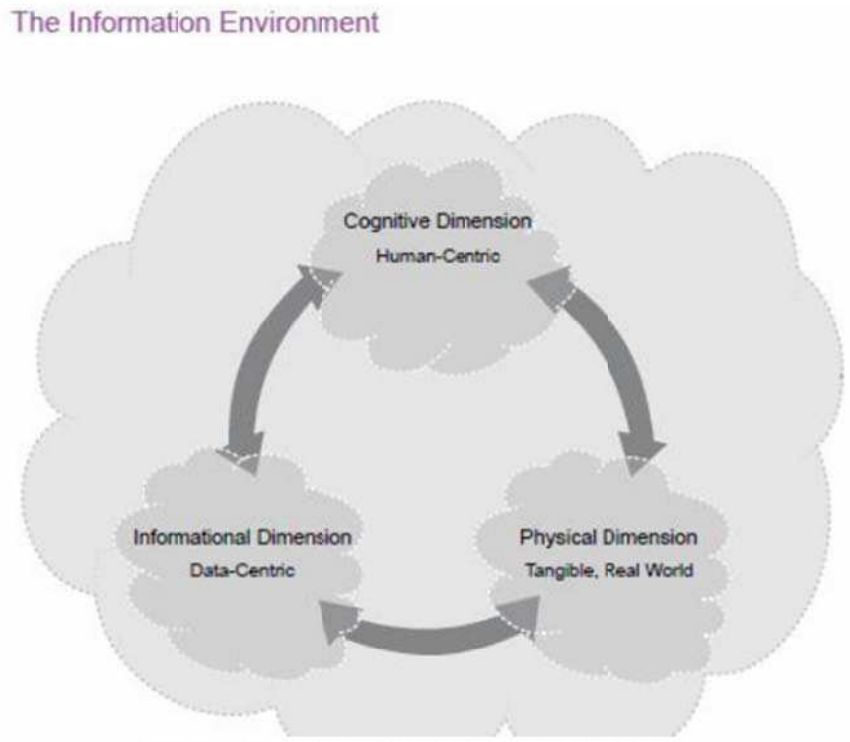


Figure 1: The Information Environment

Imagem 5 - Modelo de ambiente informacional que, segundo o manual JCOIE, privilegia a ideia de controle das transmissões de informação (Fonte: DEPARTMENT OF DEFENSE, 2018)

Voltando ao manual JCOIE e a sua crítica ao modelo de ambiente informacional vigente entre os anos 90 e 2010, que é denominado como "centrado em transmissão", os autores sugerem o desenvolvimento e a adoção de um novo modelo lógico de ambiente informacional, com o objetivo de incorporar à nova lógica os entendimentos e desenvolvimentos relacionados às novas tecnologias digitais, formas de comunicação e redes sociais, assim como a utilização destes para a contestação da ordem e das normas. Enquanto o antigo modelo se baseia no tripé: compartilhamento interno de informações no DoD, garantia do funcionamento pleno da cadeia de C2 e disrupção do fluxo de informações dos inimigos; o novo modelo baseia-se em pensar como "audiências com visões de mundo distintas interpretam e contextualizam informação" (DEPARTMENT OF DEFENSE, 2018, p. 3), uma mudança extraordinária e que como veremos pode ter imensas repercussões, sendo uma das mais importantes a possibilidade já esboçada na subseção anterior de uma necessidade urgente expressa pelo DoD de aproximar as ciências comportamentais às atividades militares. A principal proposta por trás do novo modelo logico de AI é o posicionamento das forças de

segurança dos EUA como atores prioritariamente comunicacionais. Em outras palavras, parece haver no novo conceito de AI a tentativa de estabelecimento de um novo mandato para o DoD: o policiamento ge ral das comunicações.

No próximo capítulo destrincho o que são as *Information Related Capabilities* através, principalmente, do manual *JP 3-13 Information Operations*, também emitido pelo JCS, e como são conduzidas as operações que envolvem a IRCs (operações de informação). Além disso, trago breves relatos históricos relacionados a casos em que as atividades hoje conhecidas como IRCs foram utilizadas.

CAPÍTULO 2 - Information related capabilities: da guerra fria aos anos 90

Como vimos no último capítulo, o Departamento de Defesa dos EUA está desde o ano de 2016 implementando oficialmente o conceito de "operação em ambiente informacional" em todas as forças militares sob seu guarda-chuva, com as chamadas *Information Related Capabilities* (IRCs) sendo adotadas como métodos —- formas sistematizadas de ação — para tal operacionalização. Neste capítulo voltamos aos manuais militares, destrinchando como os militares definem as principais IRCs — enganação militar (MILDEC); operações psicológicas (PYSOPS) / *military information support operations* (MISO); segurança operacional (OPSEC); e operações em redes de computadores (CNO) — que são consideradas pelos militares atividades básicas de inteligência militar, sendo conhecidas anteriormente como "operações de informação". As definições serão complementadas com exemplos da história recente das forças militares estadunidenses relacionados às operações que envolveram as principais IRCs, com a finalidade de caracterizar a tentativa recente do DoD de estabelecer o "ambiente informacional" como um ambiente de trabalho de toda força de segurança contemporânea.

As principais IRCs

No prefácio de um dos principais livros sobre a doutrina militar de operações de informação, o Professor Doutor Dan Kuehl, da National Defense University defende que:

> This new battlespace [the information environment] is focused on the "wetware", the "grey matter" of the brain in which opinions are formed and decisions made. The most – perhaps only – effective weapon in this battlespace is information, and the hallmarks of the information revolution, such as transparency of events and the global immediacy of coverage, have only heightened the importance and impact of Information Operations. (ARMISTEAD, 2004, p. 4).

Ecoando tais termos e relações, é possível encontrar no manual definidor da doutrina atual de operações de informação (JP 3-13) a seguinte enxuta definição de operações de informação, assim como uma breve explicação da relação delas com as IRCs:

> The Secretary of Defense now characterizes IO as the integrated employment, during military operations, of IRCs in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision making of adversaries and potential adversaries while protecting our own. (DEPARTMENT OF DEFENSE, 2012, p.vii).

Nesse resumo oficial, além de situar os esforços das IRCs e das operações de informação na alteração e influência sobre o processo decisório humano, observa-se o estabelecimento de uma clivagem entre operações de informação ofensivas, chamadas pelos militares de "operações de projeção de informação", e operações de informação defensivas, chamadas de "operações de proteção de informação" (ARMISTEAD, 2004, p. 2). Para os vários militares autores do já citado influente livro sobre a doutrina de IO, o desafio que orientaria as operações de *information projection* seria o policiamento e formatação da rede de computadores e sistemas que hoje forma a internet (ARMISTEAD, 2004, p. 39), enquanto as operações de *information protection* teriam como objetivo a proteção do funcionamento — agora digital e computadorizado — das "burocracias modernas" (ARMISTEAD, 2004, p.61).

No manual JP 3-13 (DEPARTMENT OF DEFENSE, 2012, p.viii) encontramos uma definição que converge com a vista anteriormente de ambiente operacional: constituído de três dimensões interdependentes e interconectadas, sendo essas as dimensões física, informacional e cognitiva. As operações de informação englobam, portanto, operações defensivas e ofensivas em todas as três dimensões do ambiente informacional. Algumas dessas operações são realizadas em computadores, celulares, cabos e outros itens de infraestrutura, outras em dados digitais propriamente ditos — protegendo-os e/ou analisando-os —, e outras, ainda, são realizadas nas mentes de seus alvos:

> IRCs are the tools, techniques, or activities that affect any of the three dimensions of the information environment. The joint force (means) employs IRCs (ways) to affect the information provided to or disseminated from the target audience (TA) in the physical and informational dimensions of the information environment to affect decision making and ultimately the adversary actions in the physical dimension. (DEPARTMENT OF DEFENSE, 2012, p.viii)

Como muitos — talvez todos — os manuais consultados, o manual JP 3-13 se refere às capacidades dos inimigos como justificativa para o desenvolvimentos das próprias capacidades do DoD na área de IO:

> The nation's state and non-state adversaries are equally aware of the significance of this new technology, and will use information-related capabilities (IRCs) to gain advantages in the information environment, just as they would use more traditional military technologies to gain advantages in other operational environments. (DEPARTMENT OF DEFENSE, 2012, p. vii)

É possível perceber uma analogia explícita entre o ambiente informacional e um campo de batalha tradicional. O trecho acima evidencia que o *Joint Chiefs of Staff* e o

Departamento de Defesa como um todo creem que, no campo de batalha informacional, há uma equalização em termos de importância das ameaças aventadas pelos adversários estatais e não-estatais dos EUA. De maneira convergente com as lógicas manifestas nos vários documentos analisados neste trabalho, os militares estadunidenses preconizam uma imagem atual de adversário como indivíduos e/ou grupos muito sofisticados ideológica e tecnologicamente, além de bem versados nos vários aspectos do ambiente digital. Tal inimigo é caracterizado inclusive como constituído de redes de relações complexas, e o Departamento de Defesa prepara-se para o presente e para o futuro com base nessa imagem de inimigo.

O documento JCOIE apresenta como solução para a atuação nas três dimensões do ambiente informacional o conceito de "operações globais integradas", e lista cinco IRCs essenciais para a operação das forças militares em ambiente informacional no âmbito da segurança e defesa.

Sobre as operações globais integradas, o manual declara que o novo cenário de problemas enfrentados pelo DoD só pode ser resolvido com uma abordagem integralmente global, o que implica no estabelecimento de alianças entre o governo dos EUA e organizações diversas como think tanks, empresas estadunidenses operando fora dos EUA, ONGs, assim como movimentos "cívicos" e outros, conforme a necessidade da operação:

> Globally integrated operations require a Joint Force that is postured to quickly combine capabilities with itself and mission partners across domains, echelons, geographic boundaries, and organizational affiliations. Globally integrated operations take place within a global IE. (DEPARTMENT OF DEFENSE, 2018, p. 2).

De maneira convergente com o manual JP 3-13, no JCOIE as atividades que dão suporte às "operações globais integradas" são as *Information Related Capabilities* (IRCs). As IRCs, não por coincidência, são exatamente as atividades que, como vimos, participaram das diversas definições de operações de informação ao longo da história do termo. As atividades listadas como as principais IRCs são: operações em redes de computadores — *computer network operations* (CNO), que incluem como subáreas o ataque de redes, a defesa de redes e a exploração de vulnerabilidades em redes; operações psicológicas — *psychological operations* (PSYOP); operações no espectro eletromagnético — *electromagnetic spectrum operations* (EMSO); segurança de operações — *operational security* (OPSEC); e a enganação militar — *military deception* (MILDEC).

É no já mencionado manual *JP 3-13 Information Operations* que encontramos as definições mais recentes[49] para as *Information Related Capabilities*. Destinado tanto a comandantes militares quanto a soldados que venham a participar de ações que envolvam IRCs, um exemplo de situação retratada no manual (JP 3-13, p. 27, II-3) chama particular atenção por mostrar o que seria um caso modelo de aplicação de OI e IRCs. Nesse exemplo, um "movimento adversário dos EUA" tenta derrubar o governo de um país. O movimento utiliza-se de "meios letais e não letais" para demonstrar que o "governo não está apto a defender e manter o seu povo" e, assim, enfraquecer o governo. Na simulação, o DoD — atuando em conjunto com outras agências do governo dos EUA e "parceiros interorganizacionais" — adotaria uma estratégia de mitigação da efetividade do adversário, através do emprego de IRCs, como a enganação militar, operações psicológicas, operações no ciberespaço, diplomacia, relações públicas e suporte militar convencional associado a outras IRCs. O texto não menciona uma requisição de ajuda por parte do governo ameaçado pelos subversivos; o que fica explícito é que o governo "aliado" pode cooperar ou não na ação, que ocorrerá com ou sem consentimento. O texto indica que, no caso padrão, o DoD e o governo dos EUA avaliariam a situação e decidiriam que o futuro do governo "aliado" é importante demais para não estar sob coordenação direta político-militar do governo dos EUA.

Como em um jogo de estratégia de videogame, o manual atribui ao comandante das forças envolvidas o seu objetivo: "Proteger o governo do país X, impedindo sua derrubada". Para impedir a derrubada do governo "aliado" do país X, o manual diz que o comandante precisa obter dois efeitos desejados finais: 1. "Que os cidadãos do país X tenham confiança na habilidade do governo de dar suporte e proteger seus cidadãos"; e 2. "Que o adversário seja incapaz de derrubar o governo do país X". O manual define as lideranças adversárias e a população do país X — incluindo explicitamente amigos, neutros e potenciais adversários — como "audiência alvo". Entre os recursos listados para ajudar os aliados estão: ação diplomática; comunicação estratégica; mídia; forças militares empregadas em combate; coleta de informações; relações públicas; invasão de redes de computadores e enganação; sanções econômicas contra os adversários; e injeções de capital no país. Ao final, a conclusão do exemplo indica que todos esses recursos se encontram à disposição do Comandante em questão e que todos podem ser utilizados, sendo observado que o que os torna realmente poderosos seria a eficiência na aplicação de cada meio. Para avaliar a eficiência de cada recurso, o manual propõe um sistema (JP 3-13, p. 51, IV-8) que gera, a partir de uma

[49] Verbete: "Information Operations" (JOINT CHIEFS OF STAFF, 2022; JP 3-13, 2014)

avaliação qualitativa da situação de conflito, dados quantitativos que são usados pelos altos escalões militares para comparar e medir a efetividade de suas ações.

Digamos, então, que um Comandante tenha particular fé na utilização de IRCs como maneira de se travar conflitos na atualidade. No que consistem as principais opções de IRCs que envolvem a informação digital e que devem, segundo o DoD, estar à disposição dos comandantes?

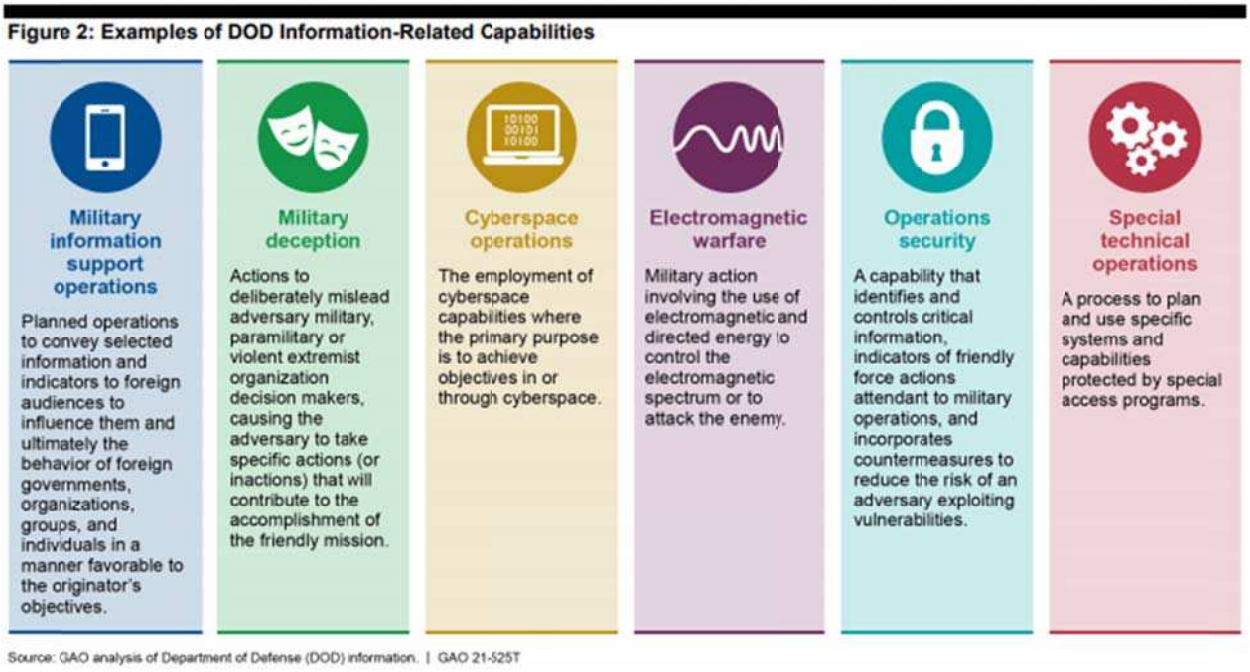


Imagem 6 - Principais Information Related Capabilities, como listadas no DoD *Strategy for Operating in the Information Environment* de 2016 (Fonte: GAO Report)[50].

Computer Network Operations (CNO) são operações que envolvem defender os computadores e redes de computadores envolvidos no esforço político-militar aliado, e invadir, assim como monitorar e possivelmente controlar, os computadores, redes e celulares utilizados pelos adversários e potenciais adversários[51]. Tais operações tem como objetivo mapear a infraestrutura comunicacional dos adversários e permitir que seja coletada a maior quantidade de dados sobre determinado alvo.

[50] Ver mais em: https://www.gao.gov/assets/gao-21-525t.pdf. Acesso em: 10 nov. 2021.
[51] JP 3-13 GL-1 (DEPARTMENT OF DEFENSE, 2014)

Segundo documentos vazados por Snowden em 2014, a "comunidade de inteligência"[52] dos EUA conta com acesso a uma plataforma conhecida como XKEYSCORE, que, segundo slides[53], é capaz de acessar e-mails de qualquer endereço de e-mail, históricos de navegação de qualquer computador, traçar relações entre *accounts* em diferentes sites para criar uma ficha policial online unificada dos alvos e mapear fisicamente onde o alvo se localiza com base nos seus aparelhos digitais de comunicação. Uma atividade como a antiga "busca de informações", que os militares brasileiros utilizaram durante o regime militar e que foi detalhada no "Bagulhão"[54], agora pode ser conduzida em parte digitalmente, por meio de sistemas como o XKEYSCORE. Se no passado as principais formas de obtenção de informações foram o interrogatório sob tortura, ou a utilização de informações provenientes de fontes não voluntárias, agora seria possível seguir passo a passo os movimentos físicos e ações online de todas as pessoas próximas a qualquer suspeito de ser adversário das forças de segurança contemporâneas. Segundo o ex-chefe da NSA, hoje executivo da Amazon, General Keith Alexander[55], não precisamos nos preocupar com nada, pois os sistemas não coletam dados ilegais e só são acessíveis para membros da comunidade de inteligência com as

---

[52] Como no caso do Brasil, nos EUA também há uma designação coletiva que engloba todas as agências, empresas e indivíduos que colaboram com os esforços de inteligência voltados à segurança nacional: "intelligence community — All departments or agencies of a government that are concerned with intelligence activity, either in an oversight, managerial, support, or participatory role. Also called IC. (JP 2-0)" (JOINT CHIEFS OF STAFF, p. 107, 2022).

[53] Ver, por exemplo: https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASH015a/aeed7b88.dir/doc.pdf ou https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASH017d/5ff5ccff.dir/doc.pdf Acesso em: 10 nov. 2021.

[54] O Bagulhão foi o primeiro documento que denunciou a utilização sistemática da tortura como ferramenta principal do regime militar para a obtenção do controle político. O documento, destinado ao Presidente da OAB e ao Cardeal Dom Paulo Evaristo Arns, foi escrito em 1971 em colaboração com os presos políticos no Presídio Barro Branco da Justiça Militar, e é organizado em três eixos, dando materialidade à operação da polícia secreta do regime militar brasileiro. Na primeira parte do documento são descritos alguns dos modos como os militares "buscam informações": são listadas formas de abordagem, uma dezena ou mais de formas de tortura, além de serem descritos e indicados os locais onde a tortura ocorria. Na segunda parte do documento são relatadas práticas dos órgãos de segurança utilizadas para distorcer e manipular a aplicação da lei. São listadas dezenas de nomes de policiais, militares, escrivães e médicos — torturadores e cúmplices. Os relatos de práticas abusivas e ilegais vão desde a violência desmedida e abuso psicológico no momento da prisão, passando pela incomunicabilidade do preso, a execução de exames falsos de corpo delito, a autenticação em cartório de depoimentos falsos obtidos sob tortura — inclusive com tortura e abuso sexual de familiares e crianças —, a convocação de testemunhas falsas, a prática de juízes de desconsiderar a palavra do preso e de supervalorizar a palavra dos agentes das forças de segurança, a ocultação da identidade dos agentes, etc. A lista de práticas irregulares é extensa e abrange todas as etapas e esferas da execução da lei. A terceira e última parte do documento compila detalhes de dezenas de casos de presos políticos mortos sob tortura. Estava assim revelado, pela primeira vez em detalhes e com nomes, o funcionamento do aparato de controle político-militar do regime que duraria formalmente de 1964 a 1985.

[55] Ver mais em: https://www.newyorker.com/news/news-desk/were-at-greater-risk-q-a-with-general-keith-alexander Acesso em: 10 nov. 2021.

credenciais necessárias. Maiores explicações oficiais não foram dadas e não parece haver uma perspectiva de mudança de atitude quanto a isso no horizonte político estadunidense.

Electromagnetic Spectrum Operations (EMSO) é uma IRC que se associa fortemente a *Computer Network Operations*, pois, enquanto CNO trata de coletar e controlar dados digitais que circulam entre computadores, EMSO trata de coletar e analisar dados de outros tipo de dispositivos que operam no espectro eletromagnético, como sinais de rádio, radar, telefone, satélite, transmissões de TV, sinais analógicos em cabos submarinos e escutas ambientais[56]. Com a soma dos dados obtidos por CNO e por EMSO, é possível criar um retrato digital parcial (por meio de modos de visualização, como mapas, áudios, tabelas, dashboards, relatórios, imagens e vídeos) do que o DoD chama de "*security environment*", destinado a ser consumido pelos comandantes militares.

As próximas três IRCs, *Psychological Operations* (PSYOPS) / *Military Information Support Operations* (MISO), *Operational Security* (OPSEC) e *Military Deception* (MILDEC), são algumas das maneiras de se utilizar as informações coletadas por CNO e EMSO, para além dos relatórios internos destinados aos comandantes. A prática de PSYOPS/MISO, OPSEC e MILDEC também são motivos muito razoáveis para se duvidar da afirmação da NSA sobre a segurança e ética dos seus programas de coleta e processamento de dados.

PSYOPS, também nomeadas de *Military Information Support Operations* (MISO), se referem a operações que visam

> to convey selected information and indicators to audiences to influence their emotions, motives, and objective reasoning, and ultimately the behavior of governments, organizations, groups, and individuals. (JP 3-13, Anexo 2, p. GL-1)

Modos de fazer isso seriam todos os que pudessem apelar para os instintos e vontades das "audiências alvo", fazendo os alvos orientarem suas ações de maneira simpática aos anseios dos comandantes militares. Espalhar notícias criadas com finalidades políticas específicas; criar armadilhas a fim de gravar líderes políticos, funcionários públicos e adversários, em geral, em situações comprometedoras; ridicularizar e difamar adversários pública e privadamente; utilizar informações coletadas por CNO ou EMSO para chantagem, são alguns dos meios mais comuns de operações psicológicas. Nesse sentido, tanto os

[56] JP 3-85 Electromagnetic Spectrum Operations (Gl-1) (DEPARTMENT OF DEFENSE, 2020. Gl-1).

manuais da EdA como diversos eventos históricos[57] apontam para a utilização comum e rotineira de todas essas técnicas pelos órgãos de inteligência.

Military Deception (MILDEC) é a IRC que utiliza a "arte da enganação" como auxiliar para as operações militares em geral e para as operações em ambiente informacional em específico. Segundo o manual que define a doutrina de MILDEC (anexo 1 do manual *JP 3-13 Information Operations*), a enganação militar seria composta de:

> actions executed to deliberately mislead adversary military, paramilitary, or violent extremist organization (VEO) decision makers, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly mission.

MILDEC inclui o uso ativo da negação de informações ao adversário, por exemplo conduzindo operações com identidades falsas ou ataques físicos ou online sob outra identidade ou IP, visando incriminar outro indivíduo ou grupo pelas ações executadas. MILDEC se funde com a IRC *Operational Security* OPSEC, pois a segurança operacional se refere a ações que devem ser tomadas para que as forças de segurança executem suas missões com sucesso, sem baixas, prisões ou responsabilizações legal posteriores de qualquer aliado envolvido. Lendo os manuais, MILDEC e OPSEC parecem ser projetadas para garantir a impossibilidade de monitoramento da atividade militar por civis. Acredito que essas três IRCs (PYSOPS, MILDEC, OPSEC) combinadas com a gigantesca quantidade de informações sobre tudo e todos — as quais são coletadas pelos esforços de inteligência estadunidenses através das duas outras IRCs (CNO e EMSO) — têm o potencial real de ser as ferramentas básicas para a construção de um estado policial digital, o que parece ser a intenção dos autores dos documentos analisados.

Como utilizar IRCs: O *Information and Influence Framework* (IIF)

Para escolher como e quais IRCs devem ser utilizadas em quais situações, o DoD propõe que suas forças operacionalizem o chamado *Information and Influence Framework* (IIF), framework que sistematiza o processo de tomada de decisões a respeito da utilização das IRCs para alcançar os objetivos dos comandantes. O IIF utiliza as IRCs como maneiras de coletar, processar e disseminar informação até as audiências-alvo — *target audiences* (TA), sendo essas compostas dos "individual[s] or group[s] selected for influence and can be allies,

[57] Verificar, por exemplo, o episódio Pentagon Papers no auge da Guerra do Vietnã.

multinational partners, adversaries, or potential adversaries" (DEPARTMENT OF DEFENSE, 2012, p. I-3). Tais audiências são classificadas conforme o framework em "allies, neutrals, adversaries, or potential adversaries" (DEPARTMENT OF DEFENSE, 2012, p. I-5) e o processo de classificação de um indivíduo ou grupo em qualquer uma dessas categorias faz parte dos objetivos do próprio IIF. O IIF pode ser aplicado contra aliados e adversários e inclusive sua aplicação pode resultar na recategorização de um aliado como potencial adversário, o que poderia, por exemplo, levar ao monitoramento de inteligência no ambiente informacional de membros do próprio governo e das forças de segurança.

A aplicação do IIF tem o objetivo principal de influenciar as TAs, sendo estas compostas de humanos ou sistemas:

> The purpose of integrating the employment of IRCs is to influence a TA. While the behavior of individuals and groups, as human social entities, are principally governed by rules, norms, and beliefs, the behaviors of systems principally reside within the physical and informational dimensions and are governed only by rules. Under this construct, rules, norms, and beliefs are:
> (1) Rules. Explicit regulative processes such as policies, laws, inspection routines, or incentives. Rules function as a coercive regulator of behavior and are dependent upon the imposing entity's ability to enforce them.
> (2) Norms. Regulative mechanisms accepted by the social collective. Norms are enforced by normative mechanisms within the organization and are not strictly dependent upon law or regulation.
> (3) Beliefs. The collective perception of fundamental truths governing behavior. The adherence to accepted and shared beliefs by members of a social system will likely persist and be difficult to change over time. Strong beliefs about determinant factors (i.e., security, survival, or honor) are likely to cause a social entity or group to accept rules and norms. (DEPARTMENT OF DEFENSE, 2012, p. I-5).

É possível observar como através da abordagem que integra "regras", "normas" e "crenças", os militares eliminam as barreiras entre humanos e sistemas, de modo que o IIF funciona independentemente do alvo a ser influenciado, seja esse uma máquina que controla um sistema de radares ou um sistema bancário na China, um militar do próprio governo dos EUA, um funcionário de uma emissora de televisão estadunidense operando no estrangeiro ou um grupo de usuários do Facebook.

Identificada a TA a partir da interpretação das ordens dos comandantes ou através da análise de informações prévias de inteligência (DEPARTMENT OF DEFENSE, 2012, p. IV-3), é realizada uma análise pela equipe de OI de modo que as "regras", "normas" e "crenças" que mobilizam a "percepção do ambiente" pela audiência alvo sejam descritas em relatórios padronizados. Os relatórios serão utilizados para que os militares encontrem "pontos de entrada" efetivos para se obter influência sobre os alvos. As IRCs — como a

invasão de computadores ou uma operação de chantagem de um funcionário — serão então integradamente aplicadas em atores nomeados "influenciadores chave", "audiências de massa" e "populações vulneráveis", através dos pontos de entrada avaliados como potencialmente efetivos pela equipe de OI:

> Such means may include (but are not limited to) diplomatic, informational, military, or economic actions, as well as academic, commercial, religious, or ethnic pronouncements. (DEPARTMENT OF DEFENSE, 2012, p. I-5).

A ideia é que a ação militar crie um *loop* entre as percepções desses três tipos de atores que compõem a TA, afetando o ambiente informacional como um todo — em suas dimensões cognitiva, informacional e física —, de modo a garantir o controle da AI pela equipe de OI, pelo menos em relação à percepção das TA em questões interseccionadas aos objetivos militares:

> Influencing the behavior of TAs requires producing effects in ways that modify rules, norms, or beliefs. Effects can be created by means (e.g., governmental, academic, cultural, and private enterprise) using specific ways (i.e., IRCs) to affect how the TAs collect, process, perceive, disseminate, and act (or do not act) on information. (DEPARTMENT OF DEFENSE, 2012, p. I-5).

Tal processo é ilustrado na imagem abaixo:

P

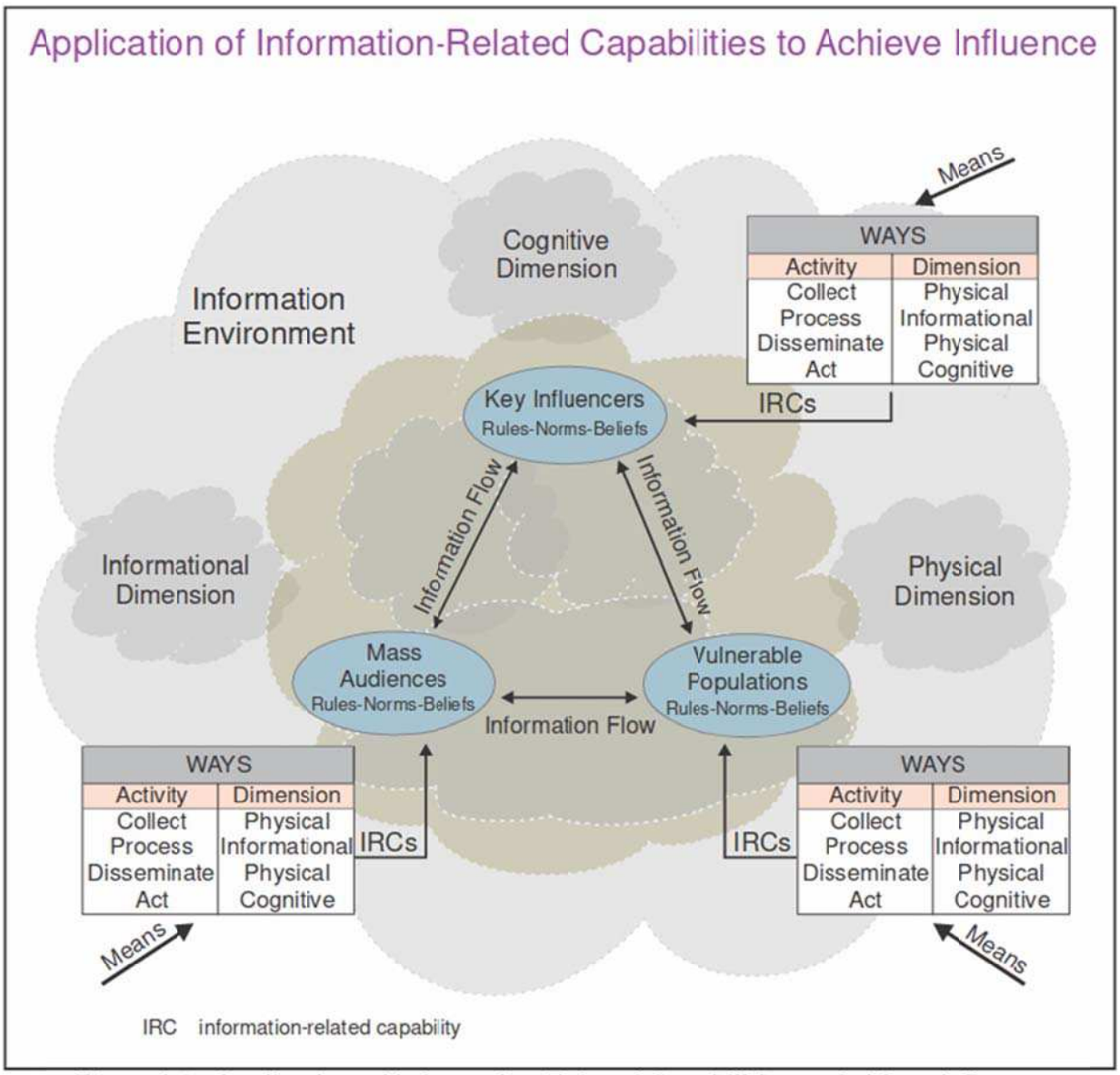


Figure I-4. Application of Information-Related Capabilities to Achieve Influence

Imagem 7 - Diagrama que ilustra o processo de aplicação de IRCs para obter influência sobre humanos e sistemas (DEPARTMENT OF DEFENSE, 2012, p. I-7).

Quem executa operações de informação: a célula de OI

Para a execução de OI, o DoD estipula a criação de uma "célula de OI" dentro da unidade militar que executará a ação[58], sendo esta composta por especialistas em todas as IRCs — as principais delas descritas na primeira seção deste capítulo. Os especialistas necessários[59] são provenientes das áreas de contrainteligência, enganação militar (MILDEC), segurança operacional (OPSEC), operações em redes de computadores (CNO), operações especiais, serviços e suporte legal, *public affairs* (PA), relações civis-militares e operações em espectro eletromagnético (EMSO), como pode ser visto na Imagem 8 abaixo.

[58] O manual JP 3-13 nota que não existem requisitos legais formais para o estabelecimento de uma equipe de OI, estando sua formação à discrição do comandante militar responsável pela execução de uma missão que ele considere ser uma OI (DEPARTMENT OF DEFENSE, 2012, p. III-1).

[59] Lembrando que esses funcionários podem ter origem militar, *contractor* ou indicação política civil, como descrito no início do capítulo 1.

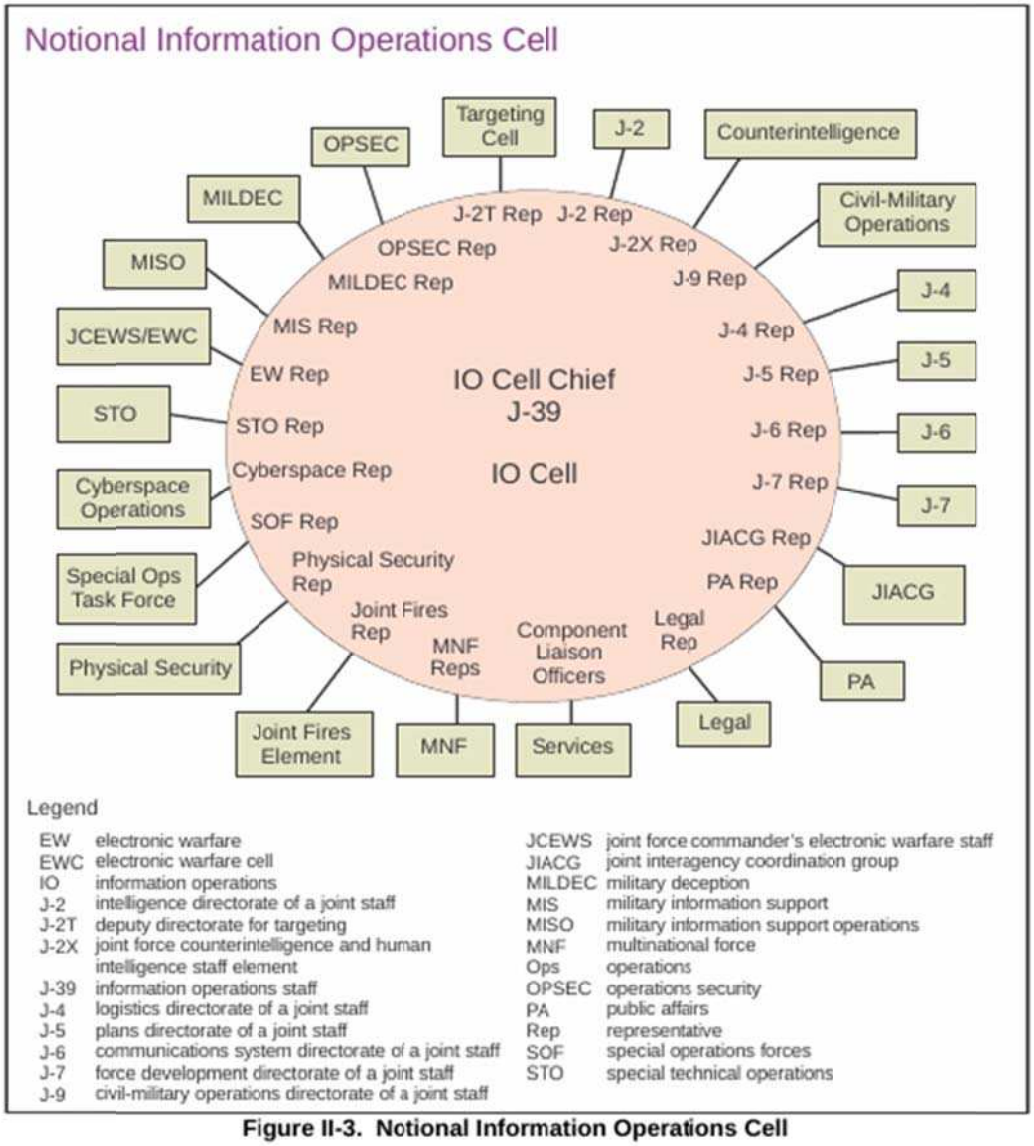


Figure II-3. Notional Information Operations Cell

Imagem 8 - Componentes básicos de uma célula de operações de informação, como proposto no manual *JP 3-13 Information Operations*. Notar as várias IRCs mencionadas.

O manual JP3-13[60] dá ênfase ao fato de as OI serem realizadas primariamente em um contexto que integra diferentes agências (DEPARTMENT OF DEFENSE, 2012, p. ix, II-2, IV-11) nas quais os militares executam a operação que, por sua vez, foi concebida a partir de demandas que podem vir de fora do aparato militar, ou seja, dentro das porções civis do governo dos EUA. Tal cooperação interagência, assim como a preparação de operações de informação em geral, exige a criação de um grupo de coordenação chamado de *Joint Interagency Coordination Group* (JICG). O JICG é essencial para a execução de ações conjuntas entre órgãos militares e civis, e pode incluir representantes de empresas privadas e

[60] Assim como o JCOIE (DEPARTMENT OF DEFENSE, 2018, p. iii, 21, 37).

ONGs, a fim de utilizar todas as possibilidades de pressão possíveis disponíveis aos comandantes de OI:

> Interagency coordination occurs between DOD and other USG departments and agencies, as well as with private-sector entities, nongovernmental organizations, and critical infrastructure activities, for the purpose of accomplishing national objectives. Many of these objectives require the combined and coordinated use of the diplomatic, informational, military, and economic instruments of national power[61]. (DEPARTMENT OF DEFENSE, 2012, p. II-7).

Os mencionados "instrumentos de poder nacional" são construtos utilizados pelo DoD para estender o seu alcance e potencial de operação para todo o mundo, caso surjam situações relacionadas ao governo e aos empresários dos EUA:

> The instruments of national power (diplomatic, informational, military, and economic) provide leaders in the United States with the means and ways of dealing with crises around the world. (DEPARTMENT OF DEFENSE, 2012, p. I-1).

> instruments of national power — All of the means available to the government in its pursuit of national objectives. They are expressed as diplomatic, economic, informational and military. (JP 1) (JOINT CHIEFS OF STAFF, 2022, p. 112).

A Imagem 9 abaixo resume algumas organizações que requerem aos militares auxílio para a realização de OI (Departamento de Estado, Departamento do Tesouro, a agência USAID[62], Departamento de Comércio, Departamento de Saúde e Serviços Humanos, Departamento de Justiça, Departamento de Defesa, assim como a Casa Branca). Tal combinação de agências — que passa por órgãos responsáveis por assuntos relacionados desde o comércio até assuntos relacionados à saúde — evidencia novamente o amplo escopo que pode assumir as operações de informação, assim como a disparidade e multiplicidade de seus objetivos. As funções principais do grupo de coordenação interagências são:

> Participate in combatant command security cooperation, contingency, crisis, and transition planning; Advise on civilian agency planning efforts; Work military civilian operational issues; Present civilian agency perspectives, approaches, capabilities, and limitations; Provide habitual links to interagency, regional, and international planners; Arrange interface on interagency activities Coordinate with regional players. (DEPARTMENT OF DEFENSE, 2012, p. II-8).

---

[61] The instruments of national power (diplomatic, informational, military, and economic) provide leaders in the United States with the means and ways of dealing with crises around the world. (DEPARTMENT OF DEFENSE, 2012, p. I-1)

[62] A *US Agency for International Development* é uma agência voltada ao financiamento de projetos de infraestrutura fora dos EUA, principalmente em estados do terceiro mundo em que os EUA têm interesses políticos ou econômicos fortes. A USAID é conhecida por funcionar como parte do aparato de inteligência dos EUA, financiando grupos cívicos "liberais" e "conservadores" "pró-democracia" pelo mundo todo (BUTLER; GILLUM; ALBERTO ARCE, 2021) (IGOE, 2019).

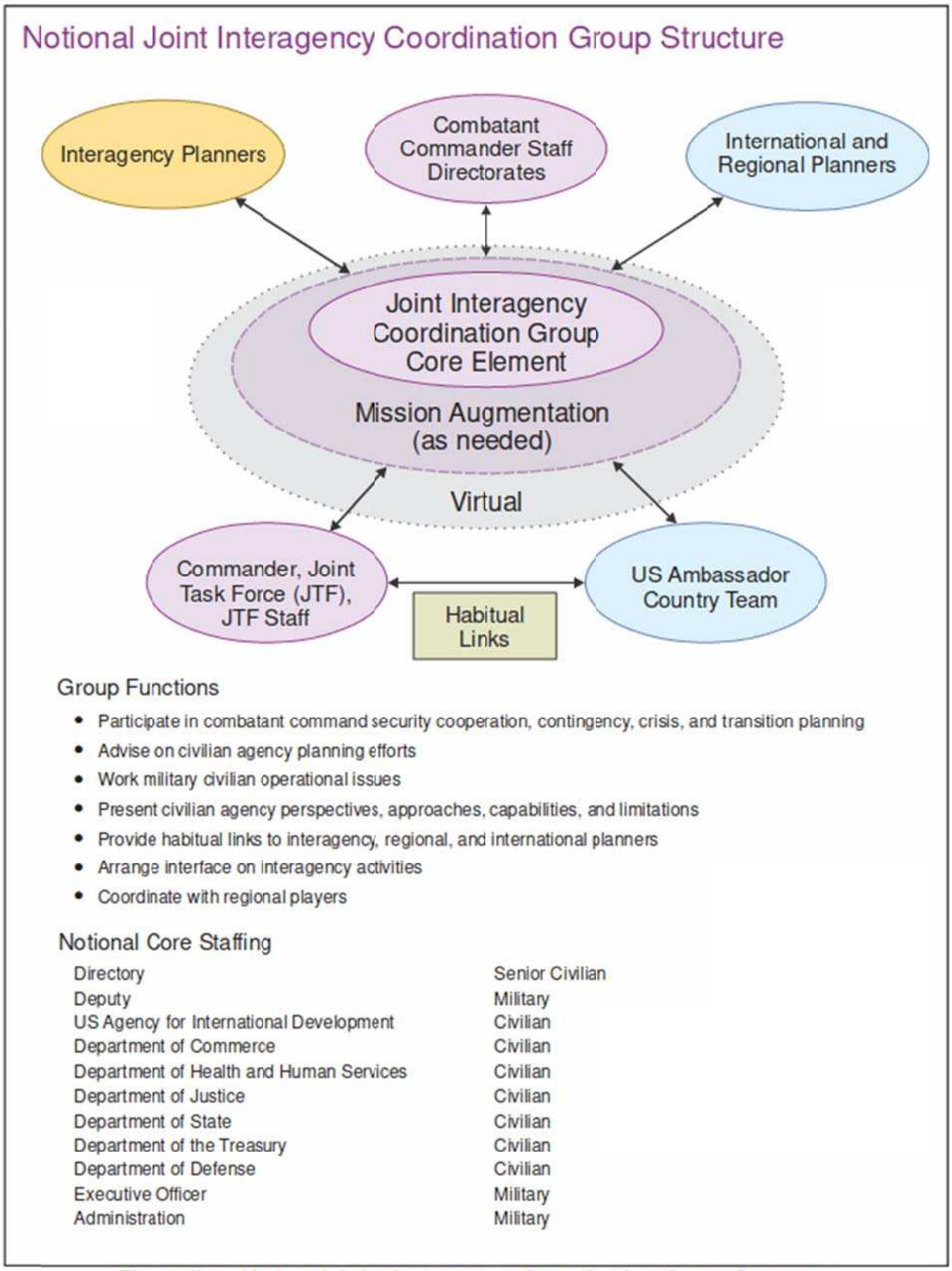


Figure II-4. Notional Joint Interagency Coordination Group Structure

Imagem 9 - Estrutura proposta pelo manual JP 3-13 para a coordenação de OI no caso de operações executadas em contexto interagências (em conjunto com órgãos civis do governo dos EUA). (Fonte: DEPARTMENT OF DEFENSE, 2012, p. II-8).

Vale a pena notar aqui que os manuais de acesso público podem conter partes classificadas como secretas, de modo que não é possível para nós observarmos de maneira totalmente transparente a estrutura proposta pelo DoD para a realização de operações de informação. Citando um exemplo de uma situação dessas, a IRC Operações em Redes de Computadores (CNO) foi secreta até o ano de 1998, não aparecendo nos manuais públicos de OI (ARMISTEAD, 2004, p. 62).

Como são planejadas e executadas operações de OI: a coordenação interagências e a imaginação do inimigo como etapas cruciais

O manual também apresenta um procedimento burocrático detalhado (Imagem 10) feito para ser seguido internamente pelas forças militares em todas as operações de informação (DEPARTMENT OF DEFENSE, 2012, p. IV-3).

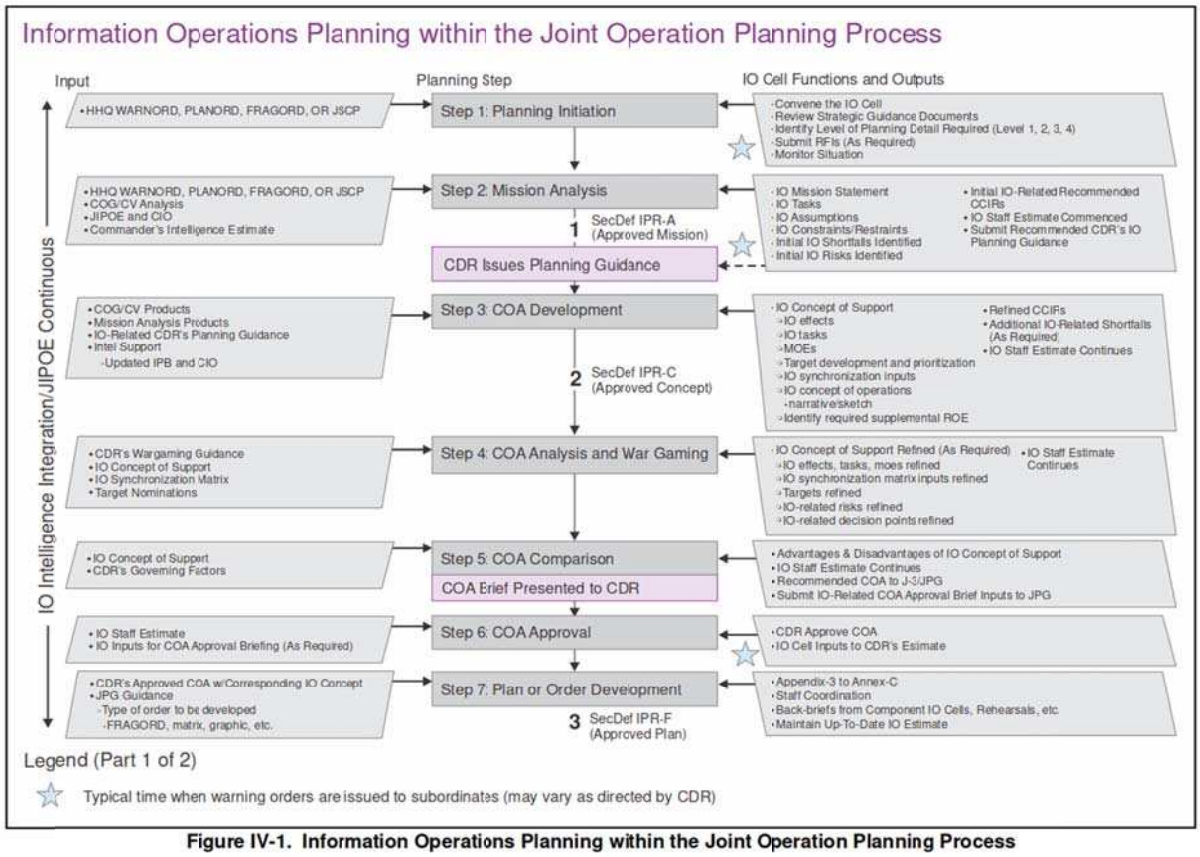


Figure IV-1. Information Operations Planning within the Joint Operation Planning Process

Imagem 10 - Diagrama que detalha etapa por etapa o processo de planejamento e acompanhamento inicial de uma operação de informação no DoD (Fonte: DEPARTMENT OF DEFENSE, 2012, p. IV-3).

O procedimento inicia-se na chamada "Etapa 1 - planejamento" através do recebimento em uma unidade militar[63] de uma ordem de execução de OI. Três tipo de ordem são aceitas: ordens provenientes de uma unidade hierarquicamente acima, as quais requerem a execução de uma operação[64]; ordens de criação de uma nova operação baseada nos desenvolvimentos de uma operação já em curso que necessita de novas ações e operações para sua continuidade[65]; ou ordens provenientes de planos estratégicos de longo prazo a serem realizados pelas forças militares[66]. As ordens podem ser tão específicas e militares, como "monitorar o comandante da unidade X inimiga", quanto gerais e políticas, como "alterar pesquisas eleitorais em um local X", ou, então, "garantir que tal governo aliado não caia".

Com a ordem de início de uma OI, o comandante da unidade, normalmente uma unidade de inteligência militar, ordena a formação de uma célula de OI. Para tanto, são reunidos os especialistas necessários; é realizada a revisão por parte desses profissionais dos guias de ação necessários[67]; são requisitadas as informações coletadas por outros órgãos, especialmente órgãos de inteligência militar[68]; e é executado o monitoramento preliminar da situação pela nova equipe de OI.

Para o início da segunda etapa, intitulada "Análise da missão", são necessários uma nova ordem superior definindo a continuidade da missão, um relatório da equipe de OI

---

[63] Qualquer uma que tenha capacidade e autonomia suficiente para juntar um time de OI como as seções de inteligência do exército ou da marinha, a *Defense Intelligence Agency* ou mesmo a *National Security Agency*.

[64] Chamadas de *warning orders* (WARNORDs) — ordens para o começo imediato de uma operação militar; e *planning orders* (PLANORDs), ordens de planejamento, destinadas a fazer com que a unidade militar em questão se planeje para a execução em breve de uma operação. Segundo o Dicionário de Termos Militares do DoD: "warning order — 1. A preliminary notice of an order or action that is to follow. 2. A planning directive that initiates the development and evaluation of military courses of action by a supported commander and requests that the supported commander submit a commander's estimate. 3. A planning directive that describes the situation, allocates forces and resources, establishes command relationships, provides other initial planning guidance, and initiates subordinate unit mission planning. Also called WARNORD. (JP 5-0)" (JOINT CHIEFS OF STAFF, 2022, p. 257) e "planning order — A planning directive that provides essential planning guidance and directs the initiation of execution planning before the directing authority approves a military course of action. Also called PLANORD. See also execution planning. (JP 5-0)" (JOINT CHIEFS OF STAFF, 2022, p. 186).

[65] Essas são as chamadas *fragmentary orders* (FRAGORD). Segundo o DTMA: "fragmentary order — An abbreviated form of an operation order issued as needed after an operation order to change or modify that order or to execute a branch or sequel to that order. Also called FRAGORD. (JP 5-0)" (JOINT CHIEFS OF STAFF, 2022, p. 94).

[66] Ordens provenientes de *Joint Strategic Capabilities Plans* (JSCP): "Joint Strategic Capabilities Plan — A plan that provides guidance to the combatant commanders and the Joint Chiefs of Staff to accomplish tasks and missions based on current military capabilities. Also called JSCP. See also combatant commander; joint. (JP 5-0)" (JOINT CHIEFS OF STAFF, 2022, p. 132).

[67] Como guias de regulação, manuais como os analisados neste trabalho ou planos estratégicos contendo diretivas de política externa.

[68] São as chamadas *Requests for Information* (RFIs), que abrangem informações como interceptações de dados de internet da *National Security Agency;* informações obtidas de fontes humanas da CIA; ou ainda imagens obtidas por satélite da *Geospatial Intelligence Agency*.

definindo as vulnerabilidades críticas[69] e os centros de gravidade[70] da missão e relatórios contendo as estimativas de inteligência[71] do comandante e da seção de inteligência sobre a missão[72]. Nesse momento serão formalizados em relatórios orais ou escritos um sumário descritivo da missão, as tarefas gerais ligadas às IRCs a serem utilizadas, as suposições da equipe de OI sobre as tarefas, uma identificação dos obstáculos e possíveis limitações à ação militar, os riscos identificados decorrentes das implementações das tarefas e ações previstas, assim como uma primeira lista de informações consideradas críticas para a realização da operação[73]. Tudo isso será combinado no chamado *Plano Guia de Operações de Informação (PGOI)*[74], emitido pelo comandante responsável pela operação. O PGOI nesse momento é revisado pelo gabinete do Secretário da Defesa — onde os cargos são mistos civis e militares — e sua aprovação por esse gabinete é condição para o prosseguimento da OI.

A próxima etapa de uma operação de informação como realizada no DoD é o "desenvolvimento do curso de ação[75]", fase em que a operação será projetada em detalhes, através do refinamento das informações e suposições realizadas anteriormente pelo comandante e pela equipe de OI. Nesse passo as operações cruciais são: o "desenvolvimento e priorização de alvos", em que cada alvo será descrito em detalhes, através de informações provenientes de outros órgãos de inteligência e a partir da lista de informações críticas gerada na etapa anterior; a elaboração de rascunhos contendo todas as possibilidades propostas de cursos de ação, descritos através de narrativas escritas pela equipe de OI, baseadas em todas as suposições da equipe sobre o ambiente operacional; a definição das regras de

---

[69] "critical vulnerability — An aspect of a critical requirement which is deficient or vulnerable to direct or indirect attack that will create decisive or significant effects. (JP 5-0)" (JOINT CHIEFS OF STAFF, 2022, p. 57).

[70] "center of gravity — The source of power that provides moral or physical strength, freedom of action, or will to act. Also called COG. See also decisive point. (JP 5-0)" (JOINT CHIEFS OF STAFF, 2022, p. 29).

[71] "intelligence estimate — The appraisal, expressed in writing or orally, of available intelligence relating to a specific situation or condition with a view to determining the courses of action open to the enemy or adversary and the order of probability of their adoption. (JP 2-0)" (JOINT CHIEFS OF STAFF, 2022, p. 114).

[72] Essas estimativas concernem a uma descrição breve de que tipos de adversários e obstáculos serão encontrados em uma determinada missão. Sobre este processo: "joint intelligence preparation of the operational environment — The analytical process used by joint intelligence organizations to produce intelligence estimates and other intelligence products in support of the joint force commander's decision-making process. Also called JIPOE. (JP 2-01.3)" (JOINT CHIEFS OF STAFF, 2022, p. 126).

[73] "commander's critical information requirement — An information requirement identified by the commander as being critical to facilitating timely decision making. Also called CCIR. See also information requirements; intelligence; priority intelligence requirement. (JP 3-0)" (JOINT CHIEFS OF STAFF, 2022, p. 41).

[74] Do inglês *Information Operation Planning Guide* (IOPG).

[75] "course of action — 1. Any sequence of activities that an individual or unit may follow. 2. A scheme developed to accomplish a mission. 3. A product of the course-of-action development step of the joint operation planning process. Also called COA. (JP 5-0)" (JOINT CHIEFS OF STAFF, 2022, p. 55).

engajamento[76]; o refinamento dos requisitos de informação crítica; a definição das métricas de efetividade da missão, que serão utilizadas para definir se houve sucesso ou falha em toda a empreitada. Todas essas informações são formalizadas em dois documentos, um deles chamado *Conceito de Suporte de Operação de Informação (CSOI)*[77] e outro chamado *Matriz de Sincronização de Operação de Informação (MSOI)*[78].

Com vários cursos de ação possíveis projetados e formalizados nos documentos, a próxima etapa envolve a realização de jogos de guerra — simulações realizadas através de computadores ou da imaginação, como em um jogo de tabuleiro ou um *role-playing game* — que testarão cada um dos cursos de ação em busca de vantagens e desvantagens relacionadas a determinadas decisões das forças militares e de seus adversários. Nesses jogos de guerra, os inimigos serão simulados conforme o imaginário sociotécnico dos militares, já que a equipe de OI terá que personificar o adversário conforme imagens pré-concebidas, tanto dos aspectos sociais — culturais e psicológicos — dos adversários quanto dos aspectos técnicos, como quais equipamentos são utilizados por eles. Com as informações novas provenientes da execução dos jogos de guerra, somados aos documentos gerados previamente, os cursos de ação são comparados e alguns são escolhidos para servirem como planos padrão para serem executados.

Os cursos de ação escolhidos são apresentados ao comandante e ao grupo responsável por requisitar a OI, que os aprova ou não. Com os cursos de ação mais vantajosos formalizados e aprovados pelos proponentes, o Conceito de Suporte de Operação de Informação e a Matriz de Sincronização de Operação de Informação são atualizados para conter apenas os cursos de ação escolhidos. Tal conjunto de documentos é submetido novamente ao gabinete do Secretário de Defesa para a sua aprovação final, o que acarreta em ordens para que o comandante militar execute de fato a operação de informação — o que significa que a equipe de OI e o comandante militar responsável estão livres para a começar a utilizar as IRCs, e o *Information Influence Framework* livre para começar a influenciar os

[76] Situações específicas que serão utilizadas para, caso ocorram, decidir se a missão será abortada ou continuada. "rules of engagement — Directives issued by competent military authority that delineate the circumstances and limitations under which United States forces will initiate and/or continue combat engagement with other forces encountered. Also called ROE. See also law of war. (JP 1-04)" (JOINT CHIEFS OF STAFF, 2022, p. 207).

[77] Do inglês *Information Operation Concept of Support* (IOCS).

[78] A matriz de sincronização serve para alertar todas as agências envolvidas sobre os tempos previstos para a execução de tarefas em uma operação específica de modo que ela transcorra sem gargalos. No DTMA: "synchronization — 1. The arrangement of military actions in time, space, and purpose to produce maximum relative combat power at a decisive place and time. 2. In the intelligence context, application of intelligence sources and methods in concert with the operation plan to answer intelligence requirements in time to influence the decisions they support. (JP 2-0)" (JOINT CHIEFS OF STAFF, 2022, p. 207).

sistemas ou pessoas que compõem a audiência alvo da operação, coordenados e supervisionados pelo comandante militar ou pelo *Joint Interagency Coordination Group*.

Apresento agora de que modo os militares estadunidenses definem se uma operação de informação foi ou está sendo bem sucedida ou não, fato que baliza o acompanhamento e as ações da célula de OI durante e após a operação. Segundo o manual JP 3-13, são utilizadas duas métricas de sucesso para OIs, sendo essas as chamadas *Measures of Performance* (MOPs) e *Measures of Effectiveness* (MOEs). "MOPs are criteria used to assess friendly accomplishment of tasks and mission execution." (DEPARTMENT OF DEFENSE, 2012, p. IV-8) e exemplos destas incluem:

> Numbers of populace listening to military information support operations (MISO) broadcasts; Percentage of adversary command and control facilities attacked; Number of civil-military operations projects initiated/number of projects completed; Human intelligence reports number of MISO broadcasts during Commando Solo missions (DEPARTMENT OF DEFENSE, 2012, p. IV-9).

As MOEs, por sua vez, são:

> In contrast to MOPs, MOEs are criteria used to assess changes in system behavior, capability, or operational environment that are tied to measuring the attainment of an end state, achievement of an objective, or creation of an effect. Ultimately, MOEs determine whether actions being executed are creating desired effects, thereby accomplishing the JFC's information objectives and end state. (DEPARTMENT OF DEFENSE, 2012, p. IV-9).

E exemplos de fontes utilizadas para estimar qualitativamente as MOEs são:

> Possible Sources of Measures of Effectiveness Feedback: Intelligence assessments (human intelligence, etc.); Open source intelligence Internet (newsgroups, etc.); Military information support operations, and civil-military operations teams (face to face activities); Contact with the public; Press inquiries 0and comments Department of State polls, reports and surveys (reports); Open Source Center; Nongovernmental organizations, intergovernmental organizations, international organizations, and host nation organizations; Foreign policy advisor meetings; Commercial polls; Operational analysis cells. (DEPARTMENT OF DEFENSE, 2012, p. IV-9).

É interessante notar que a avaliação dos MOEs — e das MOPs, em menor grau — é realizada de maneira qualitativa, contando com uma variedade imensa de inputs que precisam ser conciliados pela equipe de OI para a execução do processo de avaliação qualitativa, o que faz variar bastante a consistência das formas de avaliação em diferentes OI e entre diferentes comandantes e equipes:

> Effectiveness assessment is one of the greatest challenges facing a staff. Despite the continuing evolution of joint and Service doctrine and the refinement of supporting tactics, techniques, and procedures, assessing the effectiveness of IRCs continues to be challenging. MOEs attempt to accomplish this assessment by quantifying the intangible attributes within the information environment, in order to assess the effectiveness of IRCs against an adversary or potential adversary. (DEPARTMENT OF DEFENSE, 2012, p. IV-8).

Nesse ponto, é inevitável perguntar se todo esse processo de planejamento e operacionalização de operações de informação não poderia conter falhas, de modo que certas checagens — como as etapas que preveem o controle civil do processo — possam não acontecer, deixando a execução das OI totalmente a cargo dos militares. Nesse sentido, fica em aberto se, uma vez colocadas em campo todas essas capacidades de influenciar pessoas, organizações e sistemas, não seria possível, por exemplo, a execução de operações de informações clandestinas, que burlariam toda a burocracia e aconteceriam sem nenhuma supervisão, sendo realizadas à discrição daqueles comandantes militares com autoridade suficiente para mobilizar impunemente e fora da lei esses recursos.

Sabendo mais sobre o que são as IRCs, como elas são utilizadas (*através do Information Influence Framework*), para que são utilizadas (para influenciar comportamentos de sistemas, pessoas e organizações) e como são propostas, planejadas, discutidas, simuladas, autorizadas, acompanhadas e avaliadas, a seção final deste capítulo trata de avaliar alguns casos de operações de informação realizados na história recente, como forma de materializar ainda mais o trabalho da inteligência militar no ambiente informacional.

Antes das operações de informação: operações de influência e as estratégias de deterrência e contrainsurgência

Antes de 1998, quando nasce oficialmente a doutrina de IO, as operações militares para influenciar organizações e pessoas eram ligadas à inteligência militar, mas sob o nome “operações de influência” (LARSON *et al.*, 2009, p. 3; RAND, 2022). Tais operações ganharam importância enorme no contexto da chamada estratégia de deterrência, caracterizada pelo uso político por parte do governos dos EUA de suas forças militares e do poderio econômico dos empresários estadunidenses contra a expansão do comunismo no período conhecido como Guerra Fria (MORGAN, 1977, p. 26) (GARTZKE; LINDSAY, 2019;) (ART; GREENHILL, 2015, p. 3). A estratégia de deterrência formatou a estrutura e os objetivos das forças militares e aparato de política externa dos EUA durante o conflito com os soviéticos, tendo maior influência dos anos 60 até meados dos anos 70, influência que diminui

durante os anos 80 para ressurgir no período pós-Guerra Fria como uma resposta à "nova desordem internacional" pós-1991 (ENGLISH *et al.*, 2007, p. 71).

O texto *Arms and Influence,* de 1966, é considerado um dos trabalhos mais importantes sobre a teoria da deterrência. No argumento do texto, Thomas Schelling — considerado um dos autores mais importantes dos campos da teoria da deterrência e também da teoria dos jogos — apresenta a guerra como um problema essencialmente comunicacional e realizado entre a diplomacia e a guerra propriamente dita[79]. Para os aderentes à deterrência, a prática da guerra deve equilibrar-se entre as "ações" militares e econômicas e as "ameaças" e possibilidades de ameaças realizadas por um governo aos seus adversários, de modo que a influência sobre o adversário seja o objetivo principal do esforço de guerra, que não pode ser conduzido de maneira puramente militar:

> Whether it is sheer terroristic violence to induce an irrational response, or cool premeditated violence to persuade somebody that you mean it and may do it again it is not the pain and damage itself but its influence on somebody's behavior that matters. (SCHELLING, 2020, p. 3).

A partir dos anos 60, a visão de Schelling e da corrente de profissionais ligados à política externa dos EUA associados à deterrência será aplicada pelo governo dos EUA em conflitos por todo o mundo, migrando de uma mentalidade ligada à "guerra total" — aplicação da força e da violência visando o rendimento incondicional dos inimigos — para uma ideia de guerra "limitada", ou de "aplicação gradual da força". A ideia central da deterrência é a de coerção:

> Coercion requires finding a bargain, arranging for him to be better off doing what we want - worse off not doing what we want - when he takes the threatened penalty into account. (SCHELLING, 2020, p. 4).

A coerção desloca a prática da guerra no sentido de mitigar o uso de violência, no entanto, não deixa de prever sua utilização. A teoria da deterrência performa a inovação no aparato de guerra dos EUA ao entender a coerção como um dos principais instrumentos para a operação do poder nacional, visando através desta a alteração dos comportamentos dos adversários:

---

[79] "The usual distinction between diplomacy and force is not merely in the instruments, words or bullets, but in the relation between adversaries—in the interplay of motives and the role of communication, understandings, compromise, and restraint." (SCHELLING, 2020, p. 1)

> This difference between coercion and brute force is as often in the intent as in the instrument. To hunt down Comanches and to exterminate them was brute force; to raid their villages to make them behave was coercive diplomacy, based on the power to hurt. (SCHELLING, 2020, p. 5).

O exemplo que, de maneira explícita, endossa o "assalto" a vilas indígenas como instrumento pedagógico é, na verdade, o centro do argumento de Schelling e dos teoristas da deterrência. Para eles, a coerção figura como modo de funcionamento constituinte de algumas das principais ameaças enfrentadas pelo governo dos EUA, o que exige, portanto, uma resposta também coercitiva, como no caso das revoltas civis e do tratamento aos criminosos:

> [coercion] is usually associated with the most vicious labor disputes, with racial disorders, with civil uprisings and their suppression, with racketeering. It is also the power to hurt rather than brute force that we use in dealing with criminals. (SCHELLING, 2020, p. 5).

Para outro influente autor da teoria da deterrência, Patrick Morgan, a combinação entre coerção e as armas pode servir a sete grandes propósitos:

1) To fight a war;
2) To threaten to fight and thus not have to by means of:
a) Compelling someone to surrender without a fight;
b) Forestalling an attack;
3) To settle internal clashes or to control and manipulate internal politics;
4) As an index of national power or status;
5) As an index of national ambition for greater success or power;
6) To "show the flag", a combination of 4 and 5.
7) To provide a general (psychological) sense of security; (MORGAN, 1977, p. 27).

Nesse espectro de ação e com as ideias relacionadas à coerção em ascensão, o governo dos EUA operacionaliza, durante a Guerra Fria, a chamada Estratégia Nuclear, que envolveu a criação tanto de um gigantesco arsenal nuclear — que nos anos 60 e 70 teria entre 25 mil e 30 mil ogivas prontas para o uso (NUCLEAR WARHEAD INVENTORY PER COUNTRY 1945-2022, 2022) — como de uma vasta rede de satélites militares dos EUA — concebidos para espionar o mundo todo através de imagens em tempo quase real, coordenar as comunicações militares e do governo dos EUA, e para monitorar especificamente os locais relacionados ao programa nuclear soviético.

A paranoia geral caracterizada pela popularização do conceito de *mutual assured destruction*[80], no final dos anos 60, leva concomitantemente aos desenvolvimentos tecnológicos ligados à supremacia nuclear e espacial e à criação de novas instituições políticas de cooperação face à opção dos EUA e da URSS por estratégias coercitivas:

> a panoply of measures was developed about how to coexist ideologically, resolve areas of dispute, regulate the military relationship to ensure that it remained stable, and maintain intense channels of communication, including a hotline at all times so that it was always possible to confer during a crisis (RUSI, 2009, p. 251).

Na periferia do mundo, porém, surgiam nos anos 60 uma série de insurgências comunistas que representavam sérios problemas para as empresas dos EUA, assim como para seu governo e forças de segurança. Nesses casos, a pretensa estabilidade criada pela coerção não era evidente, se é que existiu: como a URSS não controlava de fato o despontar de insurgências pelo mundo — apesar de financiar algumas delas — o aparato nuclear e as linhas de comunicação e conduta estabelecidas entre comando civil e militar estadunidenses e soviéticos eram inúteis. Para a deterrência de eventos como a guerrilha cubana de Fidel Castro, a tomada de Angola pelo MPLA, e a vitória e imensa influência dos comunistas no Vietnã, o governo dos EUA cria a chamada doutrina de contrainsurgência, concebida para ser operada através de uma conjugação de seu aparato militar com o aparato de política externa, visando aplicar a coerção não mais ao soviéticos, uma grande nação industrializada, mas a pequenos grupos de guerrilheiros e ativistas políticos comunistas em todos os rincões do mundo.

A doutrina de contra insurgência e as operações de influência

Nesta seção, descrevo brevemente algumas situações que envolvem manuais militares — em geral emitidos para serem consumidos por agentes treinados na disciplina de inteligência militar — que ensinam e dão referências para a execução de operações de influência e operações de contrainsurgência. Tais manuais foram continuamente utilizados entre o final dos anos 60 e os anos 90, no contexto dos muitos conflitos anticomunistas protagonizados pelas forças militares dos EUA, como no conflito no Vietnã, nos diversos conflitos em El Salvador, Nicarágua, Colômbia e por toda a América Latina. Desse modo,

[80] Ideia que preconizava que um ataque de um país ao outro utilizando arsenal nuclear resultaria em retaliação e esse processo levaria a uma destruição mútua dos EUA e da URSS, desencorajando a guerra nuclear.

eles servem para mostrar um pouco das lógicas e ações que marcaram os antecedentes imediatos das hoje chamadas *Information Related Capabilities* (IRCs).

A experiência institucional da inteligência militar estadunidense no combate aos comunistas no Vietnã representou um avanço muito significativo para a doutrina de operações de influência e contrainsurgência, gerando manuais de inteligência, influentes até hoje, focados nessas operações. Logo no início do envolvimento militar estadunidense no Vietnã, os EUA criaram equipes clandestinas de "propaganda armada" que realizaram diversos atos terroristas, como a explosão de bombas em ônibus e locais públicos, a fim de atribuir tais explosões aos comunistas. Esses ataques inviabilizaram o Acordo de Genebra de 1954, que previa um cessar-fogo seguido da realização de eleições (DEPARTMENT OF DEFENSE, 1971, p. 108). Como as informações de inteligência e pesquisas eleitorais contratadas pelo governo dos EUA indicavam que as eleições seriam avassaladoramente ganhas pelos comunistas, o governo dos EUA — principal proponente dos Acordos de Genebra e de seus termos — resolveram que seria melhor dinamitar o próprio acordo, de modo a forçar uma guerra e impedir que os comunistas vencessem eleitoralmente.

Nessa época, essas operações eram chamadas pelo DoD de *armed propaganda operations* ou de *influence operations* e poderiam ser categorizadas nos termos militares de hoje como operações especiais (para a parte da execução militar das explosões), combinadas com *public affairs* e *military information support operations* (para balizar a mídia contra os comunistas), assim como *military deception* (para atribuir crivelmente os ataques aos comunistas) e, por fim, *operational security* (para proteger as identidades e os planos militares de tal operação, que, se revelados, poderiam causar problemas políticos ao governo e penais no Vietnã aos militares que executaram as ordens).

Complementar e concomitantemente, nos anos do governo Diem (1954-1963), a inteligência militar dos EUA esteve ativamente envolvida na sustentação política e pública do regime fantoche, controlando com mão de ferro a mídia e os principais atores do processo eleitoral sul-vietnamita, de modo que Diem se manteve no poder por um longo período, não importando sua absoluta falta de legitimidade popular (DEPARTMENT OF DEFENSE, 1971, p. 201). A operação de fato de tal controle da mídia e da manutenção de influência sobre juízes e magistrados seriam ações hoje associadas às subdisciplinas de *psychological operations*, *military information support operations* e *civil military affairs*, todas elas contidas na definição atual de *information operations*.

Ainda no Vietnã, o chamado Programa Phoenix, que durou oficialmente de 1960 a 1972, também marcou a história da inteligência militar, das operações de influência e da contrainsurgência. O programa originou alguns dos manuais que seriam posteriormente utilizados para treinar as diversas forças anticomunistas pelo mundo em operações de influência e de contrainsurgência (WATCH, 2020). O programa, que era coordenado pela CIA, principal órgão da inteligência militar dos EUA entre os anos 60 e 2001[81], tinha como objetivo "[to get] rid the south of the existing communist parallel government in the villages and eradicate the Viet Cong Infrastructure (VCI) in the countryside" e teve como resultado a "neutralização"[82] de mais de 80 mil vietnamitas tidos como comunistas (FINLAYSON, 2009). O programa funcionou de maneira similar aos esforços de contrainsurgência realizados pelos EUA durante a experiência colonial nas Filipinas: no centro dos trabalhos ocorreu uma grande operação de inteligência, responsável por identificar e fichar detalhadamente os inimigos e as áreas sob sua influência. Com tal finalidade, a CIA e o Exército dos EUA estabeleceram vários postos de interrogação e triagem de presos, em conjunto com as forças aliadas sul-vietnamitas, chegando a empregar 600 profissionais de inteligência estadunidenses somente na execução de interrogatórios (Ibid., 2009). Os interrogatórios, que envolviam tortura, coerção psicológica e estupro, geravam novos dados para o aparato de inteligência, que poderia com eles produzir novas operações de captura de inimigos ou de reconhecimento e policiamento de áreas. Os centros se espalhavam por todo o Vietnã, e a CIA coordenava os esforços e atuava nas tarefas de processamento e análise das informações geradas, produzindo dados de inteligência que seriam remetidos ao comando do Departamento da Defesa e aos comandantes locais. Dentro do Programa Phoenix foram realizadas muitas operações de influência, entre elas, a formação artificial de milícias de extrema direita, as quais compunham o esforço de inteligência, espionando, intimidando, detendo e torturando extraoficialmente suspeitos, e o equipamento das polícias locais com técnicas e tecnologias de inteligência, treinando tanto paramilitares quanto policiais locais para serem executores da política anticomunista dos EUA. Ecoando a preocupação com uma aplicação limitada e gradual da força por meio de coerção realizada através, principalmente, do esforço de inteligência e policiamento, um dos documentos guia do programa, a diretriz MAVC 381-41, determina que a estratégia consiste em utilizar uma "rifle shot rather than a shotgun approach

[81] Após os atentados de 11 de Setembro de 2001, o diretor da CIA deixa de ser concomitantemente o diretor da CIA e da comunidade de inteligência, passando essa a ser presidida pelo novo *Office of the Director of National Intelligence* (ODNI).

[82] Termo utilizado pelos militares durante o conflito no Vietnã para denotar inimigos mortos ou seriamente feridos.

to target key political leaders, command/control elements and activists in the VCI [Viet Cong Infrastructure]" (MILITARY COMMAND ASSISTANCE VIETNAM, 1988).
Diversas técnicas tiveram que ser inventadas, levando em conta, por exemplo, o estado mental das populações locais que se recusavam a cooperar com os soldados estadunidenses:

> The problem was, how do you find the people on the blacklist? It's not like you had their address and telephone number. The normal procedure would be to go into a village and just grab someone and say, "Where's Nguyen so-and-so?" Half the time the people were so afraid they would not say anything. Then a Phoenix team would take the informant, put a sandbag over his head, poke out two holes so he could see, put commo wire around his neck like a long leash, and walk him through the village and say, "When we go by Nguyen's house scratch your head." Then that night Phoenix would come back, knock on the door, and say, "April Fool, motherfucker." Whoever answered the door would get wasted. As far as they were concerned whoever answered was a Communist, including family members. Sometimes they'd come back to camp with ears to prove that they killed people. (APPY, 2004, p. 361).

Anacronicamente, classificando as subpartes do Programa Phoenix conforme as IRCs, podemos pensar novamente na *military deception* e na *operational security* (para não entregar a identidade do informante, inclusive operando a noite), operações especiais (para a execução dos assassinatos políticos), *psychological operations* (para inventar uma técnica que faça com que um informante possa "seguramente" levar os militares ao seu alvo) e *military information support operations* (para influenciar a mídia e também para providenciar o gerenciamento — coleta, processamento e disseminação — das informações de inteligência necessárias para a realização da operação).

Ainda na guerra do Vietnã vemos serem executadas operações que envolvem ações as quais lembram muito as definições das IRCs associadas ao ambiente informacional. Nesse conflito, o governo dos EUA inaugura uma política oficial das forças armadas e da comunidade de inteligência dos EUA, em que a influência sobre os adversários e populações é central para o esforço militar. Para tal, tem início uma grande mobilização interna de definição de doutrina para cada uma dessas disciplinas envolvidas na resolução de disputas políticas por parte das forças militares e do governo dos EUA como um todo.

Como parte desse esforço de institucionalização de cada especialidade relacionada à informação, manuais foram desenvolvidos e utilizados no treinamento dos novos membros e como material de consulta por membros experientes dos aparatos de inteligência militar — principais responsáveis pela execução da coerção através da utilização de informação sobre o inimigo ou controle do hoje chamado ambiente informacional.

Na América Latina, tais manuais e ensinamentos provenientes do Programa Phoenix também teriam impactos históricos devastadores. Historiadoras como Fabiana Andrade (2011), Carlos Fico (2015) e Martha Huggins (2001), entre outras, mostram como as principais instituições ligadas ao setor de inteligência e "segurança interna" no Brasil foram criadas em interação direta com o governo dos EUA: a Escola Superior de Guerra (ESG), instituição chave no Golpe de Abril de 1964, é fundada e supervisionada nos seus primeiros doze anos por uma missão estadunidense, que disponibiliza manuais de doutrina militar e ministra cursos para os oficiais que seriam os responsáveis pela Escola (ANDRADE, 2014, p. 27); o SNI, que coordenava toda a inteligência brasileira e que tinha seções dentro de todos os ministérios civis e militares, também foi criado e formatado em intensa cooperação com o governo dos EUA (Ibid., p. 55). Complementarmente, a análise da grade curricular e do material de ensino da Escola Nacional de Informações (ESNI) — responsável por formar os oficiais de inteligência brasileiros — mostra que o currículo educacional da instituição seria praticamente uma cópia da formação estadunidense, incluindo o conteúdo dos manuais utilizados na formação dos brasileiros[83].

Durante o regime militar e até hoje, boa parte dos cursos oferecidos tanto na ESG quanto na ESNI eram oferecidos através de intercâmbios com os EUA, muitos deles ocorridos no Panamá, onde o Departamento de Defesa dos EUA (DoD) mantinha a Escola das Américas (EdA), assim como outras instituições de ensino militar. Analisando documentos obtidos através do *Freedom of Information Act* (FOIA), Martha Huggins (2001) revela que, entre os anos 1958 e 1979, teriam sido treinados por volta de 100 mil agentes de segurança brasileiros em intercâmbios com os EUA.

Segundo a lei que estabelece a Escola das Américas[84], hoje renomeada Instituto do Hemisfério Ocidental para a Cooperação em Segurança[85] e movida em 1984 do Panamá para o Fort Bragg, no estado da Geórgia, nos EUA, os objetivos da escola são: "Promover o profissionalismo militar, avançar a cooperação entre as forças multinacionais militares na América Latina e expandir o conhecimento das forças armadas latino-americanas sobre os costumes e tradições dos Estados Unidos."

---

[83] Em maio de 1964, o congresso brasileiro sob controle dos militares aprova dois acordos de assistência militar com os EUA. Tais acordos proíbem o Brasil de receber assistência técnica militar de qualquer país sem a permissão dos EUA, assim como também proíbe os oficiais brasileiros de serem treinados por outro país que não os EUA. (SODRÉ, 2010, p. 476).

[84] O texto muda levemente nas várias versões da lei com o passar do tempo, mas a essência é a mesma. Ver https://fas.org/irp/crs/soa.htm e https://www.govinfo.gov/app/details/USCODE-1996-title10/USCODE-1996-title10-subtitleB-partIII-chap407-sec4415. Acesso em: 30 jul. 2021.

[85] *Western Hemisphere Institute for Security Cooperation (WHINSEC).*

A EdA e o complexo militar-educacional do DoD formaram e deram suporte doutrinário à guerra contra as diversas insurgências de esquerda na América Latina, e até hoje atuam no treinamento de forças de segurança latinoamericanas, com foco na guerra contra as drogas. Alguns dos alunos mais famosos da Escola são o ditador panamenho Manuel Noriega, o general e ditador boliviano Hugo Banzer, o líder da junta militar argentina Leopoldo Galtieri, o ditador argentino anterior Roberto Viola, o general golpista equatoriano Guillermo Rodriguez, e, no Brasil, o desvairado Brigadeiro João Paulo Burnier[86], entre outros vários personagens centrais nas muitas ditaduras latinoamericanas. Durante a maior parte do Século XX, a EdA esteve envolvida na formação militar de integrantes de esquadrões da morte e grupos paramilitares de extrema direita responsáveis por massacres por toda a América Latina: milícias colombianas[87], contras nicaraguenses[88], esquadrões da morte em El Salvador[89], Honduras[90], Brasil[91], Peru[92], Bolívia[93] e Uruguai[94]. Manuais que vieram a público no final dos anos 90[95], parte dos materiais utilizados na Escola das Américas, ensinam a tortura física e psicológica, a utilização de abuso sexual e suborno como armas políticas, as operações *false-flag*[96], a prática de sequestros e execuções, assim como a prática da negação de informações e a da condução de operações em sigilo, sem acompanhamento do sistema judicial. Sobre esses manuais, a pesquisadora Lisa Haugaard afirma:

---

[86] João Paulo Burnier foi um dos militares brasileiros mais ferrenhamente anticomunistas. Foi o arquiteto do plano de atentado contra o gasômetro no Rio de Janeiro. Então chefe da 4ª Zona Aérea da Aeronáutica, convocou 40 homens das forças especiais da Força Aérea e os comandou a explodir uma série de bombas em vias públicas da cidade do Rio de Janeiro. Os ataques seriam assumidos por grupos falsos comunistas a fim de justificar um endurecimento do regime com os movimentos de esquerda. O plano foi abortado, pois seus subordinados se recusaram a seguir suas ordens e o denunciaram ao alto comando da Força Aérea, que não tomou qualquer ação contra o Brigadeiro Burnier. Esteve envolvido com o desaparecimento de Rubens Paiva, Stuart Angel e Anísio Teixeira.

[87] O site "Derechos" lista dezenas de paramilitares colombianos graduados na EdA http://www.derechos.org/soa/colom-not.html. Acesso em: 5 ago. 2021.

[88] Disponível em: https://www.nytimes.com/1996/09/28/opinion/school-of-the-dictators.html. Acesso em: 5 ago. 2021.

[89] Disponível em: http://www.derechos.org/soa/elsal-not.html. Acesso em: 5 ago. 2021.

[90] Disponível em: http://www.derechos.org/soa/hond-not.html. Acesso em: 5 ago. 2021.

[91] Disponível em: http://www.derechos.org/soa/br-not.html. Acesso em: 5 ago. 2021.

[92] Disponível em: http://www.derechos.org/soa/peru-not.html. Acesso em 5 ago. 2021.

[93] Disponível em: http://www.derechos.org/soa/bol-not.html. Acesso em 5 ago. 2021.

[94] Disponível em: http://www.derechos.org/soa/uy-not.html. Acesso em: 5 ago. 2021.

[95] Após anos de batalhas legais, em 1997, o DoD libera os manuais publicamente, através de requerimentos judicializados baseados no *Freedom of Information Act* (FOIA). Os manuais estimulam diretamente a formação de grupos paramilitares anticomunistas. O Pentágono alega que o material já foi corrigido, não reflete as posições doutrinárias do DoD dos EUA e agora inclui aulas de direitos humanos. Ver mais em: https://fas.org/irp/crs/soa.htm e https://www.envio.org.ni/articulo/2044. Acesso em: 18 ago. 2018.

[96] Operações *false-flag* são as operações militares projetadas para confundir o adversário quanto a quem praticou de fato a ação.

> Talvez o aspecto mais persistente e nefasto dos manuais seja a falta de distinção entre oposição política e cívica legítima e rebelião armada. O manual *Contra Inteligencia*, por exemplo, define como potenciais alvos de contra-espionagem "equipes de partidos políticos locais ou nacionais, ou partidos que tenham objetivos, crenças ou ideologias contrárias ou em oposição ao Governo Nacional", ou "equipes ou organizações hostis cujo objetivo é criar dissensão ou causar inquietação entre a população civil na área de operações." (p. 228) Este manual recomenda que o exército crie uma "lista negra" de "pessoas cuja captura e detenção são de extrema importância para as forças armadas" (p. 225), que deve incluir não apenas "agentes inimigos", mas também "subversivos", "dirigentes políticos conhecidos ou suspeitos de hostilidade às Forças Armadas ou aos interesses políticos do Governo Nacional" e "colaboradores e simpatizantes do inimigo", conhecidos ou suspeitos[97].

Os manuais da EdA em questão foram utilizados desde os anos 60 até meados dos 90, e são guias práticos de como operar polícias e exércitos. Nos manuais, preconiza-se abertamente o uso de violência e de autoritarismo desmedido para a resolução de qualquer conflito, seja esse militar ou político. Segundo esses manuais, qualquer um poderia ser considerado um inimigo. No manual *Inteligência de Combate*[98], indicadores de um ataque iminente de guerrilhas incluem manifestações de grupos minoritários, construção de casas, recusa dos moradores a colaborar com as forças de segurança, a celebração de festivais religiosos e nacionais e a presença de estrangeiros. Indicadores que mostram que insurgentes estão conduzindo "operações psicológicas" incluem: acusações de corrupção governamental, circulação de petições, tentativas de desacreditar o governo ou as forças armadas, manifestações ou greves e acusações de brutalidade policial. Qualquer crítica ao governo, às forças de segurança ou qualquer outra expressão de descontentamento popular é citada como um possível indicador de atividade insurgente. Nos manuais da EdA quase não são mencionados mandados de prisão, direitos dos presos ou de cidadãos em geral ou mesmo formas de acompanhamento judicial das operações de inteligência — quando esses fatores são mencionados, as frases parecem ter sido escritas às pressas e por vezes contradizem o resto do texto. Pelo contrário, em muitas passagens é estimulada abertamente a ação clandestina. É sugerido que prisioneiros suspeitos de serem insurgentes não sejam cobertos pela Convenção de Genebra[99] — convenção que bane o uso de tortura e utilização de força contra a população civil —, pois não são combatentes regulares em uma guerra regular. É sugerido que os presos suspeitos sejam interrogados nus, que seja utilizada pressão familiar, que sejam utilizados locais clandestinos de interrogação, que os interrogadores utilizem nomes falsos, e que não divulguem para o preso os motivos de sua prisão.

---

[97] Artigo disponível em; https://www.envio.org.ni/articulo/2044. Acesso em: 18 ago. 2021.
[98] Página 148 do documento disponível em: https://soaw.org/wp-content/uploads/2020/04/6-SOA-Intel-Combate.pdf. Acesso em: 4 ago. 2021.
[99] "Revolutionary War, Guerrillas and Communist Ideology", EdA, p. 61.

Um exercício recente do Exército brasileiro revela que, pelo menos no Brasil, tal mentalidade não é apenas uma relíquia do passado. Documentos anonimamente vazados para a mídia descrevem um exercício realizado como uma espécie de vestibular para o ingresso no batalhão de forças especiais (considerados a elite) do Exército Brasileiro. No exercício, os militares simulam viver uma situação em que combatem uma dissidência armada de um certo Partido dos Operários, nascido da luta sindical e que se radicaliza a partir de uma onda de protestos realizados em junho de 2014. Os manifestantes mais engajados no vandalismo nas jornadas de junho de 2014, um antigo líder sindical e uma vereadora trans, irão organizar um movimento armado (chamado de Aliança de Libertação Nacional), com intensa presença propagandista online, visando a queda do governo local. O exercício, portanto, envolve a espionagem de membros ligados a movimentos sociais que possam ter ligações com a Aliança e também a infiltração de militares nesses grupos, visando a localização e neutralização dos líderes revolucionários (MARTINS, 2021). Parece algo que ocorreria em 1968, mas, infelizmente, o exercício foi realizado em 2019.

Com esses exemplos sinistros, observamos que a história das IRCs no passado recente é uma história ligada à utilização da informação para fins sangrentos e politicamente orientados, principalmente visando o combate de qualquer ameaça associada à esquerda. No próximo capítulo, voltamos ainda mais no tempo para investigar as origens da relação entre militares e informação.

CAPÍTULO 3 - A origem da noção de guerra como um problema cibernético: inteligência, informação e controle durante a primeira metade do século XX nos EUA

> Until the latest of our world conflicts, the United States had no armaments industry. American makers of plowshares could, with time and as required, make swords as well. But we can no longer risk emergency improvisation of national defense. We have been compelled to create a permanent armaments industry of vast proportions. Added to this, three and a half million men and women are directly engaged in the defense establishment. We annually spend on military security alone more than the net income of all United States corporations.
>
> Now this conjunction of an immense military establishment and a large arms industry is new in the American experience. The total influence—economic, political, even spiritual—is felt in every city, every Statehouse, every office of the Federal government. We recognize the imperative need for this development. Yet, we must not fail to comprehend its grave implications. Our toil, resources, and livelihood are all involved. So is the very structure of our society.[100].

Este capítulo trata de como os militares estadunidenses estabeleceram materialmente uma dimensão informacional ao seu próprio trabalho durante o curso da primeira metade do século XX. Baseado principalmente no trabalho de historiadores e historiadoras, tento reconstruir um pouco da dinâmica e da confusão dos eventos e modos de pensar o mundo que guiaram o início do processo de forja do conceito contemporâneo de informação. Este capítulo também pode ser pensado como uma genealogia possível da comunidade de inteligência dos Estados Unidos da América e dos computadores no Departamento de Defesa. Os argumentos principais desta seção relacionam o desenvolvimento inicial da disciplina de inteligência nos EUA com a experiência colonial e com uma preocupação permanente da classe política com a manutenção da ordem interna. Também é argumento importante que tal processo acelera-se a partir do estabelecimento de uma aliança poderosa entre ciência, mercado e Estado, realizada no curso da Primeira Guerra Mundial, mas principalmente no curso da Segunda Guerra Mundial. Secundariamente, busco demonstrar como tecnologias políticas (como decretos presidenciais e escolas para a formação de agentes disfarçados) e tecnologias físicas (radares, grampos de telefone, cartões perfurados, computadores) sempre aparecem nesta história acoplados uns aos outros.

O capítulo se divide em quatro subseções organizadas de maneira cronológica: a primeira seção narra as origens humildes da atividade de inteligência nos EUA, seguindo duas experiências que serão formativas para os primeiros oficiais de inteligência: a "Expedição Punitiva" contra Pacho Villa no México, em 1917, e a invasão estadunidense das Filipinas

[100] Dwight D. Eisenhower em seu último discurso público como Presidente dos EUA, 17 de janeiro de 1961(EISENHOWER, 1961).

(1889-1948). A segunda subseção mostra como a Primeira Guerra Mundial e a instabilidade política entre os anos 20 e 40 provocam a institucionalização da inteligência como parte principal do aparato de manutenção da ordem interna dos EUA. A terceira subseção narra o estabelecimento da aliança mercado, ciência e Estado ocorrida durante a Segunda Guerra e mostra como tal aliança gera novas teorias e tecnologias que impactarão diretamente as atividades dos militares, com a inteligência sendo particularmente afetada. Por fim, a quarta subseção narra como o novo cenário mundial pós-Segunda Guerra, somado às ideias da cibernética e da análise de sistema, impactarão a organização da inteligência militar, que, no começo da Guerra Fria, se reestrutura, visando uma operação mais sistematizada e científica.

A experiência colonial, novas tecnologias e o nascimento da inteligência militar estadunidense

Como indica o discurso de Eisenhower, os anos que culminam na Guerra Fria são intensamente transformadores para o aparato militar estadunidense, que precisa se adequar a muitos novos tipos de ameaças e desafios no âmbito global. O começo do século XX viu — para nos restringirmos a uma lista não exaustiva — o surgimento e ascensão do fascismo italiano e do nazismo alemão, ambos movimentos com ampla influência e simpatia na política europeia e estadunidense até meados dos anos 30 (KATZ, 2022); uma onda de revoluções e movimentos socialistas por todo o mundo, como a Revolução Bolchevique, de 1917, as diversas tentativas de golpe socialista durante a República de Weimar (FAYE, 2009) ou o começo da guerra civil entre comunistas e nacionalistas na China, em 1927. O período também foi marcado pela intensificação de uma segunda onda de colonialismo (MCCLINTOCK, 1995) e pelas transformações na indústria e nos modos de viver trazidas pelo aço, pela eletricidade e pela química fina (FREEMAN; SOETE, 2009). Tais novidades permitem a ascensão do petróleo como combustível e dos tanques, metralhadoras, aviões, submarinos, trens, telégrafos e do rádio como algumas das formas principais para a resolução de conflitos.

Nesse contexto, as seções de inteligência —- órgãos internos das forças militares destinados a "coletar informações sobre o inimigo e sobre o ambiente de batalha para o comandante" (FINNEGAN; DANYSH, 2015, p. 3) — podem servir como local privilegiado para observar como os Estados — e os funcionários operadores do Estado — lidam com as mudanças tecnopolíticas do período, principalmente no âmbito do controle político-militar. As seções de inteligência são historicamente responsáveis por lidar com problemas tão políticos

como a criação de procedimentos para identificar inimigos, ou o planejamento de como tal ameaça será neutralizada; e tão técnicos como a questão de como se fará o monitoramento de tal inimigo, ou como serão consolidadas as informações em relatórios a serem enviados para os comandantes.

Nos EUA, esse tipo específico de organização, baseado principalmente na coleta, processamento e disseminação de informações, e que se propõe a, através dessas atividades, identificar e monitorar inimigos do Estado, foi criado em 1882, vinte anos após o fim da Guerra Civil. A *Military Information Division* (MID), gabinete de pouca importância e subordinado ao *Adjutant General*[101] do *Departament of War* (DoW), inicialmente tem a responsabilidade de levantar informações de cunho estatístico, como o números de tropas internas mobilizadas por estado ou o número estimado de tropas inimigas por país; a organização também é responsável por criar mapas, assim como formular planos de mobilização de pessoal e material instrutivo para oficiais. Poucos anos após sua fundação, em 1889, a MID começa timidamente a enviar *attachés* militares pelo mundo, visando a coleta sistemática e internacional de informações relevantes militarmente, porém, tais esforços esbarram na falta de definição de padrões a serem seguidos e nas confusas ordens oficiais do *Adjutant General,* que tornam o trabalho desse *attachés* genérico e deixado à sua própria discrição[102]. O acúmulo de funções não parece ser visto como um problema à época, pois, em 1893, a *Military Information Division* recebe também a função de catalogar e manter museus históricos contendo acervos de peças e relíquias militares. Como exemplo da relativa desimportância da atividade de coleta de informações, para a realização de todas essas tarefas, durante a Guerra de 1889 entre EUA e Espanha, a MID contava com um total de 67 empregados: 11 trabalhando no edifício que concentrava os Departamentos da Guerra, de Estado e da Marinha em Washington D.C., 16 servindo como *attachés* no estrangeiro e outros 40 trabalhando no levantamento de estatísticas e na elaboração de mapas e material para oficiais (FINNEGAN; DANYSH, 2015, p. 13). Para fins de comparação, enquanto escrevo no ano de 2022, estimativas dão conta de que a chamada "comunidade de inteligência"[103] emprega nos EUA por volta de 850.000 pessoas (PRIEST; ARKIN, 2011).

---

[101] Posição militar administrativa do Exército dos EUA, o *Adjutant General* serve como auxiliar administrativo subordinado diretamente ao Comandante Geral (*Chief of Staff*).

[102] As ordens oficiais são: "sempre que praticável, façam relatórios sobre tudo o que possa ser desejável ao governo saber no caso de uma guerra súbita" (FINNEGAN; DANYSH, 2015, p. 12).

[103] O termo "comunidade de inteligência" tem origem nos anos 50 na gestão do General Walter Bedel Smith como diretor da CIA, e designa o conjunto das agências, organizações subordinadas às agências do governo e hoje também as empresas privadas prestadoras de serviços de inteligência para o governo, que trabalham

O envolvimento colonial dos EUA nas Filipinas (1889-1948), assim como a Guerra de Fronteira entre EUA e México (1910-1919) fomentam de maneira significativa o esforço de inteligência estadunidense, que apesar disso não é plenamente incorporado como uma das funções principais do Exército ou do Departamento de Guerra até a Primeira Guerra Mundial. Tecnicamente, o trabalho de inteligência realizado nesse momento — até por volta da Primeira Guerra — se assemelha mais ao trabalho acadêmico de levantamento de fontes públicas e no cálculo de estatísticas do que na espionagem, apesar de que já no conflito entre EUA e Espanha de 1889 é possível observar um componente misto de alta tecnologia e espionagem quando a *Military Information Division* grampeia os cabos submarinos de telégrafo dos espanhóis, interceptando informações valiosas sobre os planos dos inimigos — informações que, no entanto, não são utilizadas devido à falta de prestígio da atividade de inteligência no comando das forças armadas, que simplesmente desconsidera a informação fornecida pela MID.

Durante a invasão estadunidense às Filipinas, ocorrerá outro experimento crucial do Exército dos EUA em relação à atividade de inteligência: em seu primeiro posto no ramo da inteligência militar, a partir de 1902, o Major Ralph van Deman — conhecido como o pai da inteligência estadunidense — coordena uma extensa operação de contrainsurgência que contará com o processamento de documentos inimigos interceptados, a utilização de informantes contratados entre os locais, a infiltração de agentes nos movimentos que contestavam a presença estadunidense (sendo esses movimentos militares ou não), assim como a utilização sistemática de tortura em centros de triagem responsáveis pela interrogação de suspeitos. Nesta campanha, marcada pela utilização da inovadora tecnologia dos cartões-ficha perfurados, a informação proveniente da inteligência militar é catalogada e processada por meio de computadores mecânicos[104], gerando novos cruzamentos de dados que levam a novas operações para a coleta de mais informações. A confecção de mapas será utilizada, por exemplo, para mapear o campo de batalha entre áreas sujeitas à menor ou maior influência dos movimentos guerrilheiros, com as cidades e vilas "mais inimigas" sendo destruídas e as populações desses locais movidas para campos de concentração onde a maioria dos locais eram interrogados e submetidos ao trabalho forçado (LINN, 1989; KARNOW, 1990). Os

separadamente e em conjunto para dar suporte à política externa e à segurança nacional dos EUA (WARNER; MCDONALD, 2005, p. 13).

[104]A tecnologia de cartões perfurados foi utilizada pela primeira vez no censo estadunidense de 1890, com uma máquina projetada por Hermann Hollerith como coração da operação. Van Deman utilizou o mesmo tipo de máquina em sua campanha contra-insurgente nas Filipinas. Para saber mais sobre a história e funcionamento da tecnologia dos cartões perfurados consultar (JONES, 2012).

cartões-ficha, intitulados "*Descriptive Cards of Inhabitants*" e via de regra preenchidos com informações obtidas sob tortura, continham campos a serem preenchidos como "Lista de parentes e relações", "Raça", "Aparência", "Ocupação e local de trabalho", "Locais frequentados" e "Opinião sobre os EUA". Ao final da gestão de Van Deman na *Insurgent Records Division*, 70% da população das Filipinas se encontrava fichada em detalhes, com uma vasta rede de informantes operada pela polícia e pelo Exército filipino e coordenada pelos militares dos EUA (HOCHSCHILD, 2018; MCCOY, 2014).

Repercutindo os eventos e retratando uma visão corrente na época, nos EUA, em maio de 1902 a famosa revista LIFE publica uma matéria de capa sobre a guerra nas Filipinas: " (...) nossos soldados bombeiam água salgada para dentro de homens para 'fazê-los falar'. Levam como prisioneiros pessoas que se renderam pacificamente com as mãos ao alto. Uma hora depois, sem nem mesmo um átomo de evidência que mostre que eles possam ser *insurrectos*, todos são enfileirados em uma ponte e um a um são executados a tiro, caindo na água abaixo". O texto pode parecer repreender o ocorrido, mas a conclusão da reportagem mostra o contrário: "(...) não é uma guerra civilizada, mas não estamos lidando com pessoas civilizadas." (BRASWELL, 2017).

Outros diversos registros da época mostram como nos editoriais de mídia e nas declarações públicas de autoridades dos EUA, a invasão das Filipinas e os métodos do Exército estadunidense seriam plenamente justificados como parte de uma missão civilizatória que, além das Filipinas, englobaria Cuba, Haiti e Porto Rico (PALATINO, 2016; KRAMER, 2006). Uma análise do conteúdo dos cartões perfurados filipinos realizada pelo já citado historiador Alfred Mccoy, mostra que, nesse momento de experimentos contingenciais em inteligência — realizados mais à discrição de pessoas e menos baseados em planos e procedimentos padrão — a visão de um inimigo racializado e bestial povoa as mentes dos oficiais estadunidenses, o que pode em parte explicar a preferência dos militares por ações barbaramente violentas e desumanas contra a resistência filipina à invasão. O diário pessoal de Van Deman, assim como declarações de muitos comandantes estadunidenses que serviram nas Filipinas indicam a adoção de ideias semelhantes.

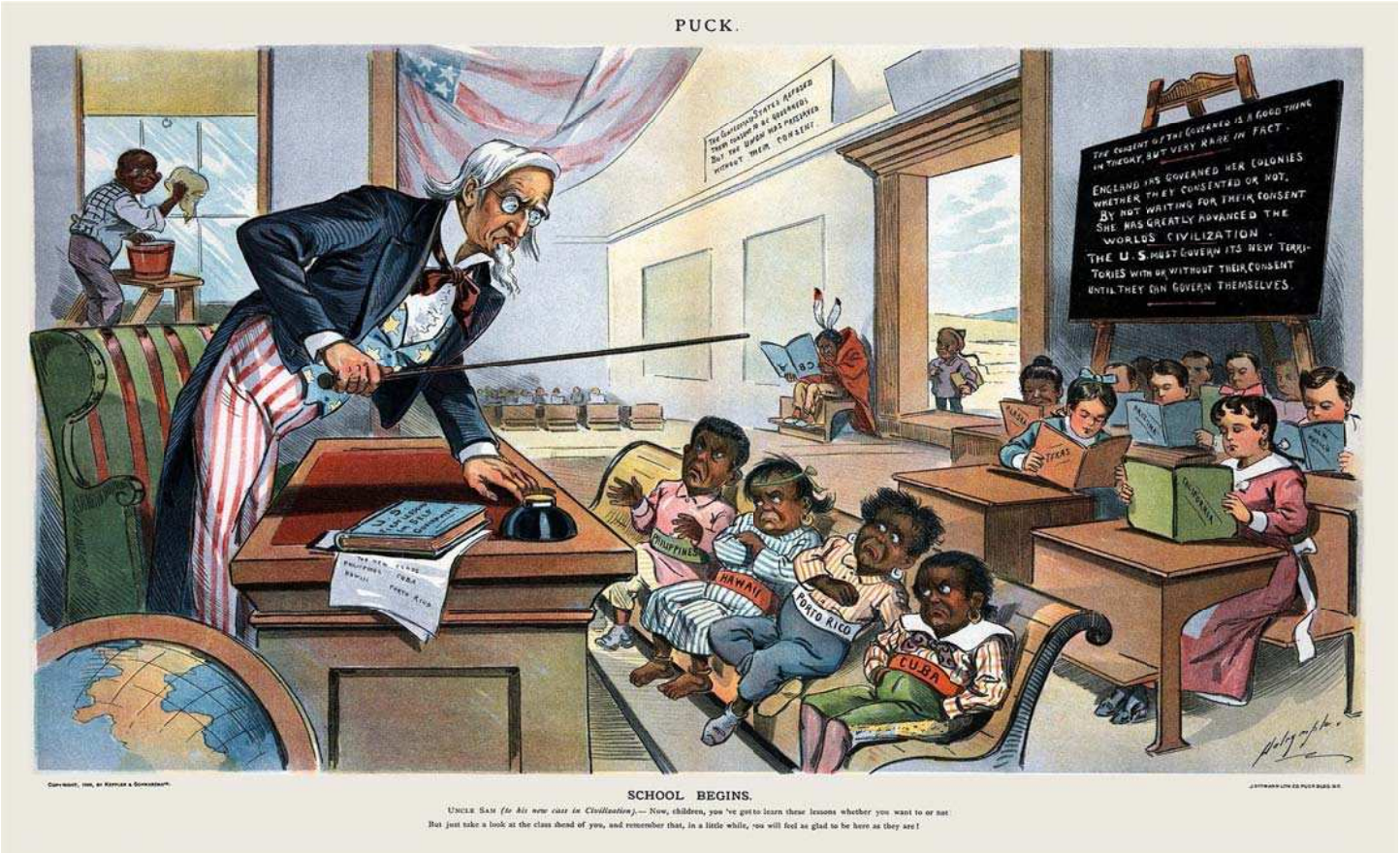


Imagem 11 - Cartum *School Begins* de Louis Dalrymple, publicado na revista Puck de 25 de janeiro de 1899[105].

[105] A ilustração mostra o Tio Sam como professor, ensinando o livro "Lições estadunidenses de autogoverno" a uma pequena turma de crianças negras relutantes e esfarrapadas, com os rótulos "Filipinas", "Havaí", "Porto Rico" e "Cuba" escritos em suas roupas. Atrás desses rebeldes negros, uma turma de estudantes bem vestidos e bem comportados estuda sozinha, sem o auxilio de um professor; em seus livros encontram-se os rótulos "Califórnia", "Novo México", "Alaska", "Arizona" e "Texas", estados recentes, mas já plenamente integrados aos EUA, representados aqui como a "turma passada" da escola. Nas lousas, os ensinamentos de que o consentimento não é necessário para que o país mais avançado ensine aos menos avançados como viver e se organizar. No canto do estudante "burro", um índio nativo americano lendo de ponta cabeça um livro sobre o alfabeto, sem perspectiva de chegar às lições de autogoverno recebidas pelo resto dos alunos. Na porta, um estudante chega atrasado vestido com trajes típicos chineses. Limpando os vidros da escola e ouvindo de relance as lições de Tio Sam, um garoto negro trabalha.

Diversificando o modo de operação da inteligência estadunidense, fato relacionado à participação dos EUA como um ator estatal na Ásia, em 1907, o Exército investe na formação de agentes disfarçados preparando-os para a atuação no exterior. Assim, manda funcionários de inteligência para Japão e China, a fim de que cursem aulas de idioma e cultura (FINNEGAN; DANYSH, 2015, p. 15). Os *Signal Corps*, grupos táticos do Exército criados durante a Guerra Civil estadunidense e responsáveis pela manutenção da comunicabilidade interna militar, experimentam com mais ou menos sucesso o uso de balões, dirigíveis e dos novíssimos aviões para a coleta de informações meteorológicas e para a configuração do campo de batalha (FINNEGAN; DANYSH, 2015, p. 18). Em 1916, o primeiro manual militar do Exército dos EUA sobre criptografia de mensagens é publicado pelo Capitão do *Signal Corps*, Parker Hitt (SMOOT, 2022), indicando um interesse crescente na manutenção de segredos e em comunicações seguras[106]. Os *Signal Corps* ficarão também responsáveis pela fabricação de dispositivos codificadores e decodificadores, para o qual serão estabelecidas fábricas do Exército em parceria com a iniciativa privada.

Acompanhando a tendência lenta mas progressiva de sofisticação, também em 1916 acontece uma operação militar que marca a história dos serviços de inteligência pela ampla gama de técnicas e tecnologias empregadas, mostrando o entusiasmo do comando militar com o uso de novas tecnologias: trata-se da "expedição punitiva"[107] dos EUA no México para a captura do revolucionário Pancho Villa e para a destruição de seu bando de guerrilheiros, operação que ocorre após o grupo de Villa realizar uma série de cruéis ataques em solo estadunidense. Nessa operação, ordenada pelo presidente Woodrow Wilson e comandada pelo *Brigadier General* John Pershing, além de informantes locais e agentes disfarçados, um esquadrão de vinte índios Apache foi recrutado para levantar informações sobre o terreno e junto aos habitantes locais. Um grande contingente de homens a cavalo monitorava todas as estradas e informava os comandantes militares sobre elas. O governo mexicano, inicialmente parceiro — e posterior inimigo — dos estadunidenses, teve suas comunicações por carta, telégrafo e rádio interceptadas durante a operação. Pela primeira vez na história das operações de inteligência foram utilizados veículos automotores e caminhões, assim como aviões[108] e câmeras aéreas, além de dois caminhões customizados como estações

[106] Até a Primeira Guerra, os padrões de comunicação dos militares estadunidenses privilegiavam os custos sobre a segurança, o que fazia com que a maioria das comunicações fosse realizada de maneira não criptografada.
[107] Nome originalmente dado à operação.
[108] Oito aviões, todos destruídos nos primeiros dois meses de operação no México. A operação foi coordenada pelo Major Benjamin Foulois, o primeiro oficial americano a aprender a pilotar um avião.

de transmissão e interceptação de rádio (FINNEGAN; DANYSH, 2015, p. 18). A operação estadunidense teve efeito negligível no Exército de Pancho Villa — que nunca foi preso nem localizado — e se estendeu por 11 meses e 500 milhas adentro do território mexicano, causando e catalisando diversos conflitos internos em um México em processo de Guerra Civil e Revolução Constitucionalista. O General George Patton, responsável pela invasão da Normandia na Segunda Guerra Mundial, e o futuro presidente dos EUA, Dwight D. Eisenhower, foram alguns dos combatentes da expedição punitiva. Um mês após a debandada da operação de caça a Villa, o governo dos EUA decide envolver-se diretamente na guerra que acontece na Europa — posteriormente chamada de Primeira Guerra Mundial — e o General Pershing é escolhido comandante das Forças Expedicionárias estadunidenses na França. Durante a Primeira Guerra Mundial, com auxílio dos serviços de inteligência britânico e francês, Pershing replicará na Europa, em escala aumentada e de maneira mais estruturada e profissional, os esforços de inteligência militar realizados no México, transformando o Exército dos EUA em uma máquina sofisticada de obtenção e processamento de inteligência militar.

Os eventos relatados acima mostram que, nessa época, entre 1889 e 1916, há uma concentração do aprendizado estadunidense no ramo da inteligência militar em determinadas pessoas que, por seus protagonismos em conflitos importantes, se tornam influentes, como é o caso de Van Deman e Pershing. No entanto, até os primeiros meses de seu envolvimento na Primeira Guerra, o comando das forças armadas dos EUA ainda não vê a atividade de inteligência como realmente importante ou equiparável à infantaria ou à logística, o que a relega ao segundo plano no organograma militar. No início da Primeira Guerra Mundial, a burocracia de inteligência militar se encontra em tal estado de precariedade que os oficiais responsáveis por compilar relatórios sobre as forças alemãs são obrigados a basear os planos iniciais militares dos EUA em documentos provenientes de fontes abertas, como um almanaque público sobre exércitos do mundo, uma lista contendo todas as transações marítimas entre EUA e Alemanha e um documento contendo os próprios números e proporções do Exército estadunidense (FINNEGAN; DANYSH, 2015, p. 17). No curso dos próximos dezessete meses a situação mudaria da água para o vinho. A atividade de inteligência será ampliada drasticamente, de modo que todos os batalhões das forças expedicionárias estadunidenses, assim como todos os batalhões no continente americano conterão suas próprias unidades de coleta e processamento de informações militares ao final de 1918. No continente, tal expansão do serviço de inteligência institui um extenso aparato de

vigilância política gerido pelo Departamento de Guerra, visando o controle da subversão no Exército e na sociedade estadunidense como um todo.

A instabilidade da primeira metade do século XX como catalisadora da atividade de inteligência

Ao início do envolvimento dos EUA na Primeira Guerra Mundial, uma reestruturação no Departamento de Guerra cria o chamado *General Staff*, um gabinete composto por um número seleto de oficiais com status de general, cada um contando com uma equipe com funcionários fixos e responsável por uma função essencial para a operação das forças armadas[109]. O novo corpo burocrático é responsável por instaurar regularidade nas políticas e decisões do Departamento de Guerra, assim como supervisionar a execução de tais políticas. Nessa reorganização, o lobby de longa data do agora General Van Deman pela ascensão da inteligência militar ao posto de função essencial das forças armadas finalmente dá frutos, e não só é criada uma nova *Military Information Division*, como ela agora opera em pé de igualdade e importância em relação aos serviços e divisões considerados essenciais no Departamento de Guerra, como a divisão de planejamento de guerra, ou os novos *Tank Corps* e o novo *Chemical Warfare Service* (HEWES JR., 1975).

Agora uma das pessoas mais importantes no Departamento de Guerra, Van Deman é nomeado comandante da nova Divisão de Informação Militar e inicia um processo de cooperação intenso com as potências aliadas europeias, de modo a obter delas a informação a qual o Departamento de Guerra dos EUA ainda não é capaz de gerar por si mesmo. Na Europa, onde a guerra acontece de fato, o comandante das Forças Expedicionárias, General John Pershing, também inicia uma colaboração com os aliados Grã Bretanha e França no setor de inteligência e, paralelamente aos esforços de adequação do Departamento de Guerra, cria uma estrutura complexa e multifuncional de inteligência militar que tratará no campo de batalha de tarefas diversas, compreendendo desde a produção de mapas e operação de equipamentos de detecção de aviões, até a operação de grampos de

[109] A estrutura de funcionamento do *General Staff*, hoje nomeado *Joint Chiefs of Staff*, lembra as diretorias de uma empresa privada, com o *Chief of Staff* submetido ao Secretário de Guerra, hoje Secretário de Defesa. Os oficiais que compoẽm o *General Staff* (ou hoje o *Joint Chiefs of Staff*) normalmente formam-se através dos colégios de guerra, em turmas especiais compostas pelos melhores estudantes. Esses oficiais têm um grande senso de camaradagem e e*sprit de corps*, o que conduz a uma postura ativa de proteção aos seus iguais (FOREIGN POLICY RESEARCH INSTITUTE, 2014, 54:00).

comunicação, o gerenciamento de operações de enganação militar[110] e de grupos responsáveis por censurar reportagens que pudessem afetar a moral das tropas aliadas. Após depender das escolas de formação de oficiais de inteligência dos franceses e ingleses durante os primeiros meses do envolvimentos dos EUA na guerra, Pershing institui na França uma escola de inteligência própria das forças armadas estadunidenses, inicialmente com professores ingleses e franceses — muitos deles com experiência militar colonial — ou treinados diretamente por eles. Nessa escola, os alunos aprenderão como executar as atividades básicas de inteligência, com destaque para o ensino prático de técnicas de interrogação, com os alunos e professores testando-as em prisioneiros reais (FINNEGAN; DANYSH, 2015, p. 35).

Influenciados diretamente pelo sistema de organização britânico, ambos Von Deman e Pershing irão copiar a estrutura da inteligência militar inglesa e sua doutrina. Dividindo a atividade de inteligência entre "inteligência positiva" e "inteligência negativa" — a primeira consistindo em obter informações do e sobre o inimigo e a segunda em negar ao inimigo a capacidade de obter informações sobre suas forças e governo — a inteligência militar estadunidense será subdividida em várias seções pertencentes a um ou outro ramo da atividade. Nas Forças Expedicionárias, Pershing criará no GHQ[111] a "segunda seção"[112], que, por sua vez, será dividida em G2-A, responsável pela inteligência positiva, e G2-B, responsável pela inteligência negativa. Tais seções operarão diretamente integradas ao comando de guerra (G1) e conterão subunidades responsáveis por cada atividade de inteligência. Tais subunidades serão replicadas em todas as 102 divisões das forças expedicionárias durante a Primeira Guerra[113], com cada uma delas reportando à sua unidade mãe na segunda seção do GHQ. Nos EUA continental, as subunidades da nova MID do Departamento de Guerra — que também serão replicadas em todas as forças armadas subordinadas ao DoW —, serão inclusive nomeadas de acordo com a prática dos serviços de inteligência britânicos: MI-1, responsável pela administração da inteligência; MI-2,

[110] Para os militares, negar ao adversário a capacidade de saber o que se passa nas próprias forças e território, e nas de seu inimigo também, é uma das principais atividades a serem realizadas para se garantir a superioridade militar. A atividade de enganação militar — a disseminação de mentiras e estratagemas com finalidade de enganar, desmoralizar ou comprometer de alguma forma a ação do inimigo — é um dos pilares das atividades de inteligência e contrainteligência.

[111] Do inglês *General Head Quarters*, Quartel General (QG).

[112] Segunda seção é o apelido dado pelos militares britânicos às suas seções de inteligência. O apelido implica uma importância secundária apenas ao comando geral das forças militares. O termo ganhou tal força e influência que hoje em quase todo o mundo ocidental — incluindo aí o Brasil e a maior parte da América Latina — as seções de inteligência, por exemplo das polícias, são chamadas de segunda seção ou de "P2".

[113] Para saber mais sobre a evolução das divisões militares estadunidenses durante a Primeira Guerra, consultar (WILSON, 1999, p. 23, 40-42, 47, 73).

exclusivamente dedicado à coleta de inteligência do estrangeiro; MI-3, dedicado à contraespionagem nos serviços militares; MI-4, dedicado a combater a subversão civil; MI-5, responsável pela administração das publicações e circulação interna de informação; MI-6, serviço de tradução; MI-7, gerenciamento de informações confidenciais e elaboração de gráficos; MI-8, responsável por criptografia e comunicações seguras, assim como pela quebra dos códigos inimigos; MI-9, dedicado à coordenação das informações provenientes das forças militares em campo; MI-10, responsável pela execução da censura militar (HEWES JR., 1975). Outras subunidades serão criadas e desaparecerão com o tempo, como o caso da MI-13, especializada na investigação de casos de corrupção e fraude no governo.

Sob influência das doutrinas militares dos aliados, conciliando sua experiência colonial em contrainsurgência e reconhecendo que, em uma sociedade industrial, os aspectos militares se encontram interseccionados com a economia e com a política de maneira mais ampla, sob Von Deman a inteligência estadunidense sofrerá uma transformação fundacional, passando a coletar e a processar não somente informações puramente militares, mas também informações de cunho cultural, social e psicológico de qualquer um que possa ser considerado suspeito por eles, o que inclui militares das próprias forças. Distante cerca de três mil milhas do campo de batalha da Primeira Guerra e com o GHQ das forças expedicionárias executando suas próprias funções de inteligência — principalmente inteligência positiva por causa da proximidade com o inimigo — nos EUA os principais esforços da nova MID do Departamento de Guerra se localizavam no setor de inteligência negativa, e buscavam dar conta de dois grandes temores da classe política dos EUA da época: a subversão comunista e anarquista nas fábricas, e a infiltração de simpatizantes do inimigo — principalmente da Alemanha — nos quase 4 milhões de cidadãos dos EUA convocados a fazer parte das tropas militares estadunidenses. Para lidar com tais ameaças, as subunidades MI-3 (contraespionagem militar) e MI-4 (contraespionagem e combate à subversão civil) se tornam particularmente importantes, esbarrando no problema da falta de pessoal especializado. Inicialmente, o Departamento de Guerra e a MID recorrem a detetives privados, como os da agência Pinkerton[114], e a policiais do Departamento Antibomba da Polícia de Nova Iorque, acostumados a investigar grupos anarquistas. Não sendo possível satisfazer a demanda por profissionais de inteligência somente através de policiais emprestados e detetives privados, o Departamento de Guerra e o MID, em julho de 1917, instituem o *Corps of Intelligence Police (CIP)* ou Corpos da Polícia de Inteligência do Exército, primeira agência regular dedicada à

[114] Uma das primeiras empresas estadunidenses no ramo de mercenários e investigadores privados. Foi ator importante no processo de proibição da operação de forças mercenárias em solo estadunidense (WEISS, 2007).

formação sistemática de agentes de inteligência e contrainteligência dos EUA. Os primeiros esforços dos oficiais formados pelo CIP e lotados no MI-3 serão concentrados na organização de um aparato dedicado à vigilância de todos os níveis existentes do Exército dos EUA, com pelo menos dois agentes independentes recrutados como informantes em cada unidade militar (FINNEGAN; DANYSH, 2015, p. 26).

Se a infiltração estrangeira nas forças armadas de um país formado por imigrantes pode ser considerada uma ameaça racional a ponto de justificar o mandato e os esforços da subunidade MI-3, no MI-4 o mandato se tratava muito menos da defesa da integridade militar e muito mais da manutenção da ordem social interna nos Estados Unidos. Problemas trabalhistas, conflitos e tensões raciais, movimentos indígenas, contraespionagem econômica e casos políticos em geral formam nessa época o substrato do trabalho do MI-4. Frequentemente alguns dos temas de trabalho se misturavam, inclusive de maneira muito improvável, como vemos em um comentário de Van Deman sobre a vigilância da pastora negra feminista Nannie Burroughs: "Estou certo de que os alemães estão por trás da revolta preta" (JOHNSON, 1999, p. 35).

Trabalhando em casos internos dos EUA, o MI-4 operava em cooperação intensa com outras agências do governo, em especial com o Departamento de Justiça, órgão com a competência de realizar a deportação e a prisão de pessoas acusadas de ofensas contra as forças armadas. Para auxiliar no trabalho de inteligência e com a finalidade de coletar informações sobre o ambiente de trabalho e sobre vizinhanças de todo os EUA, o MI-4 articula o funcionamento de várias organizações híbridas civil e militar, como o *Plant Protection Service*, ou, a mais importante, *American Protective League*. O *Plant Protection Service* foi uma organização subordinada ao Exército, formada por agentes recrutados entre trabalhadores civis industriais, responsáveis por trabalharem como infiltrados, passando informações e relatórios para os militares sobre possíveis desordens e distúrbios em fábricas. Inicialmente destinada a monitorar apenas o setor de aeronáutica, durante a guerra a organização se estende para todas as fábricas que trabalham para o esforço militar estadunidense (FINNEGAN; DANYSH, 2015, p. 29). A *American Protective League*, proposta por um milionário do setor de marketing para o Advogado Geral dos EUA[115] como uma maneira de aumentar sem custos o poder do governo contra desordens sociais, foi uma organização que operou em caráter semioficial[116] entre 1917 e 1919, e reuniu civis voluntários

[115] Equivalente ao Ministro da Justiça no Brasil.

[116] A organização contava com a autorização do Estado para a atuação paramilitar, mas era caracterizada legalmente como uma associação privada de caráter "cívico".

que trabalhavam — com poder de polícia — em casos designados pela inteligência militar ou pelo *Bureau of Investigation* (BOI), precursor do *Federal Bureau of Investigation* (FBI), agência de investigação civil ligada ao Departamento de Justiça. "Tenho hoje várias centenas de milhares de cidadãos privados ajudando as infatigáveis autoridades federais a manterem um olho nos indivíduos desleais e a elaborarem relatórios sobre enunciações desleais", diria, em 1919, o Advogado Geral dos EUA, Thomas Watt Gregory, classificando a organização como "uma organização patriótica poderosa!" (KENNEDY, 2004, p. 62). Seus agentes ilegalmente grampeavam espaços e pessoas, invadiam domicílios e espionavam oponentes. Durante o período em que a organização esteve em atividade, ela se envolveu em milhares de casos de monitoramento e prisões arbitrárias de suspeitos de serem simpatizantes de alemães entre a população. No entanto, não só os imigrantes alemães foram perseguidos pelos membros paramilitares da APL: um relatório interno sobre as atividades da organização, durante cinco meses em 1918, mostra que uma parte considerável do esforço da seção noroeste havia sido gasto com a repressão a greves e eventos ligados à *International Workers of the World*[117] (LINFIELD, 1990, p. 38). Durante sua existência, o movimento paramilitar atuou em centenas de casos relacionados à repressão de organizações de esquerda, sindicatos e do movimento antiguerra. Membros da APL organizam, por exemplo, as chamadas *Slacker Raids*, batidas policiais em bares durante fins de semana a fim de buscar evasores da convocação ao exército. Somente no dia 14 de setembro de 1917, o movimento, em conjunto com a polícia, prendeu ilegalmente 60 mil pessoas em Nova Iorque, cerca de apenas 500 dessas de fato evadiram da convocação (TOUREK, 2013; TOUREK, 2013b). A APL foi também ator principal em algumas das mais importantes ações anticomunistas realizadas entre o final dos anos 10 e durante os anos 20, como nas chamadas *Palmer raids*[118], em 1919, e durante o *Lusk Committee*[119], entre 1919 e 1920. O movimento foi oficialmente desarticulado em 1919, com o fim da guerra, mas continuou atuando durante muitos anos através de

[117] Sindicato de inspiração socialista e anarquista fundado em Chicago. Nos anos 20 chegou a ter 150 mil membros pelos EUA.

[118] *Palmers raids* foram uma série de operações realizadas a mando do presidente Woodrow Wilson entre novembro de 1919 e janeiro de 1920, destinadas a identificar, prender e deportar líderes socialistas, comunistas e anarquistas. Mais de 10 mil pessoas foram presas, com cerca de 600 estrangeiros deportados, incluindo muitas lideranças do movimento sindical e dos trabalhadores (AVAKOV, 2006).

[119] O *Lusk Committee* foi uma comissão parlamentar investigativa realizada no estado de Nova Iorque a pedido de industriais. A comissão foi criada para investigar a subversão de esquerda no estado e tomar medidas para que essa ameaça fosse neutralizada. A comissão mobilizou o trabalho investigativo do *Bureau of Investigation* do Ministério da Justiça, além de informantes e espiões da APL, e teve como alvos sindicatos, escolas, embaixadas e a imprensa alternativa (SMITH, 1922, p. 313-323).

organizações e associações menores ligadas à direita, fornecendo, por exemplo, muitos membros para a Ku Klux Klan e outros movimentos reacionários (HAGEDORN, 2007).

Ao final da guerra, o *establishment* de inteligência nos EUA não é mais uma colcha de retalhos, mas sim uma organização com operação burocrática relativamente bem estabelecida — apesar de muito redundante institucionalmente, com esforços duplicados em vários órgãos paralelos — e agentes na Europa, Ásia e mesmo nos EUA. No período entreguerras essa estrutura continua em operação, mas com importância diminuída, tanto em termos de pessoal como em termos de recursos. Trocas no comando do Departamento de Guerra e de Justiça arrefecem as temperaturas, diminuindo a cada ano mais a atividade da inteligência até por volta da metade dos anos 30. Nesse período, a inteligência militar foca seu trabalho em prosseguir a cooperação com outras agências do governo dos EUA, como a *Drugs Enforcement Agency* (DEA) e o *Bureau of Investigation* (BI)[120], principalmente em casos relacionados à subversão interna e ao monitoramento do crescente movimento de esquerda pelos EUA e pelo mundo, assim como em casos internos de fraude, crime organizado e corrupção no governo dos EUA (RUDMAN; BROWN, 1996, FINNEGAN; DANYSH, 2015, p. 40-49).

Com o aumento das tensões pelo mundo nos anos 30, o governo dos EUA torna a segurança das comunicações militares e do governo uma prioridade — através do *Federal Communications Act* de 1934, fazendo com que a criptologia receba atenção e orçamento especiais, sendo um dos únicos ramos da atividade da inteligência militar que no período de "paz" teve importância crescente e um desenvolvimento técnico constante. Até o começo da Segunda Guerra Mundial ocorreria um esforço interno constante da inteligência interna no setor de códigos, assim como também estava em curso uma caçada a qualquer movimento ou indivíduo que pudesse ser julgado como ameaça à ordem social. Ao mesmo tempo, ocorreria uma relativa calmaria nos serviços de inteligência voltados ao exterior — que, por exemplo,

[120] Interessante notar que tanto o DEA quanto o FBI terão diretores que ocuparão o cargo por muito tempo, acumulando muito poder, chegando a ser considerados czares do combate às drogas e da inteligência interna, respectivamente. Ambos são personalidades muito importantes na política dos EUA e professavam um incrível racismo, o que provavelmente influenciou muito de seu trabalho. Harry Anslinger comandou o *Federal Bureau of Narcotics*, hoje *Drugs Enforcement Agency*, de 1930 a 1962, sendo um dos principais proponentes da criminalização da maconha. Anslinger foi autor rotineiro — inclusive como testemunha no Congresso — de comentários como: "There are 100,000 total marijuana smokers in the US, and most are Negroes, Hispanics, Filipinos, and entertainers. Their Satanic music, jazz and swing, results from marijuana use. This marijuana causes white women to seek sexual relations with Negroes, entertainers, and others." (SOLOMON, 2020). No BI, hoje FBI, J. Edgar Hoover comandou o órgão de 1924 até a sua morte em 1972, se envolvendo durante todo esse período em diversos escândalos relacionados à sua política de perseguição contra a esquerda, contra o movimento negro e outras minorias. Hoover foi promovido a diretor da inteligência interna por seu papel no combate aos comunistas, principalmente pela coordenação do trabalho policial nas já mencionadas *Palmer raids* (POTTER, 2019; ELLIS, 1994).

regridiriam a um estado anterior em que a maior parte da coleta de inteligência do estrangeiro seria obtida através dos serviços de inteligência aliados, o que novamente mudaria com o ímpeto expansionista dos regimes nazista alemão e fascista italiano durante a metade final dos anos 30. Como veremos, nos anos seguintes, a atividade de coleta, processamento e disseminação de informações será novamente elevada a uma posição de extrema importância e se tornará parte principal do esforço de guerra estadunidense, gerando consequências que resultarão na vitória da guerra pelos aliados dos EUA e na criação do cenário de fundo que possibilitou o florescimento das chamadas Tecnologias da Informação e Comunicações (TICs).

Inimigos informacionais, a análise de sistemas e a cibernética

Aeronáutica, criptologia, telégrafo, rádio, aviões, câmeras, cartões perfurados. Fábricas, associações cívicas conservadoras de caráter paramilitar, perseguição a movimentos sociais contestadores da ordem e a estrangeiros, agentes infiltrados, interrogatórios violentos, censura militar e controle estatístico de populações. Como vimos, no começo do século XX, a resolução de conflitos praticada pelo governo dos EUA dependeu tanto de equipamentos físicos — novíssimas e potentes invenções da época — como de tecnologias essencialmente políticas, como a vigilância e a repressão policial, que garantiram a estabilidade necessária para a produção em massa do próprio *hardware* de guerra e da nova estrutura de sociedade que estava em construção à época — marcada, por exemplo, por uma grande influência do governo dos EUA na vida política e social internacional. Esta subseção trata de como paralelamente ao desenvolvimento da atividade de coleta de informações militares, no curso da Segunda Guerra Mundial e começo da Guerra Fria, a comunidade científica fará ativamente uma espécie de meio de campo entre os militares e a indústria. Essa colaboração estreita refinará os conceitos de informação, comunicação e controle, possibilitando a realização — não sem percalços e uma quantidade exorbitante de violência — de alguns dos sonhos tecnopolíticos mais selvagens dos militares, como a vigilância irrestrita realizada hoje por membros da inteligência militar estadunidense dos hábitos individuais de cada usuário da internet.

Meses antes do estouro da Segunda Guerra, com a Europa em tensão permanente, no dia 26 de junho de 1939, o presidente Franklin Delano Roosevelt publica um decreto que dá "autoridade absoluta" para que os três órgãos centralizadores de inteligência (a *Military Information Division*, do Departamento de Guerra; o *Bureau of Intelligence*, do Departamento

de Justiça; e o *Office of Naval Intelligence*, do Departamento da Marinha, até então não integrado ao Departamento de Guerra) conduzam conjuntamente operações visando a manutenção da "segurança interna"". Um dos muitos abusos cometidos pelo governo dos EUA nessa época, essa operação conjunta é responsável pela compilação nos meses pré-guerra das chamadas *ABC lists*, arquivos de cartões perfurados similares aos utilizados nas Filipinas, contendo o perfil de centenas de milhares de indivíduos estadunidenses, japoneses, italianos e russos suspeitos de serem comunistas ou simpatizantes do inimigo. Através das listas e perfis, 31.899 pessoas foram presas provisoriamente sem o devido processo legal por todos os EUA com o começo da Segunda Guerra Mundial. Durante a guerra, a comunidade interna de inteligência participaria ativamente de muitas outras operações do tipo, como no caso da Ordem Executiva 9066 de 1942, decreto presidencial que previa o encarceramento quase total da comunidade japonesa nos EUA e que resultou na prisão, deportação ou internação em campos de concentração de por volta de 100.000 descendentes de japoneses (NIIYA, 2020).

Por volta da segunda metade de 1940, com a queda da França e dos Países Baixos para o regime nazista e com a Inglaterra sob ataque aéreo implacável[121], a sociedade estadunidense começa a exibir sinais de ansiedade com a situação, com parte expressiva da comunidade técnico-científica se mobilizando publicamente a favor do esforço de guerra. Em 1940 são criadas diversas associações e grupos de trabalho formados por cientistas, engenheiros e matemáticos — como o Comitê de Emergência da *American Mathematical Association* (GALISON, 1994, p. 234) ou o comitê de referência em estudos nucleares da *National Academy of Sciences* (COCHRANE, 1978, p. 382-400) — que voluntariamente desenvolvem protótipos de equipamentos e oferecem seus serviços para as forças armadas aliadas. Eminentes cientistas como o engenheiro Vannevar Bush[122]; o físico Carl Compton[123]; o químico James Conant[124]; e o físico Frank Jewett[125] abordam pessoalmente o presidente Franklin Delano Roosevelt ao final de 1940, reivindicando a criação de um órgão específico do governo destinado à coordenação entre ciência e esforço de guerra (DANIEL GROSS;

[121] Mergulhando um pouco nos acontecimentos do período, Peter Galison descreve o clima infernal na Inglaterra em 1940: em 13 de agosto, 1500 aviões alemães bombardeiam aeroportos e fábricas de aviões britânicos; em 7 de setembro, 498 civis morrem alvos de ataques aéreos; oito dias depois, em 15 de setembro, 230 bombardeiros e 700 caças são mandados contra Londres, Southampton, Bristol, Cardiff, Liverpool e Manchester (GALISON, 1994, p. 229).

[122] Professor do *Massachusetts Institute of Technology* (MIT) e então presidente da *National Advisory Committee for Aeronautics* (NACA).

[123] Presidente do MIT.

[124] Presidente de Harvard.

[125] Presidente da Bell Laboratories e da National Academy of Sciences.

BHAVEN SAMPHAT, 2020). Roosevelt, que durante a Primeira Guerra Mundial havia servido como segundo no comando civil da Marinha dos EUA, autoriza imediatamente a criação de tal órgão, inicialmente uma estrutura provisória nomeada *National Defense Research Committee* (NDRC) e financiada pelos fundos de emergência da presidência dos EUA.

Após um ano de operação, o NDRC é substituído pelo *Office of Scientific Research and Development (OSRD)*, criado por ordem executiva e aprovado pelo Congresso. Roosevelt escolhe Vannevar Bush[126] para a presidência do novo órgão, e lhe dá autonomia e um polpudo orçamento. Como parte das atividades principais do OSRD — e antes do NDRC — estão o levantamento sistemático das necessidades militares junto aos comandantes das forças e junto ao resto do estamento do estado, a especificação de tecnologias e equipamentos a serem desenvolvidos, a coordenação entre os laboratórios de pesquisa e a indústria e, por fim, o financiamento tanto dos laboratórios quanto da indústria. Nesse período, alguns laboratórios espalhados pelos EUA se tornam gigantes, sendo responsáveis por conduzir pesquisa e desenvolvimento com o financiamento do Estado em uma escala sem precedentes até então (GALISON; HEVLY, 1992). Alguns exemplos de instituições tornadas super-laboratórios são o *Jet Propulsion Laboratory,* do *California Institute of Technology* (CalTech); os *Radiation Laboratory,* do MIT e da Universidade da Califórnia, em Berkeley; o *Applied Physics Laboratory,* da Universidade John Hopkins; e os laboratórios das empresas Bell Labs e RCA. Outras muitas instituições científicas são estabelecidas em parceria entre o governo e a iniciativa privada, incluindo diversos projetos em localizações totalmente secretas, como a rede de laboratórios que compuseram o Projeto Manhattan, das quais o Laboratório Nacional de Los Alamos, no Novo México, é o mais famoso. Se desde meados do século XIX há nos EUA um movimento de estreitamento de relações entre governo civil, militares, academia e indústria (FORTUN; SCHWEBER, 1993) — principalmente voltado para a realização de projetos de infraestrutura e projetos emergenciais de guerra (RUTTAN, 2006) —, com o estouro da Segunda Guerra Mundial, o processo de interligação entre academia, indústria e forças militares intensifica-se muito, afetando todo o aparato militar estadunidense, especialmente a atividade da coleta e processamento de dados de inteligência. Até a Segunda Guerra o governo dos EUA foi um dos principais compradores de novas tecnologias — como pode ser observado no caso do avião, da câmera fotográfica, do rádio e

[126] Famoso à época — anos 30 — por haver criado um dos primeiros computadores, o analisador diferencial analógico, utilizado principalmente para prever trajetórias de projéteis em simulações balísticas (OWENS, 1986).

dos cartões perfurados, imediatamente adaptando tais tecnologias para a utilização militar relacionada à manutenção da estabilidade política. A partir de 1939, no entanto, o governo passará a se envolver direta e ativamente no processo de concepção e desenvolvimento de novas tecnologias de guerra, de comunicações e de controle social, assumindo papel central para que tais projetos se tornem realidade.

Em meio ao aumento da atividade militar na Segunda Guerra e paralelamente à mobilização científica de guerra, o Departamento de Guerra é novamente remodelado através dos *War Powers Acts* de 1941 e 1942, para refletir as necessidades de inteligência voltadas ao exterior. Essa legislação dá autoridade absoluta para que o presidente crie, reorganize ou desmonte quaisquer agências do governo que a autoridade executiva julgar necessário. É criada dentro do MID, em 1941, uma seção denominada *Special Branch*, destinada a coordenar todas as informações interceptadas, criar relatórios a partir destas e repassar rápida e seguramente tais relatórios para as autoridades que possam precisar de tais informações. Para a realização de tal serviço que se torna muito importante após a quebra dos códigos criptográficos nazistas, o *Special Branch* inicialmente recruta dezenas de advogados das melhores bancas de advocacia dos EUA. Como na Primeira Guerra, durante os primeiros anos do conflito persistem os problemas com a falta de pessoal especializado e, por isso, logo são criadas diversas novas escolas para o treinamento de pessoal de inteligência, como a *Army Air Forces Intelligence School*, na Pensilvânia, especializada em inteligência aérea, a *Military Intelligence Training Center*, em Maryland ou a *Military Intelligence Service Language,* que, ao final da guerra, terá formado mais de 5.000 soldados na cultura e idioma japonês (FINNEGAN; DANYSH, 2015, p. 65-68). Nessas reorganizações de 41 e 42, o presidente dos EUA — seguindo sugestão de William Stephenson, maior autoridade da inteligência militar britânica — cria uma agência que nasceria com o destino manifesto de eventualmente unificar os esforços de inteligência militar dos EUA, terrivelmente fragmentados por toda as forças armadas e no Departamento de Guerra. Inicialmente, tal agência tem o nome de *Coordinator of Information* e é ligada diretamente à Presidência; mais tarde, em 1942, ela é renomeada para *Office of Strategic Services* e, posteriormente, em 1947, novamente para *Central Intelligence Agency* (CIA). Esta organização é dirigida por William J. Donovan e nasce com o objetivo de conduzir operações de coleta de inteligência no exterior, operações especiais como assassinatos seletivos, operações de desinformação e operações de guerrilha e paramilitares no exterior (SPECTOR; 2007).

A partir dessa reorganização que acontece no curso da guerra, a operacionalização dos grampos de comunicações, assim como a proteção das comunicações aliadas seria principalmente executada por uma nova agência subordinada aos Signal Corps e paralela a MID, a *Signals Security Agency* (SSA). Em cooperação com o OSRD, com cientistas e com a indústria, a SSA ficará responsável por produzir as máquinas codificadoras que serão distribuídas para todas as unidades aliadas, assim como todos os computadores utilizados nas tentativas de quebra da criptografia inimiga. Nesse momento, vemos um aumento vertiginoso no próprio emprego de cientistas e engenheiros para as atividades de processamento da informação militar: nos meses que sucedem o envolvimento dos EUA na guerra, tanto a inteligência militar britânica quanto a estadunidense começam um esforço intenso a fim de quebrar os códigos utilizados pelos governos do Eixo, utilizando-se de empresas privadas de consultoria científica e de batalhões de milhares de mulheres operadoras de tabelas e calculadoras rudimentares que executavam parte da computação necessária para a realização da descriptografia de mensagem.

Com o OSRD contratando, entre outras empresas, a Bell Labs e suas melhores equipes para o esforço da quebra de códigos inimigos, a partir de 1943 as informações interceptadas em cabos de telégrafo, rádio e correios seriam descriptografadas com sucesso notável, fornecendo aos comandantes aliados um ponto de vista privilegiado de onde podiam observar secretamente os movimentos dos inimigos (MUNDY, 2017). O sucesso na quebra da segurança da comunicação dos inimigos trouxe alguns novos problemas à tona, que, por sua vez, também só puderam ser resolvidos através da atuação do OSRD como coordenador entre cientistas e militares. Em primeiro lugar, fica evidente que, se é possível para os Aliados quebrarem os códigos do Eixo, o Eixo também poderia quebrar os códigos dos Aliados. Para lidar com tal problema, os cientistas a serviço das tropas Aliadas desenvolvem uma variedade grande de formas de codificação que podem ser combinadas entre si, além de inventarem dispositivos que inserem informações falsas nas próprias comunicações a fim de dificultar a análise de informações pelo inimigo. O segundo problema importante decorrente da quebra de códigos tem a ver com o fato de que, uma vez quebrados os códigos inimigos, deve-se ocultar dele o fato de seus códigos terem sido quebrados, evitando, assim, que o inimigo descubra que seu código está comprometido e troque-o, exigindo um novo esforço de descriptografia por parte dos Aliados. Para lidar com esse problema foi necessário o desenvolvimento de um método que possibilitasse o uso das informações interceptadas, ao mesmo tempo que se negava ao inimigo as informações necessárias que o permitissem descobrir que suas

comunicações não eram mais seguras[127]. A resolução de tais problemas originou a chamada Teoria da Informação, desenvolvida durante a guerra por vários matemáticos, em especial por Claude Shannon, trabalhando no Bell Laboratories sob contrato da OSRD. Tal teoria introduz várias inovações conceituais, por exemplo, o conceito de *bits* — *binary digits* — como menor quantia de informação possível. A própria ideia de que é possível medir e quantificar informação através da utilização da estatística é também uma das inovações propostas pelos teóricos da informação. Tais conceitos seriam a base para que nos anos do pós-guerra fossem criados os primeiros computadores digitais[128]. V

Ao mesmo tempo, em meio a persistentes bombardeios na infraestrutura europeia e torpedeamentos de embarcações comerciais, coube aos vários órgãos de inteligência militar — com ajuda do OSRD — a tarefa de inventar meios de detectar os aviões e submarinos inimigos e neutralizá-los. Dezenas de projetos de guerra foram realizados nesses temas, focados na detecção automática do inimigo. Para a detecção de aviões e submarinos, investe-se grandes somas de dinheiro no desenvolvimento de redes de radares aéreos e sonares submarinos. Para a resolução desse problema são necessários equipamentos que possibilitem a vigilância permanente do ambiente eletromagnético aéreo e naval, assim como um aparato de transmissão de informações que permita aos comandantes militares saberem rapidamente sobre o curso dos aviões e submarinos inimigos, coordenando-se entre si para deter os equipamentos inimigos de maneira cinética[129]. A ascensão do rádio como método principal de comunicação de curta e média distância fez com que cada unidade militar tivesse uma assinatura de rádio composta pela soma dos padrões de emissão de rádio de todas as unidades, o que também estimulou o desenvolvimento constante de ferramentas de detecção e monitoramento do espectro de rádio inimigo, como microfones de precisão, radares e sonares cada vez mais precisos. Métodos semiautomáticos, porém ainda altamente manuais, de interligar as informações das máquinas eletrônicas com os sistemas de cartão perfurado e de comunicação entre comandantes por rádio também foram alguns dos esforços principais

[127] Um exemplo disso pode ser observado na guerra submarina. A partir de 1943, quando as forças aliadas conseguem quebrar os principais códigos do Eixo, os comandantes aliados passam a saber, por exemplo, a localização de todas as centenas de submarinos U-boat alemães. Se as forças aliadas começassem a atacar todos os U-boats de uma só vez, certamente os alemães entenderiam que tiveram suas comunicações quebradas. Os matemáticos-soldados criaram, então, métodos de atacar que faziam com que os alemães imaginassem que os U-boat foram descobertos de outros modos que não pela quebra da segurança das comunicações. Por exemplo, uma das técnicas utilizadas baseava-se em, dias antes de destruir quaisquer submarinos, as forças aliadas mandavam aviões de reconhecimento sobrevoarem os submarinos várias vezes, indicando aos soldados alemães nos U-boats que eles foram encontrados pelo esquadrão de reconhecimento aéreo e não por outro motivo.

[128] O *paper* de 1948 "A mathematical theory of communication", de Shannon, é considerado o trabalho mais importante no estabelecimento da nascente Teoria da Informação. Ver mais em (SHANNON, 1948).

[129] *Kinetic attacks* é como os militares chamam ataques que utilizam violência física.

realizados à época dentro das forças armadas e nos laboratórios e fábricas sob contrato dos militares, como os laboratórios Bell e a empresa RCA. Os esforços britânicos e estadunidenses combinados na área resultaram no final da guerra em uma cobertura quase total do território europeu pelos sistema de aviso rápido — denominados *early warning systems* — baseados na rede de radares construída.

Norbert Wiener, professor de engenharia no MIT e ex-orientando de Vannevar Bush, propõe, em 1940, para o OSRD outro projeto notável, também na área da automatização militar e da eletrônica. Wiener propõe acoplar o computador analógico diferencial inventado por Bush a um radar e ambos a um canhão antiaéreo, de modo que esses aparelhos se comuniquem: o radar forneceria em tempo real a posição do avião inimigo para o computador, que, por sua vez, bateria os dados da trajetória do avião com um banco de dados de trajetórias humanamente possíveis de serem praticadas pelo piloto e, assim, prediria a trajetória futura mais provável do piloto, direcionando o canhão ao alvo e atirando com a antecedência necessária para que o projétil conseguisse acertar o alvo. O dispositivo visava a resolução da dificuldade da operação de canhões antiaéreos — algo quase impossível de ser realizado manualmente, mesmo por operadores experientes de canhão, já que os pilotos dos aviões mudam suas trajetórias conforme percebem que estão sob fogo inimigo, tornando a situação muito complexa e dinâmica. Desse modo, o sistema funcionava através de uma junção, proposta por Wiener, das ideias básicas da estatística com as noções de feedback, comunicação e controle, sendo toda a comunicação entre os dispositivos realizada através de pulsos precisamente modulados de eletricidade, os quais representariam o estado atual de cada um dos equipamentos da composição. Através da ciência estatística e de um universo amostral artificial de dados representando as possibilidades reais de trajetórias, a informação proveniente do radar eletrônico era categorizada em cursos mais prováveis de acontecimento. Para gerar os dados sintéticos que seriam comparados com a trajetória real do avião, a fim de realizar a classificação e a predição, a equipe de Wiener projetou um simulador de combate aéreo em um galpão, onde um piloto de testes vivia dezenas de milhares de simulações de combate enquanto um computador analisava os combates simulados e guardava todos os dados dos sensores localizados na aeronave e no canhão de simulação em bancos de dados, criando um modelo de mundo artificial povoado por dados relativos a um grande número de possíveis trajetórias que um piloto humano faria (GALISON, 1994; GALISON, 2020).

Criando um sistema que estabelecia uma comunicação e uma comparação entre os dados de trajetórias possíveis do banco de dados e a trajetória atual do piloto, foi possível

computar a diferença -— chamada por Wiener de “erro” — entre o local em que o canhão aponta atualmente e a posição que ele deveria apontar, o que acionaria automaticamente um sistema eletromecânico de engrenagens que moveria o canhão para a posição correta, de modo que o tiro fosse dado com precisão. Apesar do grande avanço científico e tecnológico do projeto, o dispositivo não foi utilizado na guerra, pois, ao final do conflito, ele era capaz de prever aproximadamente dez segundos da trajetória de pilotos reais, dez a menos do que seria necessário para a efetividade da máquina. Wiener e outros cientistas e engenheiros da época nomearam de “controle” a ideia de utilizar o erro calculado entre o estado atual e o estado previsto desejado do sistema, com finalidade de, através dessa medida, atuar para corrigir o estado atual, de modo que ele se aproximasse mais do estado desejado.

O trabalho de Wiener em sua arma antiaérea automática beberia muito de uma série de discussões que Wiener participou em vários fóruns de discussão científica, principalmente as chamadas *Macy’s Conferences* e as reuniões da sociedade científica chamada *Teleological Society*. As *Macy's Conferences* foram uma série de encontros realizados de 1941 a 1950, com o objetivo de estimular a interdisciplinaridade e a conversa entre diferentes ramos das ciências, principalmente voltados ao funcionamento da mente e do pensamento. Foram convidados eminentes psicólogos, como Warren McCulloch; antropólogas, como Margaret Mead e Gregory Bateson; neurologistas, como Arturo Rosenblueth; matemáticos, como Von Neumann e Walter Pitts; entre muitos e muitas outras intelectuais (PIAS, 2016). Um dos primeiros palestrantes foi Wiener, que apresentou a sua proposta de ciência cibernética. Wiener acreditava que sua ideia de modelo cibernético — como vimos, baseado na junção de estatística, informação, comunicação e controle — podia servir como um modelo geral para a predição do comportamento humano ou animal. Além disso, Wiener também postulava que o modelo cibernético seria a base de uma nova era tecnológica que seria marcada pela criação de máquinas híbridas biológico-eletrônicas ou biológico-eletromecânicas. Tais máquinas dependeriam do feedback humano-máquina e poderiam ser construídas, pois Wiener e seus colegas acreditavam que, para sabermos o suficiente de modo a podermos exercer controle sobre determinado sistema[130], bastaria que estudássemos — por meio de simulação ou observação — como o sistema responde a determinados estímulos, mapeando as relações possíveis entre as entradas (estímulos) e saídas (respostas) do sistema. Esse método, nomeado na época de análise de sistemas, prevê que sistemas complexos sejam modelados como “caixas-pretas” constituídas de uma entrada, uma

[130] Modular os estímulos de entrada do sistema de uma maneira específica de modo a gerar uma resposta desejada de antemão.

etapa de processamento (onde ocorre de algum modo a decisão de como o sistema lida com a entrada) e uma saída. O modelo cibernético de Wiener sugere a ligação da saída do sistema em sua entrada, de modo que a diferença entre as duas seja o erro do sistema, que, por sua vez, é utilizado como elemento de controle, reorientando o sistema por meio de uma alteração nos estímulos de entrada baseada na magnitude do erro. Na análise de sistemas e em sua filha, a cibernética, a análise de sistemas complexos se dá através da quebra desses sistemas maiores em diversos subsistemas menores, que, por sua vez, podem ser novamente abordados como caixas-pretas e testados em busca de relações de entrada-saída. A possibilidade da quebra de sistemas grandes e complexos em menores e mais simples também prevê a abordagem inversa: a criação de sistemas de comportamento complexo através da composição de vários sistemas mais simples.

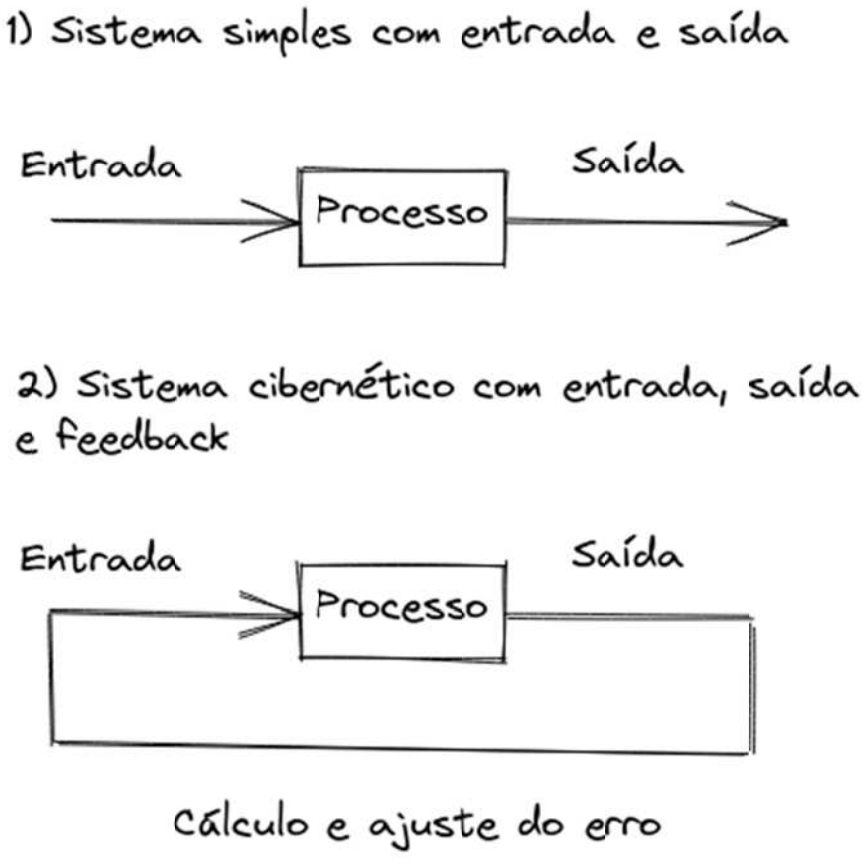


Imagem 12 - Diagramas representando um sistema comum (1) e um sistema cibernético (2) (Fonte: elaboração própria.)

Tanto nas discussões das *Macy's Conferences* quanto na *Teleological Society*, os trabalhos realizados em conjunto pelo matemático Walter Pitts e pelo psicólogo Warren

McCulloch serão muito convergentes com os de Wiener, assim como os de Claude Shannon na Bell Labs, mostrando grande potencial da análise de sistema e da cibernética para o estudo de fenômenos complexos biológicos. Pitts e McCulloch irão, em 1943, propor com base nessas ideias o primeiro modelo matemático de um neurônio e de uma rede de neurônios, ambicionando representar através desses o funcionamento elétrico do pensamento. Utilizada até hoje como base em sistemas de inteligência artificial, a "rede neural" de McCulloch-Pitts será modelada através da observação de diversos sistemas biológicos, como os neurônios alfa-motores humanos e o córtex visual de ratos, e funcionará matemática e conceitualmente de modo muito semelhante ao preditor antiaéreo de Wiener. Projetada para reconhecer padrões e entender diferenças como o cérebro, a rede neural de McCulloch-Pitts é constituída de diversos neurônios matemáticos que, ao receberem determinado estímulo, deverão em conjunto tomar uma decisão a fim de gerar um resultado de saída, normalmente uma decisão sobre a qual categoria pertence uma determinada entrada[131].

Na Marinha dos EUA também ocorre um movimento que impactará mais tarde todo o Departamento de Defesa do pós-guerra. A partir de 1940, são conduzidos ao setor de operações — o mais importante da Marinha durante a guerra — dezenas dos melhores estudantes de universidades como Harvard e Universidade da Califórnia, em Berkeley. O grupo, também muito influenciado pelas ideias da análise de sistemas e da teoria do controle, proporá interpretar os problemas de logística da Marinha em termos de sistemas e subsistemas que interagem uns com os outros e que devem ser controlados de modo a estabilizarem-se em um estado de equilíbrio desejável, compatível com os objetivos dos comandantes militares. Dentre os problemas que o grupo trabalhou utilizando essa abordagem, estão a descoberta e o

[131] Em um "período de aprendizado", apresenta-se para a rede neural um banco de dados contendo relações de causalidade descritas de forma matemática (através de *funções* matemáticas que mapeiam situações à categorias); esse banco de dados de treinamento é basicamente uma tabela contendo duas colunas: uma representando as entradas hipotéticas a serem utilizadas no treinamento, e outra representando que saída (categorias) é esperada para cada entrada hipotética. Cada linha na tabela conterá, portanto, uma situação hipotética associando a categoria correta para determinada entrada. Cada neurônio da rede é representado por um valor matemático chamado peso, que inicialmente assume valores aleatórios. Durante o treinamento, as situações da tabela descrita acima serão apresentadas uma a uma para a rede neural, que realizará uma computação simples (como verificar se o valor se encontra dentro de um intervalo ou acima de um limite) e decidirá por um resultado (saída/categoria). Se o resultado dado pela rede for diferente do previsto na tabela de treinamento, calcula-se o erro através da subtração do valor dado pela rede do valor esperado, muda-se o peso de cada neurônio com base na magnitude do erro e, em seguida, apresenta-se uma nova situação para a rede neural, que deve novamente classificar a entrada em alguma categoria, fornecer esse resultado como saída e avaliar novamente o erro, mudando os pesos da rede. Após a apresentação de várias situações e a realização de várias correções nos pesos dos neurônios, o erro deve ficar cada vez menor, representando que a rede "aprendeu" a diferenciar entre as categorias e dados apresentados durante o treinamento. Com menos erros, pode-se terminar a fase de treinamento da rede. Durante a operação *live* da rede neural, começa-se a apresentar dados de situações reais (não necessariamente contidas na tabela de treinamento) e espera-se que o sistema seja capaz de classificar corretamente as entradas reais nas categorias necessárias, mesmo que as situações reais difiram um pouco das apresentadas no treinamento (HAYKIN, 1999).

monitoramento de submarinos alemães, assim como a decisão sobre quanto bombardear determinadas áreas a fim de garantir a rendição do inimigo (FORTUN; SCHWEBER, 1993). Desse grupo de jovens oficiais viciados em informação, apelidados de *whiz kids*, seu representante máximo será Robert McNamara, que foi presidente da Ford após a guerra, até ser escolhido como secretário de Defesa durante a maior parte dos anos 60 e, posteriormente, presidente do Banco Mundial até 1981. Apelidado de modo elogioso pelo senador republicano racista Barry Goldwater de ""uma máquina IBM com pernas"[132] (ROSENZWEIG, 2010), McNamara é considerado um dos pais da disciplina *policy analysis*[133] — análise de políticas — por tê-la institucionalizado em praticamente todo o governo dos EUA durante seus anos à frente do Departamento de Defesa e do Banco Mundial.

Nos anos pós-guerra, a União Soviética emerge como uma das vencedoras do conflito e como uma grande potência militar, industrial e tecnológica; a China se torna socialista graças ao triunfo das forças de Mao Tsé-Tung; e vários países pela América Latina, África e Ásia se encontram em agitação esquerdista ou anticolonial. Apesar dos inimigos Japão, Itália e Alemanha estarem liquidados, a ameaça comunista parece mais forte do que nunca, o que leva a novas mudanças no aparato militar estadunidense. O governo dos EUA, sob forte influência da pressão anticomunista, das ideias de Vannevar Bush e do presidente[134], assim como por pressão da própria indústria, resolve continuar nos anos seguintes à Segunda Guerra realizando massivos investimentos em tecnologias militares e de defesa. Se o tempo de "paz" entre a Primeira e a Segunda Guerra foi marcado por um relativo arrefecimento da atividade de inteligência, o período da Guerra Fria foi marcado pelo contrário: uma expansão desenfreada dos esforços de coleta de informações militares, potencializada pelas novas tecnologias inventadas durante a guerra e pelo medo causado pelo fortalecimento dos comunistas por todo o mundo.

A nova era das organizações cibernéticas

Após a Segunda Guerra Mundial, o Departamento de Guerra é renomeado Departamento de Defesa, o que reflete uma mudança retórica relacionada à condenação pública da guerra e ao discurso da nova Organização das Nações Unidas (ONU) e do próprio

[132] O senador também se referia a McNamara como "o melhor secretário da defesa de todos os tempos".
[133] Também considerada filha/irmã da análise de sistemas.
[134] Como pode-se observar pela influência duradoura do relatório *Science: the endless frontier*, escrito por Bush para o presidente Roosevelt, em 1945, pedindo que o último organizasse instituições que garantissem a continuidade no pós-guerra da cooperação entre ciência, militares e indústria.

presidente FDR, que assevera que cada país tem direito a sua soberania territorial e política — transformação linguística que coloca a palavra guerra como algo ofensivo e proibido[135]. A antiga OSS — responsável nos anos finais da guerra e durante o final dos anos 40 por operações especiais de coleta de informação no exterior, assim como desinformação, operações clandestinas e a operação de guerrilhas anticomunistas — é renomeada *Central Intelligence Agency* e torna-se uma agência independente, em pé de igualdade hierárquica com o Departamento da Defesa[136]. Nela, é centralizada a coordenação de toda a atividade de inteligência voltada ao exterior (FINNEGAN; DANYSH, 2015, p. 65-68). Já nos primeiros anos de funcionamento, a CIA se estabelecerá como um braço policial da política externa estadunidense, desenvolvendo uma série de operações clandestinas visando o controle do ambiente político mundial, o que seria realizado principalmente através da manutenção de um ambiente de negócios favorável aos empresários estadunidenses e da neutralização sistemática de tentativas de mudança da ordem social que pudessem afetar ou o governo dos EUA ou os interesses de seus homens de negócio[137].

Como resultado do cruzamento dos acontecimentos relatados na comunidade de inteligência e das ideias que se originaram com a aproximação entre os militares e a comunidade científica, nos anos 50 o governo dos EUA e, em especial, a *Military Informations Division*, agora seção de inteligência do *Joint Chiefs of Staff* do Departamento de Defesa, formulará um plano de inspiração cibernética para a operação geral da atividade de

---

[135] Em *A era dos extremos,* Hobsbawm relata que, até a Segunda Guerra Mundial, era sentimento comum entre os homens desejar lutar em uma guerra. Havia na Europa uma crença disseminada em praticamente todas as classes de que a experiência da guerra seria formativa para o caráter masculino (HOBSBAWM, 1995).

[136] O Departamento de Defesa e os militares ainda manterão grande influência sobre a CIA, mesmo com sua suposta independência. Durante a segunda reorganização sofrida pelo Departamento de Guerra no curso da Segunda Guerra Mundial, o *General Staff* do DoW será substituído por uma estrutura semelhante chamada de *Joint Chiefs of Staff*, que reunirá os representantes mais graduados de cada umas das partes principais das forças armadas e que não só executivamente administrarão as forças armadas e estruturas auxiliares, como também servirão como conselheiros de segurança do Presidente da República e como formuladores das políticas e prioridades que devem ser seguidas pela CIA.

[137] Somente nos anos 1950, a CIA conduzirá centenas de operações, como a que deu suporte militar e de inteligência à ditadura de Fulgência Batista em Cuba (THOMAS, 1987); ou a operação Gladio, visando o treinamento de tropas paramilitares de extrema direita que deveriam atuar no caso de triunfo eleitoral dos comunistas na Europa (DANIELE, 2005); ou as diversas operações de sabotagem e monitoramento nos novos países comunistas no Leste Europeu; ou, ainda, o suporte militar e de inteligência aos diversos regimes coloniais que enfrentavam nesse momento lutas de independência, por exemplo, no Vietnã, na Indonésia, na Algeria e no Laos (BARNES, 1982). Nessas operações, as tropas e grupos paramilitares de grupos conservadores eram treinados de modo a executarem nas ruas e selvas o combate aos movimentos sociais de esquerda ou contestadores da ordem mundial vigente. Esses grupos paramilitares eram equipados com as tecnologias mais recentes militares estadunidenses e treinados para a utilização de tais tecnologias — como o grampeamento de comunicações ou a colocação de escutas eletrônicas em ambientes alvo — pelas forças armadas dos EUA ou pela CIA.

inteligência. Denominado de *intelligence cycle*[138] — ciclo de inteligência — a inteligência militar seria interpretada conceitualmente como um sistema composto de cinco subsistemas em feedback circular (cada sistema teria como entrada a saída do sistema anterior, sendo ligados de maneira circular e sequencial): os subsistemas seriam o de coleta de informações, o de análise e processamento das informações coletadas, o de produção de conclusões de inteligência com as análises, o de disseminação dessas conclusões para as autoridades necessárias e o de planejamento de novas necessidades de inteligência, que seriam utilizadas para guiar novas coletas.

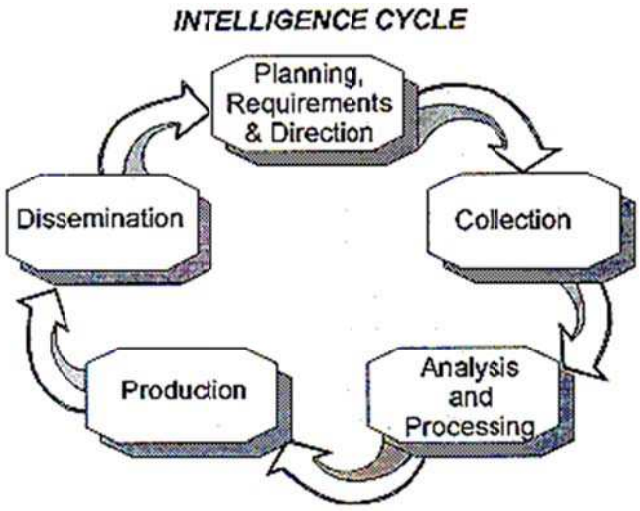


Imagem 13 - O ciclo de inteligência. Notar como cada subsistema recebe como entrada a saída do anterior. (Fonte: INTERAGENCY OPSEC SUPPORT STAFF, 2000)

Na prática, esse modelo formará a base do modo de organização dos serviços de inteligência contemporâneos e será implementado dos anos 50 até por volta do ano 2000, com a CIA[139] executando em um nível superior em termos de autoridade a coordenação de uma série de outras agências, responsáveis cada uma por operacionalizar uma das chamadas disciplinas de inteligência. As principais disciplinas de inteligência foram nomeadas *Human Intelligence* (HUMINT) e *Signals Intelligence* (SIGINT). A primeira compreenderia todas as informações coletadas diretamente através de pessoas e incluiria a informação proveniente de diplomatas, *attachés* militares, informantes, agentes disfarçados, prisioneiros, trabalho policial e forças de operações especiais. Já a SIGINT seria coletada através de meios automáticos de

[138] Para saber mais sobre a origem do termo *intelligence cycle*, consultar (WHEATON, 2011).
[139] Em conjunto com o *Joint Chiefs of Staff* do Departamento de Defesa, o Conselho de Segurança Nacional — órgão formado por cargos comissionados à discrição do presidente —, e a Presidência.

obtenção de dados, como interceptações telefônicas ou de rádio, escutas clandestinas ambientais, câmeras de monitoramento escondidas e sistemas de radares e sonares. Além da coordenação geral da inteligência, a CIA ficaria responsável pela execução da HUMINT, e a *National Security Agency* (NSA), criada em 1952, ficaria responsável pela SIGINT. Mais tarde essas disciplinas dariam origem a várias novas subdisciplinas e agências como a *Imagery Intelligence* (IMINT)[140], *Open Source Intelligence* (OSINT)[141] e *Technical and Scientific Intelligence* (TECHINT)[142]. Mantendo um pouco da pulverização e confusão prévias da organização do setor de inteligência, para além dessas agências que se tornam centrais na chamada "comunidade de inteligência", o Exército, a Marinha e a Força Aérea[143] mantiveram, na segunda metade do século XX, seus próprios serviços de inteligência, muitas vezes realizando esforços paralelos e não coordenados na área.

Como muitas operações de inteligência e de segurança em geral necessitam de elementos que envolvem diversas das disciplinas descritas — por exemplo, quando um informante precisa colocar uma escuta no escritório de um líder soviético, ou no caso em que uma informação interceptada em um grampo telefônico será utilizada para persuadir um agente do inimigo a tornar-se um colaborador —, na maior parte do tempo as agências atuarão em cooperação, sob coordenação do diretor da CIA, do Secretário de Defesa ou da presidência dos EUA, diretamente. A abordagem cibernética e de sistemas permite que esses centros de decisão da comunidade de inteligência coordenem estruturas que implementam o ciclo de inteligência internamente e que estabelecem entre si canais de feedback, de modo a tornar possível a sistematização matemática da operação de inteligência e, de maneira mais geral, a operação da segurança do Estado. Nesse momento ganhará muita importância no Departamento de Defesa[144] a ideia de uma gestão científica e eficiente da segurança, tornando-se um discurso recorrente do DoD e de seus defensores a partir da gestão de Robert McNamara, a "máquina IBM com pernas", como Secretário de Defesa. Esse será um momento ímpar no discurso oficial do governo dos EUA, com a exaltação da potência

---

[140] Responsável pela coleta de inteligência provenientes de imagens aéreas. Em 1961, o *National Reconnaissance Office* é criado para operacionalizar a IMINT gerada pela rede de sensores e pelos aviões de reconhecimento estadunidenses.

[141] Geração de inteligência a partir de fontes abertas como notícias, publicações acadêmicas e congressos científicos.

[142] Composta pela análise de equipamentos e técnicas do inimigo.

[143] Desmembrada do Exército em 1947.

[144] Com uma estrutura complexa, herança de diversos processos históricos, o DoD também adota uma ideia cibernética como norteadora de sua operação como um todo. A partir de McNamara, o modelo *Observe-Orient-Decide-Act*, assim como a ideia de Comando e Controle serão utilizados como bases para uma reformulação no modo de operação do Departamento, conforme exposto no capítulo 1.

científica, tecnológica e matemática das forças de segurança e do próprio governo eclipsando em parte o antigo discurso anticomunista e racista frequentemente proferido pelos oficiais ligados às forças de segurança dos EUA nos 60 anos anteriores. Segundo esse postulado, sendo a máquina de identificação de maus elementos muito precisa e cientificamente gerida e operada, somente aqueles sujeitos e grupos realmente "criminosos" ou "inimigos" seriam perseguidos pelo aparato de segurança estadunidense. Tal visão cai por terra durante a invasão estadunidense do Vietnã, que termina em uma humilhante derrota estadunidense, mesmo com tamanho poderio tecnológico e econômico.

Com três milhões de pessoas empregadas diretamente em 1954 (COLEMAN, 2014) e com uma organização crescentemente cibernética e computadorizada, o DoD necessita dedicar-se cada vez mais a proteger suas próprias informações, o que, combinado com a capacidade ofensiva da utilização das tecnologias informação, gerará as ideas de *information projection* e i*nformation protection*, ambas ideias chave para o conceito de Operações de Informação que surgirá nos anos 90 como evolução das chamadas "operações de influência" ou "operações psicológicas", realizadas pelos militares estadunidenses entre os anos 60 e 90.

Familiarizados com uma história resumida da comunidade de inteligência dos EUA e com alguns dos termos utilizados pelos militares para conceber e operar a atividade prática da inteligência, podemos concluir com alguns pontos que considero importantes sobre a história nos EUA dessas repartições do governo que, antes de tudo, são responsáveis por produzir uma imagem de inimigo:

1) A contemporânea atividade de inteligência esteve ligada desde suas origens ao problema da manutenção da estabilidade política, aliando ao longo de sua história novas tecnologias com novas instituições políticas para atingir os objetivos do momento. No caso estudado, a experiência colonial, a guerra e a centralização do poder político e militar no executivo foram alguns dos catalisadores que atuaram na profissionalização da atividade.

2) O que é considerado informação dentro das forças armadas varia do final do século XIX (quando é estabelecido o primeiro serviço de inteligência estadunidense) ao período inicial da Guerra Fria, nos anos 60. Passamos de um conceito mais relacionado ao levantamento de estatísticas sobre as tropas internas nos inícios da MID, em 1889, para informações de cunho social, psicológico, cultural e político de pessoas suspeitas de terem

sentimentos antiamericanos na MID sob Van Deman dos anos 20, e, então, para informações obtidas através do monitoramento automático do espectro eletromagnético, com os sistemas de radares da Segunda Guerra.

3) A cibernética e a análise de sistemas — resultados de uma aliança entre mercado, ciência e Estado — atuam para juntar todos esses tipos de informação em um só modelo conceitual, transformando a própria comunidade de inteligência e de defesa dos EUA em uma máquina cibernética formada por muitos componentes e vastas proporções.

4) No começo do século XX, a informação é literalmente desprezada pelos comandantes militares na Guerra Hispano-Americana e, em meados dos anos 60, a operação do DoD e da comunidade de inteligência seria quase toda computadorizada e o setor de inteligência, por sua vez, ocuparia uma porcentagem significativa dos esforços das forças de segurança estadunidenses. Conforme a informação foi ganhando importância, as estruturas foram contingencialmente se adaptando, por vezes gerando caos organizacional no setor de inteligência.

No próximo capítulo, apresento as conclusões deste trabalho, seguidas de algumas intuições antropológicas que me ocorreram durante a execução da pesquisa. Por fim, finalizo com algumas questões derivadas dessas intuições antropológicas que ficaram em aberto, as quais podem ser desenvolvidas em pesquisas e artigos posteriores.

CONCLUSÃO

Durante este trabalho, parti de uma investigação acerca da constituição do ambiente informacional proposto pelo DoD, sendo levado a pesquisar como o departamento se organiza e como vivem seus funcionários. Essa pesquisa me levou aos manuais militares, materiais que utilizei para analisar a doutrina militar, especificamente a doutrina do setor de inteligência relacionada ao uso militar da informação. Nesse contexto e investigando os manuais, fui levado a entender em que consistem as chamadas *Information Related Capabilities* (IRCs) e como elas são utilizadas, através das "operações de informação", com finalidade de influenciar o comportamento de pessoas e máquinas. Seguindo a história das operações de informação, chegamos às subdisciplinas de inteligência, chamadas por exemplo de "operações psicológicas", "enganação militar", "operações no ciberespaço" e, no passado ainda mais longínquo, "operações de influência" ligadas à "operações de contrainsurgência". Em busca de uma contextualização histórica ainda mais ampla, o capítulo 3 tratou de uma genealogia da atividade de inteligência e da relação entre militares e informação, relação que se intensificou muito a partir do firmamento de uma estreita aliança entre mercado, Estado e ciência, coordenada pelo governo dos EUA a partir da Segunda Guerra Mundial.

Neste processo, alguns pontos me chamaram mais a atenção. Foram "descobertas" que o trabalho etnográfico "em campo" me trouxe a partir do contato com este "outro" militar com quem estive durante a pesquisa. A primeira descoberta realizada ao longo deste caminho se relaciona com um preconceito que predominava em minha cabeça sobre a atividade militar como um todo. Vivendo no Brasil e, mais especificamente, na periferia da cidade de São Paulo, meus encontros com a polícia — e posteriormente com o exército — sempre me marcaram pela impressão de que os militares seriam ignorantes, com suas ações sempre tendendo para a brutalidade e para a violência autoritária. Minha opinião se somava ao meu conhecimento da história do mundo, de modo que eu generalizava essa impressão, pensando que a ignorância seria uma característica particular dos funcionários de todas as forças militares. Durante a execução da pesquisa, porém, me aproximei do raciocínio utilizado pelos militares estadunidenses e fui — através de um exercício involuntário de alteridade — surpreendido pela profundidade epistemológica do pensamento militar contemporâneo. No entanto, a surpresa foi um tanto atenuada pelo fato de que tal profundidade é utilizada como justificativa lógica e científica para dar continuidade à execução de atos bárbaros por todo o mundo. Na verdade, essa utilização pelos militares de conceitos científicos — provenientes das ciências humanas, em particular, como no caso da discussão cibernética que envolveu a

participação de Bateson, Mead, McCulloch e Pitts, nos anos 50, ou da discussão relacionada à utilização da coerção como política externa, protagonizada por cientistas políticos e analistas de relações internacionais durante a Guerra Fria — acendeu uma luz de alerta em minha mente, pois fica óbvio que avanços epistemológicos, inclusive do campo de ESCT, tais como a proposta de dissolução sujeito-objeto ou o abandono da dicotomia humano-não humano, são temas centrais no âmbito do "ambiente informacional" e dos esforços atuais das forças de segurança dos EUA. Porém, em nenhum manual encontrei uma menção sequer a algum tipo de melhoria no mundo ou de busca pela paz: o Departamento de Defesa realizou a sua própria virada ontológica, transformando a hibridez humano-não humano em arma apontada para nossa própria cabeça e destinada a ser usada para a manutenção das desgraças que são o "pão com manteiga" do status quo.

Tal situação funciona como um chamado à luta, e clama por um maior cuidado e maior exercício da responsabilidade e da capacidade de produzir "saberes localizados" na ciência, inclusive no interior das ciências sociais, campo do saber que possui tantas afinidades e vizinhanças perigosas com as ciências militares. A adoção pelos militares de nossas melhores teorias deveria ser acompanhada por uma adoção nossa das melhores teorias deles, de forma a diminuir a assimetria informacional presente na relação entre ciências sociais e uso da violência pelo Estado. É necessário que o avanço da discussão epistemológica seja acompanhado de novas práticas de responsabilidade e de responsabilização, contra-atacando o militarismo dentro da ciência de forma a minar a lógica autoritária.

Ao longo da pesquisa também me dei conta de que falar sobre a relação entre informação e militares significa falar sobre a história da profissionalização da própria atividade militar ao longo dos séculos XX e XXI. A informação é crucial para a concepção, identificação e monitoramento dos inimigos, e os inimigos, por sua vez, são a razão de viver dos aparatos de segurança. Conforme os militares foram aumentando internamente a importância da ideia de informação, mais "informatizadas" foram se tornando as operações militares, exigindo um desenvolvimento intenso de novas tecnologias e formas organizacionais — como as redes de radares, o ciclo de inteligência ou o *Information Influence Framework* (IIF) — para que as forças de segurança fossem capazes de lidar com a enxurrada informacional crescente causada pela própria operação em constante expansão. A organização chamada de *Joint Chiefs of Staff*, localizada no Departamento de Defesa e chefiada pelos oficiais mais graduados do departamento, terá papel primordial na profissionalização militar estadunidense, atuando como órgão de supervisão da operação das

forças militares, e reorganizando-se com o tempo conforme as necessidades de "segurança" dos EUA mudam. As várias reorganizações do JCS continuamente aumentaram o papel das atividades de inteligência no todo das forças de segurança, chegando ao ponto de que hoje a atividade de inteligência pode ser considerada uma das principais, senão a principal atividade executada pelas forças sob o comando do DoD. O JCS também cumpre o importante papel de homogeneizar a doutrina militar, com uma equipe interna responsável por coletar e analisar os milhares de documentos públicos e secretos que definem a doutrina de cada subcomponente das forças do DoD, criando documentos e manuais que contêm uma versão oficial e relativamente coesa da doutrina militar a ser seguida por cada setor.

Outro entendimento importante — e o meu preferido, por também quebrar alguns de meus preconceitos prévios — se relaciona com a ideia de que os militares são essencialmente um problema para uma sociedade justa, por estarem sempre focados na descoberta e na neutralização de inimigos (fato que estimularia uma paranoia permanente no interior dos órgãos de segurança, criando instituições fechadas e autocráticas). Durante o trabalho, foi possível observar que as coisas não funcionam dessa forma: durante toda a história levantada da atuação dos órgãos de inteligência, vimos que, em todos os momentos em que foram executadas as maiores violência e crimes contra a humanidade — como durante a experiência colonial dos EUA nas Filipinas, durante a Guerra do Vietnã, ou no combate ao comunismo na América Latina entre os anos 60 e 90 — o poder civil dos EUA sempre engajou o conjunto de seu aparato militar e civil na mesma direção, indicando que no mínimo os governantes civis dos EUA compartilhavam em grau muito convergente as paranoias vigentes nos aparatos de segurança, principalmente quando o assunto é o combate ao comunismo e à esquerda. O trabalho mostrou que é necessária uma interação e uma troca intensa entre civis (tanto governo como empresários e cientistas) e militares para a execução de qualquer operação militar. As "operações de informação" são locais privilegiados para observar um mecanismo de guerra híbrido civil-militar em ação, como pode ser observado através, por exemplo, da estrutura da "célula de operações de informação" ou mesmo da história de como os militares aplicaram as chamadas "operações de influência" e de "contrainsurgência": todos esses processos só foram possíveis porque civis atuaram como coordenadores da violência militar. Ao ver de perto as estruturas civil-militares que imaginam e executam o ambiente informacional, a imagem dos EUA como terra do empreendedorismo e da inovação se contorce e revela que o "sonho americano" é, na verdade, um delírio paranoico de guerra.

A seguir, apresento dois resultados frutos da análise da pesquisa etnográfica que realizei. O primeiro diz respeito à correlação entre o aumento do esforço para controle e homogeneização da linguagem referente ao ambiente informacional, e o aumento da comunidade de informação dos EUA. O segundo refere-se à construção da figura do inimigo a partir das práticas que emergem dos manuais e que configuram o ambiente informacional.

Jean Pierre Faye, especialista em totalitarismo, em seu livro *Introdução às Linguagens Totalitárias* (2009), denomina "Ciclotron[145] Goering" o processo em que um conceito específico, o de "Estado Total", vai, a partir de 1930, gradualmente ganhando as mentes e bocas dos políticos, militares e civis alemães até que ele se torne aceitável. Faye descreve as relações entre a circulação do conceito e a criação das condições que fazem com que os nazistas, até então minoritários, consigam consolidar o controle sobre a polícia e as forças armadas. A partir de então, Goering, Ministro do Interior da Prússia, organiza as tropas paramilitares SA e SS como instrumentos paralelos de gestão da segurança pública sob seu comando, instituindo em seguida a Gestapo, órgão de inteligência nazista, cujas atividades causaram temor mesmo em partidários e mecenas nazistas, como o industrial Fritz Thyssen.

Com os inimigos e desafetos políticos dos nazistas transitando sequestrados e encapuzados em trens e caminhões e tal operação sendo operacionalizada militarmente pela SS e pela Gestapo, o Estado Total finalmente se concretiza em termos de instituições e operadores, encarnados nas figuras de Goering e Himmler. A combinação sinistra das operações das SS e da Gestapo também produziu seu próprio órgão de homogeneização de doutrina e conceitos, o jornal semanal interno das SS chamado *Das Schwarze Korps.* Em pouco tempo de operação, no auge do controle político nazista da Alemanha, o corpo editorial do jornal — formado por oficiais influentes do setor de propaganda do partido nazista e das SS — decide que o conceito de Estado Total é inadequado e deve ser substituido por um tal de *Volkish Ganzheit*, este associado a uma "totalidade alemã", transmutando a ideia ainda geral de Estado Total na concepção de um estado total étnico.

Para Faye, tais acontecimentos — que terminam, como sabemos, de maneira terrível — configuram um exemplo do processo com o qual é possível a formação de "linguagens assassinas" (2009, p. XIX). Faye dá ênfase no papel da circulação da linguagem entre subgrupos de comunicação internos à sociedade alemã — como os militares e os industriais — e como a linguagem atua para a formatação de novas comunidades políticas, como no caso dos nazistas. Ao denominar esse processo de "Ciclotron Goering", Faye

[145] Ciclotron é um tipo de acelerador de partículas circular, utilizado para a geração de radiofármacos e para pesquisas em física de alta energia.

pretende chamar a atenção para a acumulação gradual de força que a circulação de determinado conceito no interior de uma comunidade pode causar, assim como uma partícula é acelerada a velocidades cada vez maiores enquanto gira dentro de um acelerador de partículas, em algum momento colidindo com um obstáculo e gerando enorme dano.

O presente trabalho demonstra que a tentativa de homogeneização da linguagem através de manuais, dicionários e doutrinas — o que exige um esforço constante do DoD — atua tanto como uma forma de ação criadora de comunidade (no caso, a comunidade de inteligência, em específico, e os militares, no sentido mais geral) quanto como um dos elementos principais necessários para a operação de fato de um órgão contemporâneo militar de inteligência por essa comunidade. Tal linguagem precisa ser estritamente controlada, de modo a guiar para uma direção específica os esforços organizacionais, assim como o próprio perfil ideológico dos participantes da comunidade. A análise das práticas material-semióticas realizadas pelo DoD em relação à informação mostra que essa organização vem continuamente preparando-se para atuar e para sobreviver em um mundo paranoico repleto de adversários, inclusive dentro do próprio governo e aparato de segurança dos EUA. Esse mundo paranoico implica a necessidade de um investimento cada vez maior no estabelecimento de capacidades sociotécnicas, que, por sua vez, são cada vez mais abrangentes, como é o caso do "ambiente informacional", em que o DoD pretende ser capaz de influenciar integralmente o comportamento de pessoas e máquinas.

Essa homogeneização da linguagem, por sua vez, é fruto de uma intensa colaboração entre o governo civil, a academia e os militares, que conjuntamente criam as bases comuns comunicacionais as quais determinam a ideia de "segurança" atualmente praticada por todo o governo dos EUA. Em outras palavras, a homogeneização da linguagem e do ferramental conceitual, expressa nos manuais e documentos analisados, atua na formatação do Estado estadunidense como um todo, ocasionando, pela complexidade de tal operação tecnopolítica civil e militar, efeitos profundos no modo de vida ocidental contemporâneo:

> Technoscience is the story of such globalization; it is the travelogue of distributed, heterogeneous, linked, sociotechnical circulations that craft the world as a net called the global. The cyborg life forms that inhabit the recently congealed planet Earth (...) gestated in a historically specific technoscientific womb. Consider, for example, only four horns of this multilobed reproductive wormhole:
> 1- The apparatuses of twentieth-century military conflicts, embedded in repeated world wars; decades of cold war; nuclear weapons and their institutional matrix in strategic planning, endless scenario production, and simulations in think tanks such as RAND; the immune systemlike networking strategies for postcolonial global control inscribed in low-intensity-conflict doctrines; and post-Cold War, simultaneous multiple-war-fighting strategics depending on rapid massive deployment, concentrated control of information and communications, and high-intensity, subnuclear precision weapons. (HARAWAY, 2018).

No trecho citado, Haraway coincidentemente faz uma alusão direta às tecnologias e comunidades que apareceram durante a realização desta pesquisa, as considerando justamente como "formas de vida ciborgues", gestadas em um "útero tecnocientífico historicamente específico", formatadoras do que chamamos de "global". O "ambiente informacional" é formado pela combinação de todos esses componentes tecnocientíficos que formam o que Haraway chama de "um dos chifres desse buraco de minhoca reprodutivo multilobo", integrando no "global" a doutrina militar do DoD, e injetando a ordem estadunidense como um *malware* no processo. Assim como o "Ciclotron Goering" e sua perigosa acumulação gradual de força e aceleração, Haraway destaca o caráter autorreplicante, reprodutivo, dos aparatos de conflitos militares, gestado nesse útero que não para de parir "planejamentos estratégicos, produções infinitas de cenários e simulações", continuamente se autoinseminando. Argumento que a pesquisa apresentada aqui retoma a noção de "Ciclotron Goering" e reitera as palavras de Haraway, apontando para uma concomitância entre o aumento dos esforços em controle e homogeneização da linguagem referente ao ambiente informacional e o aumento da própria comunidade de inteligência, seja em número de pessoas, seja em importância e influência.

Outro resultado da análise se relaciona com a "fabricação" de inimigos realizada pelos militares e especificamente pelas seções de inteligência militar. Durante toda a história analisada, os inimigos principais dos militares estadunidenses — e de seus comandantes civis — foram os movimentos de esquerda, principalmente comunistas, ao redor de todo o mundo. Nos diversos documentos e manuais consultados, em nenhum momento é dito que os comunistas são o inimigo. O adversário ou inimigo é sempre referido como algo ou alguém que se opõe à ordem, ao status quo, ou à política externa dos EUA, agindo de maneira complexa e tecnológica, dominando todas as possibilidades de contestação à força dos EUA, inclusive dominando o uso do ambiente da internet para impunemente questionar a

hegemonia estadunidense. O que vai sendo formatada através do imaginário sociotécnico é a imagem do inimigo, que emerge a partir das composições material-semióticas que configuram o ambiente informacional. Porém, imaginação e imagem são partes essenciais da criação:

> O processo de criação passa pela formação de imagem, ou seja, as imagens são fundamentais para a formação de pensamento, ou para ficar com os termos de Zuanon: "A construção de imagens constitui-se em um processo cerebral fundamental [...]. O conhecimento factual necessário para o raciocínio e a tomada de decisão vem à mente na forma de imagens" (Zuanon 2017:605). Elas são de vários tipos e podem se articular: há imagens que representam o presente, as que representam o passado e aquelas que se relacionam à projeção de futuros. As imagens do presente e do passado são decorrentes de ações, percepções, ou seja, estão relacionadas aos sentidos e ao modo de estar no mundo. (MARINI, 2021, p. 16).

A pesquisa mostra que, ao contrário do inimigo ultrarracializado muito presente durante os anos iniciais do aparato de inteligência dos EUA, o inimigo atual é imaginado e criado como um nó que carrega consigo uma rede de relações e lógicas complexas, mostrando uma sofisticação da ideia do inimigo, que também caminha paralelamente a certas idéias correntes nas ciências sociais, como a teoria ator-rede. Tal inimigo complexo e múltiplo — e que se verifica de fato na realidade, como no caso apresentado da hacker Phineas Fisher — atua como um dos principais argumentos para a expansão desenfreada de capacidades que o DoD vem realizando e sobre as quais me refiro acima com a ajuda de Haraway e Faye. A coleta exaustiva de informações sobre tudo e todos auxilia no processo de planejamento e execução de uma operação de informação descrito neste trabalho, por exemplo, através da utilização dessas informações nas etapas em que a "célula de operação de informações" irá simular os possíveis comportamentos do inimigo através da realização dos jogos de guerra. Vemos inclusive que tais jogos de guerra só são possíveis se existem dados dentro do aparato militar estadunidense que possam ser utilizados para a criação de um modelo, mesmo que imperfeito, do inimigo e do seu comportamento. Nesse sentido, para estarem prontos para todas as possibilidades de inimigos, até mesmo não-humanos, a coleta indiscriminada de todo o tipo de informação possível torna-se um modo de sentir e estar no mundo que parte de atividades realizadas no interior de uma instituição militar contemporânea e se espalha por todo o globo, este enorme planeta tão rico em potenciais inimigos.

Finalmente, apresento agora algumas das intuições antropológicas que vieram à tona durante a pesquisa e que configuram questões em aberto que podem ser exploradas em trabalhos futuros. Relacionado ainda à formatação do inimigo, um questionamento que formou-se e não foi resolvido durante a pesquisa concerne ao fato da existência de partes

secretas dos manuais públicos, assim como de manuais totalmente secretos. Uma das partes essenciais da teoria da coerção, apresentada no capítulo 2, é a ideia de que o inimigo tem de saber sobre quais recursos os EUA têm disponíveis para causar-lhe dano, como uma forma de ameaça permanente a pairar. Nesse sentido, seria possível que a publicidade dos trechos dos manuais analisados seja uma composição destinada ao mesmo tempo a formatar a comunidade militar, servir como instrumentos para a operação do dia a dia das forças militares e servir como ameaça aos inimigos?

Mudando de tópico, no começo da minha pesquisa pretendia dar mais atenção aos equipamentos físicos — ao hardware — utilizados para a condução das operações de ciberespionagem; no entanto, a dificuldade de encontrar insumos para a realização de tal tipo de pesquisa, assim como a complexidade dos próprios termos iniciais desta pesquisa (como "ambiente informacional", "doutrina" e "operações de informação") me levaram a realizar um trabalho mais baseado nos conceitos, lógicas e na história, do que de fato nos equipamentos, apesar de ter tentado por vezes evidencia-los. A própria ciberespionagem foi deixada em segundo plano com o conjunto das operações de informação assumindo o protagonismo na pesquisa. Através da descrição dos conceitos e operações presentes neste trabalho, seria interessante continuar uma investigação sobre as infraestruturas físicas que compõem as práticas material-semióticas, como forma de ampliar e complexificar o mapeamento já realizado.

Outra questão que pode resultar em uma pesquisa instigante relacionada ao tema deste trabalho seria investigar como foi possível que, em meio à tamanha sofisticação para a "operação em ambiente informacional" por parte do aparato de segurança dos EUA, tenha ocorrido um evento como a invasão do Capitólio por militantes trumpistas em 6 de janeiro de 2020. Se a interpretação de tudo o que analisei estiver correta, um evento importante e potencialmente problemático como esse deveria estar sendo monitorado por uma célula de OI, que, por sua vez, deveria ter alertado as forças de controle de distúrbio pertinentes através do documento Matriz de Sincronização de Operação de Informação (MSOI), que detalha todas as necessidades de reforços necessárias caso ocorram determinados cursos de ação. Seria possível que, nesse caso, não tenha sido criada uma célula de OI? Ou então seria possível que essa célula de OI não tenha preparado uma Matriz de Sincronização de Operação de Informação ou não tenha encaminhado-a de maneira correta? Nesse caso, seriam tais atos uma forma de sabotagem interna pró-Trump, de modo a deixar desguarnecido o Capitólio e facilitar sua invasão? Fica evidente de qualquer forma que, nesse caso, ou o DoD não atuou

como deveria — ignorando sua própria doutrina —, ou que existem maneiras de passar por cima ou sabotar internamente a realização de uma operação de informação. Tais possibilidades se encontram com outra convergente e também preocupante, a da realização clandestina de operações de informação, sem que essas passem pelo crivo burocrático oficial, tornando-se impossíveis de serem monitoradas pela sociedade civil. Investigar todas essas possibilidades pode revelar mais sobre como os manuais e a doutrina do DoD estão ou não sendo aplicados.

Seguindo a mesma intuição, me pergunto se a grande movimentação realizada contra a Dilma a partir de 2014, que teve a participação de ONGs como a *Students For Liberty*[146] e o engajamento maciço da grande mídia brasileira e internacional, não pode ter tido relação com uma operação de informação, dado a inclinação à esquerda do Partido dos Trabalhadores, partido de Dilma — ela mesma uma ex-guerrilheira de esquerda. Tal questionamento também vale para o caso da Venezuela, que sofre desde o governo Chávez com sucessivas tentativas de golpe de estado, várias delas envolvendo um componente informacional.

Outra intuição que pode resultar em uma pesquisa politicamente útil se relaciona à possibilidade de estudar o que acontece quando um manual militar destinado à utilização interna das forças de segurança dos EUA circula entre seus inimigos, como indica a situação a seguir, descrita pelo Subcomandante Marcos do Exército Zapatista de Libertação Nacional:

> Esses primeiros anos, 83-85, são muito solitários para esses grupos. Nós vamos aprender a viver na montanha, aprender a lutar, e a esperar que algum dia a revolução estale pelo México. (...) Em termos militares, durante esses anos de montanha, como não temos apoio externo, nem assessoria, nem nada, temos que recorrer à formação militar autodidata, aquela que podíamos dar a nós mesmos, através das experiências que líamos sobre as guerrilhas latinoamericanas, mas sobretudo através dos manuais de guerrilha e contra-guerrilha do exército norte americano. Nós aprendemos guerrilha nos manuais dos Rangers, dos Marines, das Operações Especiais e dos Seals, assim como de todo o aparato do tipo comando militar que há no exército norte americano e na OTAN. Aí aprendemos o que é a guerrilha; o que era o exército regular, aprendemos nos manuais de história militar. - Subcomandante Marcos do Exército Zapatista de Libertação Nacional. (MARCOS; BOT, 1997, p. 56).

Para Marcos, tudo o que os zapatistas aprenderam sobre a guerra, inclusive como luta-la, foi aprendido através do ensino autodidata, utilizando-se dos manuais dos EUA e da OTAN como fontes de aprendizado. Sendo os zapatistas relativamente bem sucedidos

[146] ONG "liberal" e "pró-democracia", que, de modo suspeito, também atuou em golpes de estado na Venezuela e na Ucrânia (DEMOCRATIZE, 2016).

militarmente, informacionalmente e politicamente — no sentido do estabelecimento de uma comunidade política autônoma relevante — estudar a experiência zapatista e a utilização por eles dos manuais estadunidenses tem relevância historiográfica e política. A apropriação do gênero manual por inimigos politicamente motivados, como Phineas Fisher, também figura como uma possibilidade interessante para a continuidade do trabalho, por exemplo para analisar de que forma os manuais se relacionam à formação de comunidades.

Por fim, minha intuição também aponta para um fato que pode ser investigado mais a fundo, o de que o "ambiente informacional" se constitui como parte de uma ecologia paranoica vigente no interior do Departamento de Defesa e da Comunidade de Inteligência. Sendo eu um leitor de ficção científica e especialmente do subgênero cyberpunk, durante muitos momentos da pesquisa eu senti que estava lendo uma ficção como *Neuromancer* ou *Cryptonomicon*. Nessas obras o caos impera na geopolítica internacional e até pequenos grupos de dissidentes têm a capacidade de realizar "operações de informação" sofisticadas. A segurança é exercida principalmente de maneira privada, com o governo agindo a reboque das grandes corporações, que basicamente controlam os governos e os fazem depender dos equipamentos e serviços fornecidos por elas. Nessa toada, uma pesquisa potencial e importante seria a realização de uma investigação para verificar a adoção ou não do termo "ambiente informacional" e das "operações de informação" pela iniciativa privada, e como governos, inclusive o governo dos EUA, reagiriam a isso.

REFERÊNCIAS

100 YEARS OF SUBTERFUGE: THE HISTORY OF ARMY PSYCHOLOGICAL OPERATIONS. [*s. d.*]. **www.army.mil**. Disponível em: https://www.army.mil/article/199431/100_years_of_subterfuge_the_history_of_army_psychological_operations. Acesso em: 3 maio 2022.

ABOUT THE JOINT CHIEFS OF STAFF. 2016. Disponível em: https://www.jcs.mil/About/. Acesso em: 27 abr. 2022.

ACTIVE DUTY U.S. DEPARTMENT OF DEFENSE PERSONNEL NUMBERS FROM 1995 TO 2020. 2020. **Statista**. Disponível em: https://www.statista.com/statistics/232350/us-department-of-defense-personnel-numbers/. Acesso em: 4 maio 2022.

ANDRADE, Dale; WILLBANKS, James H. **CORDS/Phoenix: Counterinsurgency Lessons from Vietnam for the Future**. [*S. l.*]: U.S. Army Combined Arms Center, mar. 2006. Disponível em: https://www.hsdl.org/?abstract&did=483580. Acesso em: 9 maio 2022.

ANDREWS, Jeff. Zumper National Rent Report. 22 nov. 2021. **The Zumper Blog**. Disponível em: https://www.zumper.com/blog/rental-price-data/. Acesso em: 4 maio 2022.

APPY, Christian G. **Patriots: The Vietnam War Remembered from All Sides**. [*S. l.*]: Penguin Publishing Group, 2004.

ARMISTEAD, Leigh (Org.). **Information Operations: Warfare and the Hard Reality of Soft Power**. Washington, D.C: Potomac Books, 2004. Disponível em: https://web.stanford.edu/class/msande91si/www-spr04/readings/week5/io-textbook.pdf.

ART, Robert J.; GREENHILL, Kelly M. **The Use of Force: Military Power and International Politics**. [*S. l.*]: Rowman & Littlefield Publishers, 2015.

ASSANGE, Julian; APPELBAUM, Jacob; MÜLLER-MAGUHN, Andy; ZIMMERMANN, Jérémie. **Cypherpunks: freedom and the future of the Internet**. [*S. l.*]: OR Books, 2012. Disponível em: http://gen.lib.rus.ec/book/index.php?md5=6cfbede8234a35317180e0c77cb869ac. Acesso em: 10 maio 2022.

AVAKOV, Aleksandr Vladimirovich. **Plato's Dreams Realized: Surveillance and Citizen Rights from KGB to FBI**. [*S. l.*]: Algora Publishing, 2006.

BARNES, Trevor. The Secret Cold War: The C.I.A. and American Foreign Policy in Europe 1946-1956. Part II. **The Historical Journal**, v. 25, n. 3, p. 649–670, 1982.

BASHKOW, Ira; RADCLIFFE-BROWN, Alfred Reginald; MURRAY, Hubert. " The Stakes for Which We Play Are Too High to Allow of Experiments": Colonial Administrators of Papua on Their Anthropological Training by Radcliffe-Brown. **History of Anthropology Newsletter**, v. 22, n. 2, p. 3–14, 1995.

BRASWELL, Sean. The Concentration Camps of America's Forgotten War. 22 ago. 2017. **OZY**. Disponível em: https://www.ozy.com/true-and-stories/the-concentration-camps-of-americas-forgotten-war/80333/. Acesso em: 7 abr. 2022.

BRAUDEL, Fernand; CABRAL, Álvaro. **A dinâmica do capitalismo**. [*S. l.*]: Genérico, 1987.

BROWN, A. R. Radcliffe; CAIXEIRO, Nathanael C. **Estrutura e Função na Sociedade Primitiva**. 2ª edição. [*S. l.*]: Vozes, 2013.

BUTLER, DESMOND; GILLUM, JACK; ALBERTO ARCE. US secretly built "Cuban Twitter" to stir unrest. 13 ago. 2021. **AP NEWS**. Disponível em: https://apnews.com/article/technology-cuba-united-states-government-904a9a6a1bcd46cebfc14bea2ee30fdf. Acesso em: 10 maio 2022.

BUTLER, Major General Smedley. **War is a Racket**. 1930. Disponível em: https://ratical.org/ratville/CAH/warisaracket.pdf. Acesso em: 4 abr. 2022.

CAMPBELL, I. C. Anthropology and the Professionalisation of Colonial Administration in Papua and New Guinea. **The Journal of Pacific History**, v. 33, n. 1, p. 69–90, 1998.

CHAIRMAN OF THE JOINT CHIEFS OF STAFF OF THE DEPARTMENT OF DEFENSE. **CHAIRMAN OF THE JOINT CHIEFS OF STAFF INSTRUCTION CJCSI 5705.01G**. [*S. l.*: *s. n.*], 2020. Disponível em: https://www.jcs.mil/Portals/36/Documents/Doctrine/dictionary/repository/cjcsi_5705_01g.pdf?ver=c2xGPHo3JUHiFh954zBJ_g%3D%3D.

COCHRANE, Rexmond Canning. **The National Academy of Sciences: The First Hundred Years, 1863-1963**. [*S. l.*]: The National Academies Press, 1978. DOI 10.17226/579. Disponível em: http://www.nap.edu/read/579/chapter/14. Acesso em: 27 mar. 2022.

COLEMAN, David. **U.S. Military Personnel 1954-2014: The Numbers**. 24 jul. 2014. **Research**. Disponível em: https://historyinpieces.com/research/us-military-personnel-1954-2014. Acesso em: 28 abr. 2022.

CREVELD, Martin Van. **The Rise and Decline of the State**. Cambridge England; New York: Cambridge University Press, 1999.

CREVELD, Martin van. **A History of Strategy: From Sun Tzu to William S. Lind**. [*S. l.*: *s. n.*], 2015. Disponível em: http://gen.lib.rus.ec/book/index.php?md5=e5677106eb62b85006eaf13dda2e8f3e. Acesso em: 5 maio 2022.

CUFFIA, Ashley. Research Guides: United States Army Technical Manuals: A Resource Guide and Inventory: Introduction. 2022. [research guide]. Disponível em: https://guides.loc.gov/us-army-technical-manuals/introduction. Acesso em: 10 maio 2022.

DANIELE, Ganser. **NATO's Secret Armies - Operation Gladio and Terrorism in Western Europe**. [*S. l.*]: Routledge, 2005 (Contemporary Security Studies). Disponível em: http://gen.lib.rus.ec/book/index.php?md5=0716ef2a1a37dc28220832c836ce2f9e. Acesso em: 26 abr. 2022.

DE LANDA, Manuel. **War in the Age of Intelligent Machines**. New York, NY: MIT Press, 1992.

DEMOCRATIZE. **Atlas e Students for Liberty: quem são as pessoas que financiam os protestos do dia 13?** 13 mar. 2016. **O Cafezinho**. Disponível em: https://www.ocafezinho.com/2016/03/13/atlas-e-students-for-liberty-quem-sao-as-pessoas-que-financiam-os-protestos-do-dia-13/. Acesso em: 11 maio 2022.

DEPARTMENT OF DEFENSE. **DoD Directive 5100 Functions of the Department of Defense and Its Major Components**. [*S. l.*: *s. n.*], 2020a. Disponível em: https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/510001p.pdf.

DEPARTMENT OF DEFENSE. **DoD INSTRUCTION 5025.12 STANDARDIZATION OF MILITARY AND ASSOCIATED TERMINOLOGY**. [*S. l.*: *s. n.*], 2020b. Disponível em: https://www.jcs.mil/Portals/36/Documents/Doctrine/dictionary/repository/502512p_2020.pdf?ver=c2xGPHo3JUHiFh954zBJ_g%3D%3D.

DEPARTMENT OF DEFENSE. **Joint concept for operating in the information environment**. Washington, DC: Joint Chiefs of Staff, 2018a. Disponível em: https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joint_concepts_jcoie.pdf.

DEPARTMENT OF DEFENSE. **DoD Strategy for Operating in the Information Environment**. [*S. l.*: *s. n.*], 2016. Disponível em: https://dod.defense.gov/Portals/1/Documents/pubs/DoD-Strategy-for-Operations-in-the-IE-Signed-20160613.pdf.

DEPARTMENT OF DEFENSE. **Joint Publication 3-12 Cyberspace Operations 2018**. [*S. l.*]: Department of Defense Joint Chiefs of Staff, 2018b. Acesso em: 21 mar. 2022.

DEPARTMENT OF DEFENSE. **Joint Publication 3-12 (R) Cyberspace Operations 2013**. [*S. l.*]: Department of Defense Joint Chiefs of Staff, 2013a. Acesso em: 21 mar. 2022.

DEPARTMENT OF DEFENSE. **Joint Publication 3-13 Information Operations 1998**. [*S. l.*]: Department of Defense Joint Chiefs of Staff, 1998. Acesso em: 21 mar. 2022.

DEPARTMENT OF DEFENSE. **Joint Publication 3-13 Information Operations 2006**. [*S. l.*]: Department of Defense Joint Chiefs of Staff, 2006a. Acesso em: 21 mar. 2022.

DEPARTMENT OF DEFENSE. **Joint Publication 3-13 Information Operations 2012**. [*S. l.*]: Department of Defense Joint Chiefs of Staff, 2012a. Acesso em: 21 mar. 2022.

DEPARTMENT OF DEFENSE. **Joint Publication 3-13 Information Operations 2014**. [*S. l.*]: Department of Defense Joint Chiefs of Staff, 20 nov. 2014. Acesso em: 21 mar. 2022.

DEPARTMENT OF DEFENSE. **Joint Publication 3-13 Joint Doctrine for Information Operations 2004 Second Draft**. [*S. l.*]: Department of Defense Joint Chiefs of Staff, 2012b. Acesso em: 21 mar. 2022.

DEPARTMENT OF DEFENSE. **Joint Publication 3-13.1 Electronic Warfare 2007**. [*S. l.*]: Department of Defense Joint Chiefs of Staff, 2007. Acesso em: 21 mar. 2022.

DEPARTMENT OF DEFENSE. **Joint Publication 3-13.1 Electronic Warfare 2012**. [*S. l.*]: Department of Defense Joint Chiefs of Staff, 2012c. Acesso em: 21 mar. 2022.

DEPARTMENT OF DEFENSE. **Joint Publication 3-13.1 Joint Doctrine Command and Control Warfare 1996**. [*S. l.*]: Department of Defense Joint Chiefs of Staff, 1996a. Acesso em: 21 mar. 2022.

DEPARTMENT OF DEFENSE. **Joint Publication 3-13.2 Military Information Support Operations 2011**. [*S. l.*]: Department of Defense Joint Chiefs of Staff, 2012d. Disponível em: www.bits.de/NRANEU/others/jp-doctrine/JP3-13.2C1(11).pdf. Acesso em: 21 mar. 2022.

DEPARTMENT OF DEFENSE. **Joint Publication 3-13.2 Military Information Support Operations 2014**. [*S. l.*]: Department of Defense Joint Chiefs of Staff, 2012e.

DEPARTMENT OF DEFENSE. **Joint Publication 3-13.2 Psychological Operations 2010**. [*S. l.*]: Department of Defense Joint Chiefs of Staff, 2010a. Acesso em: 21 mar. 2022.

DEPARTMENT OF DEFENSE. **Joint Publication 3-13.3 Operations Security 2006**. [*S. l.*]: Department of Defense Joint Chiefs of Staff, 2006b.

DEPARTMENT OF DEFENSE. **Joint Publication 3-13.3 Operations Security 2012**. [*S. l.*]: Department of Defense Joint Chiefs of Staff, 2012f. Disponível em: http://www.bits.de/NRANEU/others/jp-doctrine/JP3-13-3%2812%29.pdf.

DEPARTMENT OF DEFENSE. **Joint Publication 3-13.3 Operations Security 2016**. [*S. l.*]: Department of Defense Joint Chiefs of Staff, 2012g. Disponível em: http://www.bits.de/NRANEU/others/jp-doctrine/JP3-13-3%2812%29.pdf.

DEPARTMENT OF DEFENSE. **Joint Publication 3-13.4 Military Deception 2006**. [*S. l.*]: Department of Defense Joint Chiefs of Staff, 2006c. Disponível em: http://www.bits.de/NRANEU/others/jp-doctrine/jp3_13_4%2806%29.pdf.

DEPARTMENT OF DEFENSE. **Joint Publication 3-13.4 Military Deception 2012**. [*S. l.*]: Department of Defense Joint Chiefs of Staff, 2012h. Disponível em: http://www.bits.de/NRANEU/others/jp-doctrine/jp3_13_4%2806%29.pdf.

DEPARTMENT OF DEFENSE. **Joint Publication 3-13.4 Military Deception 2017**. [*S. l.*]: Department of Defense Joint Chiefs of Staff, 2017.

DEPARTMENT OF DEFENSE. **Joint Publication 3-24 Counterinsurgency Operations 2009**. [*S. l.*]: Department of Defense Joint Chiefs of Staff, 2009. Disponível em: http://www.bits.de/NRANEU/others/jp-doctrine/jp3_13_4%2806%29.pdf.

DEPARTMENT OF DEFENSE. **Joint Publication 3-24 Counterinsurgency Operations 2013**. [*S. l.*]: Department of Defense Joint Chiefs of Staff, 2013b. Disponível em: http://www.bits.de/NRANEU/others/jp-doctrine/jp3_24%2813%29.pdf.

DEPARTMENT OF DEFENSE. **Joint Publication 3-24 Counterinsurgency Operations 2018**. [*S. l.*]: Department of Defense Joint Chiefs of Staff, 2018c. Disponível em: http://www.bits.de/NRANEU/others/jp-doctrine/jp3_24%282018%29.pdf.

DEPARTMENT OF DEFENSE. **Joint Publication 6-0 Doctrine for C4 Systems Support to Joint Operations 1995**. [*S. l.*]: Department of Defense Joint Chiefs of Staff, 1995. Disponível em: http://www.bits.de/NRANEU/others/jp-doctrine/jp6_0%2895%29.pdf.

DEPARTMENT OF DEFENSE. **Joint Publication 6-01 Joint Electromagnetic Spectrum Management Operations 2012**. [*S. l.*]: Department of Defense Joint Chiefs of Staff, 2012i. Disponível em: http://www.bits.de/NRANEU/others/jp-doctrine/jp6_01%2812%29.pdf.

DEPARTMENT OF DEFENSE. **Joint Publication 6-02 Doctrine for Employment of Operational/Tactical C4 Systems 1996**. [*S. l.*]: Department of Defense Joint Chiefs of Staff, 1996b. Disponível em: http://www.bits.de/NRANEU/others/jp-doctrine/jp6_02%2896%29.pdf.

DEPARTMENT OF DEFENSE. **Program Directive for Joint Publication 3-13 Joint Doctrine for Information Warfare 1996**. [*S. l.*]: Department of Defense Joint Chiefs of Staff, 2012j. . Acesso em: 21 mar. 2022.

DEPARTMENT OF DEFENSE. **The Pentagon Papers: The Secret History of the Vietnam War**. [*S. l.*]: Bantam Books, 1971.

DEPARTMENT OF THE ARMY. **Field Manual FM 30-5: Combat Intelligence 1963**. [*S. l.*]: Headquarters Department of the Army, 1963.

DEPARTMENT OF THE ARMY. **Field Manual FM 30-5: Combat Intelligence 1973**. [*S. l.*]: GPO, Washington, DC, 1973

DEPARTMENT OF THE ARMY, THE NAVY, AND THE AIR FORCE. **Field Manual FM 30-28 Armed Forces Censorship 1964**. [*S. l.*: *s. n.*], 1964.

DEPARTMENT OF WAR. **FM 30-25 Military Intelligence: Counterintelligence 1940**. [*S. l.*]: Createspace Independent Publishing Platform, 1940.

DOD WEBSITES. [*s. d.*]. **U.S. Department of Defense**. Disponível em: https://www.defense.gov/Resources/Military-Departments/DOD-Websites/. Acesso em: 27 abr. 2022.

EISENHOWER, Dwight D. **President Dwight D. Eisenhower Farewell Address**. Washington, DC: [*s. n.*], 17 jan. 1961. Disponível em: https://www.eisenhowerlibrary.gov/sites/default/files/research/online-documents/farewell-address/reading-copy.pdf. Acesso em: 21 mar. 2022.

ELLIS, Mark. J. Edgar Hoover and the "Red Summer" of 1919. **Journal of American Studies**, v. 28, n. 1, p. 39–59, abr. 1994.Disponível em: https://doi.org/10.1017/S0021875800026554. Acesso em: 21 mar. 2022.

ENGLISH, Allan; MCKAY, J.R.; COOMBS, Howard; STEWART, Keith. Influence Operations: Historical and Contemporary Dimensions (Les Dimensions Historiques et Contemporaines des Operátions d'Influence), p. 146, 31 jul. 2007.

EVANS-PRITCHARD, E. E. **The Nuer: A Description of the Modes of Livelihood and Political Institutions of a Nilotic People**. [*S. l.*]: Clarendon, 1940. Disponível em: http://gen.lib.rus.ec/book/index.php?md5=cc3c32ec11aa096ca1080c86bed47ebb. Acesso em: 28 abr. 2022.

EXACTLY HOW MANY WASHINGTONIANS WORK FOR THE FEDERAL GOVERNMENT? 19 fev. 2018. **WTOP News**. Disponível em: https://wtop.com/business-finance/2018/02/exactly-many-washingtonians-work-federal-government/. Acesso em: 4 maio 2022.

FAYE, Jean-Pierre. **Introdução às linguagens totalitárias**. 1ª edição. São Paulo: Perspectiva, 2009.

FEDERAL CIVILIAN EMPLOYMENT. 2022. **U.S. Office of Personnel Management**. Disponível em: https://www.opm.gov/policy-data-oversight/data-analysis-documentation/federal-employment-reports/reports-publications/federal-civilian-employment/. Acesso em: 4 maio 2022.

FINLAYSON, Andrew R. A Retrospective on Counterinsurgency Operations — Central Intelligence Agency. 11 fev. 2009. Disponível em: https://web.archive.org/web/20090211215158/https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol51no2/a-retrospective-on-counterinsurgency-operations.html. Acesso em: 9 maio 2022.

FINNEGAN, John Patrick; DANYSH, Romana. **Military Intelligence**. [*S. l.*]: Center of Military History of the US Army, 2015.

FOREIGN POLICY RESEARCH INSTITUTE. **New Thinking on the Origins of World War I**. [*S. l.*: *s. n.*], 5 maio 2014. Disponível em: https://www.youtube.com/watch?v=hMKqPgWJYr8. Acesso em: 21 abr. 2022.

FORTUN, M.; SCHWEBER, S. S. Scientists and the Legacy of World War II: The Case of Operations Research (OR). **Social Studies of Science**, v. 23, n. 4, p. 595–642, nov. 1993. https://doi.org/10.1177/030631293023004001.

FREEMAN, Chris; SOETE, Luc. **A Economia da Inovação Industrial**. 1ª edição. Campinas: Editora da Unicamp, 2009.

GALISON, Peter. The Ontology of the Enemy: Norbert Wiener and the Cybernetic Vision. **Critical Inquiry**, v. 21, n. 1, p. 228–266, 1994.

GALISON, Peter; HEVLY, Bruce (Orgs.). **Big Science: The Growth of Large-Scale Research**. 1st edition. Stanford, Calif: Stanford University Press, 1992.

GALISON, Sina Najafi and Peter. **The Ontology of the Enemy: An Interview with Peter Galison | Sina Najafi and Peter Galison**. [*S. l.*: *s. n.*], 2020. Disponível em: https://cabinetmagazine.org/issues/12/najafi_galison.php. Acesso em: 21 mar. 2022.

GARTZKE, Eric; LINDSAY, Jon R. **Cross-Domain Deterrence: Strategy in an Era of Complexity**. New York: Oxford University Press, 2019. DOI 10.1093/oso/9780190908645.001.0001. Disponível em: https://oxford.universitypressscholarship.com/10.1093/oso/9780190908645.001.0001/oso-9780190908645. Acesso em: 9 maio 2022.

GONZÁLEZ, Roberto J. Anthropology and the covert: Methodological notes on researching military and intelligence programmes. **Anthropology Today**, v. 28, n. 2, abr. 2012.

GLASS, Robert Rigby; DAVIDSON, Philip Buford. **Intelligence is for Commanders**. [*S. l.*]: Military Service Publishing Company, 1948.

GROSS, Daniel; SAMPHAT, Bhaven. **Wartime Innovation: Lessons From the Office of Scientific R&D | American Association for the Advancement of Science**. [*S. l.*: *s. n.*], 12 mar. 2020. Disponível em: https://www.aaas.org/news/wartime-innovation-lessons-office-scientific-rd. Acesso em: 24 mar. 2022.

HADLEY, Greg. **Congress Unveils 2022 Spending Plan, Boosting Pentagon Funding**. 9 mar. 2022. **Air Force Magazine**. Disponível em: https://www.airforcemag.com/congress-unveils-2022-spending-plan-boosting-pentagon-funding/. Acesso em: 4 maio 2022.

HAGEDORN, Ann. **Savage Peace: Hope and Fear in America, 1919**. [*S. l.*]: Simon and Schuster, 2007.

HARAWAY, Donna. Situated Knowledges: The Science Question in Feminism and the Privilege of Partial Perspective. **Feminist Studies**, v. 14, n. 3, p. 575–599, 1988. https://doi.org/10.2307/3178066.

HARAWAY, Donna. Modest _ Witness @ Second _ Millennium. FemaleMan©_Meets_OncoMouseTM. Second Edition. New York: Routledge, 2018.

HARAWAY, Donna J. Saberes localizados: a questão da ciência para o feminismo e o privilégio da perspectiva parcial. **Cadernos Pagu**, n. 5, 1995, p. 07-42.

HARPER, Richard. **Inside the IMF**. [*S. l.*]: Routledge, 2009.

HAYKIN, Simon. **Neural Networks: A Comprehensive Foundation**. [*S. l.*]: Prentice Hall, 1999.

HEWES JR., James E. **From Root to McNamara: Army Organization and Administration 1900-1963**. [*S. l.*]: US Army Center of Military History, 1975. Disponível em: https://www.history.army.mil/books/root/index.htm#contents. Acesso em: 23 abr. 2022.

HOBSBAWM, Eric. **Era dos extremos: O breve século XX**. [*S. l.*]: Editora Companhia das Letras, 1995.

HOCHSCHILD, Adam. **How a young Army officer built America's empire of paranoia with torture, surveillance, and 85,000 index cards**. 2018. **Mother Jones**. Disponível em: https://www.motherjones.com/politics/2018/01/how-a-young-army-officer-built-americas-empire-of-paranoia-with-torture-surveillance-and-85000-index-cards/. Acesso em: 23 abr. 2022.

HOCHSCHILD; ADAM. **Lessons from a dark time: and other essays**. [*S. l.*]: University of California Press, 2018. Disponível em: http://gen.lib.rus.ec/book/index.php?md5=5A4E53121BD0F6D19732D185C6F9F970. Acesso em: 23 abr. 2022.

HOROWITZ, Brian; BRADLEY, Michelle Cadoree; LIBRARY OF CONGRESS. United States War Dept/Dept of the Army Field Manual Collection. 2017. Disponível em: https://www.loc.gov/rr/scitech/SciRefGuides/fieldmanuals4.html. Acesso em: 5 abr. 2022.

HULL, Matthew S. **Government of Paper: The Materiality of Bureaucracy in Urban Pakistan**. 0 ed. [*S. l.*]: University of California Press, 2012. Disponível em: http://gen.lib.rus.ec/book/index.php?md5=17dfe9f48b60b1045c8c53032383e2b1. Acesso em: 11 maio 2022.

HYPERWAR. U.S. Army Field Manuals from II World War. 28 mar. 2022. Disponível em: https://www.ibiblio.org/hyperwar/USA/ref/FM/index.html. Acesso em: 27 mar. 2022.

IGOE, Michael. USAID mulls proposal to train aid workers as special forces. 19 fev. 2019. **Devex**. Disponível em: https://www.devex.com/news/sponsored/usaid-mulls-proposal-to-train-aid-workers-as-special-forces-94321. Acesso em: 10 maio 2022.

INFORMATION WARFARE AND ITS 18TH AND 19TH CENTURY ROOTS. [*s. d.*]. **The Cyber Defense Review**. Disponível em: https://cyberdefensereview.army.mil/CDR-Content/Articles/Article-View/Article/2017786/information-warfare-and-its-18th-and-19th-century-roots/. Acesso em: 3 maio 2022.

INFORMS. The Origins of OR. 23 mar. 2022. **INFORMS**. Disponível em: https://www.informs.org/Explore/History-of-O.R.-Excellence/Bibliographies/The-Origins-of-OR. Acesso em: 23 mar. 2022.

INTERAGENCY OPSEC SUPPORT STAFF. **Intelligence Threat Handbook**. [*S. l.*]: Interagency OPSEC Support Staff, 2000. Disponível em: https://irp.fas.org/nsa/ioss/threat96/part02.htm. Acesso em: 23 mar. 2022.

JOHNSON, Douglas H. Evans-Pritchard, the Nuer, and the Sudan Political Service. **African Affairs**, v. 81, n. 323, p. 231–246, 1982.

JOHNSON, Wray R. Black American Radicalism and the First World War: The Secret Files of the Military Intelligence Division. **Armed Forces & Society**, v. 26, n. 1, p. 27–53, 1999.

JOINT CHIEFS OF STAFF OF THE DEPARTMENT OF DEFENSE. **Department of Defense Dictionary of Military and Associated Terms**. [*S. l.*]: Joint Chiefs of Staff, 2022.

JOINT DOCTRINE LIBRARY. [*s. d.*]. **Joint Doctrine Library**. Disponível em: https://www.jcs.mil/Doctrine/. Acesso em: 27 abr. 2022.

JONES, Douglas W. Douglas W. Jones's punched card index. 2012. Disponível em: http://homepage.cs.uiowa.edu/~jones/cards/history.html. Acesso em: 23 abr. 2022.

KAHN, David. The Rise of Intelligence. **Foreign Affairs**, v. 85, n. 5, p. 125–134, 2006. https://doi.org/10.2307/20032075.

KARNOW, Stanley. **In Our Image: America's Empire in the Philippines**. Reissue edition. New York: Ballantine Books, 1990.

KATZ, Jonathan M. **Gangsters of Capitalism: Smedley Butler, the Marines, and the Making and Breaking of America's Empire**. New York: St. Martin's Press, 2022.

KENNEDY, David M. **Over Here: The First World War and American Society**. [*S. l.*]: Oxford University Press, 2004.

KRAMER, PAUL A. Race-Making and Colonial Violence in the U.S. Empire: The Philippine-American War as Race War. **Diplomatic History**, v. 30, n. 2, p. 169–210, 2006.

LARSON, Eric V.; DARILEK, Richard E.; GIBRAN, Daniel; NICHIPORUK, Brian; RICHARDSON, Amy; SCHWARTZ, Lowell H.; THURSTON, Cathryn Quantic. **Foundations of Effective Influence Operations: A Framework for Enhancing Army Capabilities**. [*S. l.*]: RAND Corporation, 27 maio 2009. Disponível em: https://www.rand.org/pubs/monographs/MG654.html. Acesso em: 9 maio 2022.

LAW, John. Actor-network theory and material semiotics. *In*: TURNER, Bryan S. (org.). Oxford: Blackwell, 2008. p. 141–158. Disponível em: http://bookshop.blackwell.co.uk/jsp/id/The_New_Blackwell_Companion_to_Social_Theory/9781405169004. Acesso em: 27 abr. 2022.

LIN, Herbert. Doctrinal Confusion and Cultural Dysfunction in DoD: Regarding Information Operations, Cyber Operations, and Related Concepts. **The Cyber Defense Review**, v. 5, n. 2, p. 89–108, 2020.

LINFIELD, Michael. **Freedom Under Fire: U.S. Civil Liberties in Times of War**. [*S. l.*]: South End Press, 1990.

LINN, Brian McAllister. **The US Army and Counterinsurgency in the Philippine War, 1899-1902**. Chapel Hill: Univ of North Carolina Pr, 1989.

LIST OF U.S. DEPARTMENT OF DEFENSE AGENCIES. *In*: Wikipedia. [*S. l.*: *s. n.*], 5 abr. 2022. Disponível em: https://en.wikipedia.org/w/index.php?title=List_of_U.S._Department_of_Defense_agencies&oldid=1081089525. Acesso em: 27 abr. 2022.

LUPTON, Deborah. **Digital Sociology**. [*S. l.*]: Routledge, 2014. Disponível em: http://gen.lib.rus.ec/book/index.php?md5=847c18ddca31ebb8bfb600cce3405975. Acesso em: 21 abr. 2022.

MARCOS, Subcomandante; BOT, Yvon Le. **El sueño zapatista**. [*S. l.*]: Editorial Anagrama, 1997(Crónicas). Disponível em: http://gen.lib.rus.ec/book/index.php?md5=8d7362232128b7edf2894e97445c5348. Acesso em: 27 abr. 2022.

MARINI, Marisol. A atuação da imaginação no desenvolvimento de Corações Artificiais: por uma compreensão da corporificação e partilha da imaginação. **Mana**, v. 27, 10 set. 2021. DOI 10.1590/1678-49442021v27n2a207. Disponível em: http://www.scielo.br/j/mana/a/rbznpPMHF8rdjqFXW5VFMrp/abstract/?lang=pt. Acesso em: 11 maio 2022.

MARTINS, Rafael Moro. Documento mostra treino do Exército contra esquerda. 2021. **The Intercept Brasil**. Disponível em: https://theintercept.com/2021/12/07/exercito-treinamento-anti-esquerda-documento/. Acesso em: 11 maio 2022.

MCCLINTOCK, Anne. **Imperial Leather: Race, Gender, and Sexuality in the Colonial Contest**. 1ª edição. New York: Routledge, 1995.

MCCOY, Alfred William. Policing the Imperial Periphery: The Philippine-American War and the Origins of U.S. Global Surveillance. **Surveillance & Society**, v. 13, n. 1, p. 4–26, 29 jul. 2014. https://doi.org/10.24908/ss.v13i1.5161.

MILITARY COMMAND ASSISTANCE VIETNAM. **MAVC Directive 381-41**. [*S. l.*: *s. n.*], 1988. Disponível em: http://www.lexisnexis.com/documents/academic/upa_cis/3208_recsmacvpt1.pdf. Acesso em: 23 abr. 2022.

MONTEIRO, Marko Synésio Alves. Reconsiderando a etnografia da ciência e da tecnologia: tecnociência na prática. **RBCS**, v. 27, n. 79, jun. 2012.

MONTEIRO, Marko Synésio Alves. Science is a war zone: some comments on Brazil. **Tapuya: Latin American Science, Technology and Society**, v.3, n.1, p. 4-8, 2020. DOI: 10.1080/25729861.2019.1708606.

MORGAN, Patrick M. **Deterrence: A Conceptual Analysis**. [*S. l.*]: SAGE Publications, 1977.

MUNDY, Liza. **Code girls: the untold story of the American women code breakers of World War II**. [*S. l.*]: Hachette Books, 2017. Disponível em: http://gen.lib.rus.ec/book/index.php?md5=D275B64C80EA465305F2861B0419B5FB. Acesso em: 23 abr. 2022.

NATIONAL SECURITY AGENCY DIGITAL NETWORK EXPLOITATION ANALYST SALARIES. [*s. d.*]. **Glassdoor**. Disponível em: https://www.glassdoor.com/Salary/National-Security-Agency-Digital-Network-Exploitation-Analyst-Salaries-E41534_D_KO25,61.htm. Acesso em: 4 maio 2022.

NIEHAUS, Isak. Anthropology at the dawn of apartheid: Radcliffe-Brown and Malinowski's South African engagements, 1919–1934. **Focaal**, v. 2017, 1 mar. 2017. https://doi.org/10.3167/fcl.2017.770109.

NIIYA, Brian. Office of Naval Intelligence | Densho Encyclopedia. 2020. **Densho Encyclopedia**. Disponível em: https://encyclopedia.densho.org/Office%20of%20Naval%20Intelligence/. Acesso em: 21 abr. 2022.

NUCLEAR WARHEAD INVENTORY PER COUNTRY 1945-2022. 2022. **Statista**. Disponível em: https://www.statista.com/statistics/1071026/nuclear-warheads-per-country-historical-development/. Acesso em: 9 maio 2022.

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE. Members of the IC. 2022. Disponível em: https://www.dni.gov/index.php/what-we-do/members-of-the-ic. Acesso em: 4 maio 2022.

OMANG, Joanne; NEIER (AUTHORS), Aryeh. **Psychological Operations In Guerrilla Warfare**. [*S. l.*: *s. n.*], [*s. d.*]. Disponível em: http://gen.lib.rus.ec/book/index.php?md5=d381ce0380332f2fec843621e0581a18. Acesso em: 27 abr. 2022.

OSINGA, Frans. **Science, Strategy and War: The Strategic Theory of John Boyd (Strategy and History Series)**. 1. ed. [*S. l.*: *s. n.*], 2006. Disponível em: http://gen.lib.rus.ec/book/index.php?md5=bbb8b7a1d956bbceb66bc09a54cbc93f. Acesso em: 10 maio 2022.

OUR STORY. [*s. d.*]. **U.S. Department of Defense**. Disponível em: https://www.defense.gov/About/. Acesso em: 27 abr. 2022.

OWENS, Larry. Vannevar Bush and the Differential Analyzer: The Text and Context of an Early Computer. **Technology and Culture**, v. 27, n. 1, p. 63–95, 1986. https://doi.org/10.2307/3104945.

PALATINO, Mong. **Global Voices - The Racist Portrayal of the Philippines in Historical Cartoons as US Troops Invaded**. 18 fev. 2016. **Global Voices**. Disponível em: https://globalvoices.org/2016/02/18/the-racist-portrayal-of-the-philippines-in-historical-cartoons-supporting-us-invasion/. Acesso em: 7 abr. 2022.

PAUL, Christopher. Is It Time to Abandon the Term Information Operations? 13 mar. 2019. Disponível em: https://www.rand.org/blog/2019/03/is-it-time-to-abandon-the-term-information-operations.html. Acesso em: 3 maio 2022.

PHINEAS FISHER. 2022. **The Anarchist Library**. Disponível em: https://theanarchistlibrary.org/category/author/phineas-fisher. Acesso em: 27 abr. 2022.

PIAS, Claus. **Cybernetics: The Macy Conferences 1946-1953: The Complete Transactions**. [*S. l.*]: University of Chicago Press, 2016. Disponível em: http://gen.lib.rus.ec/book/index.php?md5=43EE9AC90307461CF68746BAFA3E593E. Acesso em: 26 abr. 2022.

P/K, Geplaatst door. **The NSA's regional Cryptologic Centers**. 2019. Disponível em: https://www.electrospaces.net/2019/06/the-nsas-regional-cryptologic-centers.html. Acesso em: 4 maio 2022.

PORCHE, Isaac R.; PAUL, Christopher; YORK, Michael; SERENA, Chad C.; SOLLINGER, Jerry M.; AXELBAND, Elliot; MIN, Endy Y.; HELD, Bruce J. APPENDIX B: Information Operations in Doctrine. **Redefining Information Warfare Boundaries for an Army in a Wireless World**. [*S. l.*]: RAND Corporation, 2013. p. 103–112. Disponível em: https://www.jstor.org/stable/10.7249/j.ctt3fh1qp.19. Acesso em: 3 maio 2022.

POTTER, Sonia. On the Reactionary Treatment of American Radicals By J. Edgar Hoover's FBI. **Student Projects from the Archives**, v. 2, n. 1, 7 out. 2019. Disponível em: https://ideaexchange.uakron.edu/spa/vol2/iss1/7.

PRIEST, Dana; ARKIN, William M. **Top Secret America: The Rise of the New American Security State**. 1ª edição. New York: Little, Brown and Company, 2011.

PUTNAM, Major Bill. COIN Lessons Ignored: The Philippines Campaign (1899-1902). 2013. **Small Wars journal**. Disponível em: https://smallwarsjournal.com/jrnl/art/coin-lessons-ignored-the-philippines-campaign-1899-1902. Acesso em: 7 abr. 2022.

RAND. Information Operations. 2022. Disponível em: https://www.rand.org/topics/information-operations.html. Acesso em: 9 maio 2022.

ROSENZWEIG, Phil. Robert S. McNamara and the Evolution of Modern Management. **Harvard Business Review**. seç. Decision making and problem solving, 1 dez. 2010. Disponível em: https://hbr.org/2010/12/robert-s-mcnamara-and-the-evolution-of-modern-management. Acesso em: 24 abr. 2022.

ROHDEN, F.; MONTEIRO, M. Para além da ciência e do anthropos: deslocamentos da antropologia da ciência e da tecnologia no Brasil. **BIB - Revista Brasileira de Informação Bibliográfica em Ciências Sociais**, [S. l.], n. 89, p. 1–33, 2019.

RUDMAN, Warren B.; BROWN, Harold. **Preparing for the 21st Century: An Appraisal of U. S. Intelligence**. [*S. l.*]: DIANE Publishing, 1996.

RUSI. **Deterrence in the twenty-first century**. [*S. l.*: *s. n.*], 2009. Disponível em: https://media.defense.gov/2017/Apr/05/2001727306/-1/-1/0/B_0118_DETERRENCE_TWENTYFIRST_CENTURY.PDF.

RUTTAN, Vernon W. **Is War Necessary for Economic Growth?: Military Procurement and Technology Development**. 1st edition. Oxford; New York: Oxford University Press, 2006.

SANDERS, Chris. Chapter 1 - The Practice of Applied Network Security Monitoring. *In*: SANDERS, Chris; SMITH, Jason (orgs.). **Applied Network Security Monitoring**. Boston: Syngress, 2014. p. 1–24. DOI 10.1016/B978-0-12-417208-1.00001-5. Disponível em: https://www.sciencedirect.com/science/article/pii/B9780124172081000015. Acesso em: 3 maio 2022.

SCHELLING, Thomas C. **Arms and Influence**. [*S. l.*]: Yale University Press, 2020a. DOI 10.2307/j.ctvxkn7f8. Disponível em: http://www.jstor.org/stable/10.2307/j.ctvxkn7f8. Acesso em: 9 maio 2022.

SCHELLING, THOMAS C. **Arms and Influence**. [*S. l.*]: Yale University Press, 2020b. DOI 10.2307/j.ctvxkn7f8. Disponível em: https://www.jstor.org/stable/j.ctvxkn7f8. Acesso em: 9 maio 2022.

SECURITATEA, România; VERDERY, Katherine. **Secrets and truths: ethnography in the archive of romanian's secret police**. [*S. l.*]: Central European University Press, 2014(The Natalie Zemon Davis annual lectures). Disponível em: http://gen.lib.rus.ec/book/index.php?md5=00AFDB4C9F2CB43E9C022C11D0EE9FDB. Acesso em: 11 maio 2022.

SHANNON, C. E. A mathematical theory of communication. **The Bell System Technical Journal**, v. 27, n. 3, p. 379–423, jul. 1948. https://doi.org/10.1002/j.1538-7305.1948.tb01338.x.

SILVA, Tarcizio. Por outros imaginários sociotécnicos no novo normal. **Revista Observatório Itaú Cultural**, n.28, 2020, p.37-41.

SMITH, Ray Burdick. **Political and governmental history of the state of New York**. [*S. l.*]: Syracuse, N.Y. : Syracuse Press, 1922. Disponível em: http://archive.org/details/cu31924092201031. Acesso em: 20 abr. 2022.

SMOOT, Betsy Rohaly. **Parker Hitt: The Father of American Military Cryptology**. Lexington, Kentucky: University Press of Kentucky, 2022.

SNOWDEN, Edward. **Permanent Record**. [*S. l.*]: Metropolitan Books, 2019. Disponível em: http://gen.lib.rus.ec/book/index.php?md5=9b965019fd56cebb08f6723fee806aff. Acesso em: 4 maio 2022.

SOLOMON, Robert. Racism and Its Effect on Cannabis Research. **Cannabis and Cannabinoid Research**, v. 5, n. 1, p. 2–5, 27 fev. 2020. https://doi.org/10.1089/can.2019.0063.

SPECTOR, H. Ronald. **In the ruins of empire: the Japanese surrender and the battle for postwar Asia**. 1st ed. [*S. l.*]: Random House Publishing Group, 2007. Disponível em: http://gen.lib.rus.ec/book/index.php?md5=AFC3F5DDBAF27062047B53C387553307. Acesso em: 24 abr. 2022.

STOLER, Ann Laura. **Along the Archival Grain: Epistemic Anxieties and Colonial Common Sense**. Princeton, NJ: Princeton University Press, 2010.

THE TOP 10 FEDERAL DEFENSE CONTRACTORS. 2021. **Bloomberg Government**. Disponível em: https://about.bgov.com/top-defense-contractors/. Acesso em: 4 maio 2022.

THEOHARY, Catherine A. **Defense Primer: Information Operations**. Washington DC: Congressional Research Service, 14 jan. 2014. Disponível em: https://crsreports.congress.gov/product/pdf/IF/IF10771/6. Acesso em: 22 mar. 2022.

THOMAS, HUGH. Cuba: The United States and Batista, 1952-58. **World Affairs**, v. 149, n. 4, p. 169–175, 1987.

TOUREK, Mary. **“Civil Liberty Dead,” Laments The Nation Magazine**. 22 jul. 2013a. **Today in Civil Liberties History**. Disponível em: http://todayinclh.com/?event=civil-liberty-dead-proclaims-the-nation-magazine. Acesso em: 20 abr. 2022.

TOUREK, Mary. **“Slacker Raids” Round Up Alleged Draft Evaders in WW I**. 21 jun. 2013b. **Today in Civil Liberties History**. Disponível em: http://todayinclh.com/?event=slacker-raids-round-up-alleged-draft-evaders-in-ww-i. Acesso em: 20 abr. 2022.

TULL, Bruce K. Springfield Armory as industrial policy: Interchangeable parts and the precision corridor. **Doctoral Dissertations Available from Proquest**, , p. 1–227, 1 jan. 2001.

URBAN WARFARE PROJECT. Urban Warfare Project - What Does Army Doctrine Say About Urban Warfare? 20 mar. 2021. **Google Podcasts**. Disponível em: https://podcasts.google.com/feed/aHR0cHM6Ly91cmJhbi13YXJmYXJlLXByb2plY3QuY2FzdG9zLmNvbS9mZWVk/episode/aHR0cHM6Ly91cmJhbi13YXJmYXJlLXByb2plY3QuY2FzdG9zLmNvbS9wb2RjYXN0cy80MTkzL2VwaXNvZGVzL3doYXQtZG9lcy1hcm15LWRvY3RyaW5lLXNheS1hYm91dC11cmJhbi13YXJmYXJl. Acesso em: 27 abr. 2022.

US ARMY MILITARY INTELLIGENCE SALARIES IN WASHINGTON DC. [*s. d.*]. **Glassdoor**. Disponível em: https://www.glassdoor.com/Salary/US-Army-Military-Intelligence-Washington-DC-Salaries-EJI_IE41322.0,7_KO8,29_IL.30,43_IM911.htm. Acesso em: 4 maio 2022.

U.S. BUREAU OF LABOR STATISTICS; FEDERAL RESERVE BANK OF ST. LOUIS. All Employees: Government: Federal Government in Washington-Arlington-Alexandria, DC-VA-MD-WV (MSA). 2022. **FRED, Federal Reserve Bank of St. Louis**. Disponível em: https://fred.stlouisfed.org/series/SMU11479009091000001SA. Acesso em: 4 maio 2022.

US CONGRESS. United States Code: First War Powers Act, 1941, 50a U.S.C. §§ 601-622 (1946). 1941. **Library of Congress, Washington, D.C. 20540 USA**. [image]. Disponível em: https://www.loc.gov/item/uscode1946-004050a009/. Acesso em: 27 mar. 2022.

U.S. INTELLIGENCE BUDGET DATA. [*s. d.*]. Disponível em: https://irp.fas.org/budget/. Acesso em: 4 maio 2022.

VALENTINE, Douglas. **The Phoenix Program: America’s Use of Terror in Vietnam**. [*S. l.*]: Open Road Media, 2014.

VAN DEMAN, Ralph H. **Memoirs of Major General R.H. Van Deman.** Pittsfield, Mass.: 1209th Military Intelligence Training Co., 1950.

WARNER, Michael; MCDONALD, J. US Intelligence Community Reform Studies Since 1947. *[S. l]*, p. 53, 1 abr. 2005.

WATCH, Author SOA. **SOA Manuals**. 12 fev. 2020. **SOA Watch**. Disponível em: https://soaw.org/soa-manuals. Acesso em: 10 maio 2022.

WATTS, Stephen; CAMPBELL, Jason H.; JOHNSTON, Patrick B.; LALWANI, Sameer; BANA, Sarah H. Counterinsurgency in the Philippines. **Countering Others' Insurgencies**. Understanding U.S. Small-Footprint Interventions in Local Context. [*S. l.*]: RAND Corporation, 2014. p. 63–110. Disponível em: https://www.jstor.org/stable/10.7249/j.ctt5vjvmn.12. Acesso em: 7 abr. 2022.

WEISS, Robert P. From Cowboy Detectives to Soldiers of Fortune: Private Security Contracting and Its Contradictions on the New Frontiers of Capitalist Expansion. **Social Justice**, v. 34, n. 3/4 (109-110), p. 1–19, 2007. .

WHEATON, Kristan J. **RFI: Who Invented The Intelligence Cycle?** 4 jan. 2011. **Sources And Methods**. Disponível em: https://sourcesandmethods.blogspot.com/2011/01/rfi-who-invented-intelligence-cycle.html. Acesso em: 26 abr. 2022.

WILSON, John B. **Maneuver and Firepower: The Evolution of Divisions and Separate Brigades**. [*S. l.*]: U.S. Government Printing Office, 1999.