FESPSP
Fundação Escola de Sociologia e Política de São Paulo

Glaysson Tomaz

Função, Disfunção, Distopia:
Hacktivismo, Ciberguerra e Terrorismo no Século XXI

São Paulo
2018

Glaysson Tomaz

Função, Disfunção, Distopia:
Hacktivismo, ciberguerra e terrorismo no século XXI

Projeto de conclusão de curso apresentado à Fundação Escola de Sociologia e Política de São Paulo para obtenção do título de bacharel em Sociologia, sob a orientação do (a) professor (a) Dr. Rafael de Paula Aguiar Araújo.

São Paulo
2018

Biblioteca FESPSP – Catalogação-na-Publicação (CIP)

363.325
T655f Tomaz, Glaysson dos Santos.
Função, disfunção, distopia : hacktivismo, ciberguerra e terrorismo no século XXI / Glaysson dos Santos Tomaz. – 2018.
30 p. ; 30 cm.

Orientador: Prof. Dr. Rafael de Paula Aguiar Araújo.
Trabalho de conclusão de curso (Bacharel em Sociologia e Política) – Fundação Escola de Sociologia e Política de São Paulo.
Bibliografia: p. 30.

1. Tecnologia. 2. Ciberguerra. 3. Hacking. 4. Distopia. 5. Terrorismo. I. Araújo, Rafael de Paula Aguiar. II. Título.

CDD 23. : Cyberterrorismo 363.325

Ficha catalográfica elaborada por Éderson Ferreira Crispim CRB-8 9724

Glaysson Tomaz

Função, Disfunção, Distopia: Hacktivismo, ciberguerra e terrorismo no século XXI

Projeto de conclusão de curso apresentado à Fundação Escola de Sociologia e Política de São Paulo para obtenção do título de bacharel em Sociologia, sob a orientação do (a) professor (a) Dr. Rafael de Paula Aguiar Araújo.

Data de aprovação:

_____/_____/_____.

Banca examinadora:

_____

Nome do (a) professor (a), titulação,

Instituição e assinatura.

_____

Nome do (a) professor (a), titulação,

Instituição e assinatura.

AGRADECIMENTOS

Gostaria de deixar meus sinceros agradecimentos aos meus colegas e professores da FESPSP por esses anos de acolhimento e intenso aprendizado. E em especial, agradeço ao professor Dr. Rafael Araújo pelo apoio e o incentivo que me deu desde os primeiros semestres em prol dessa distopia, que não sei onde vai dar. Dúvida que longe de ser particular, se estende ao contrário à toda humanidade.

Hack The Planet!

“Forças high-tech ‘tripuladas’ por drones sem piloto e vermes cibernéticos estão substituindo os exércitos de massas do século XX, e os generais delegam cada vez mais suas decisões críticas a algoritmos” (HARARI, 2015)

RESUMO

Este trabalho apresenta uma análise sobre as mutações tecnológicas, conceituadas como função, disfunção e distopia. Entendendo-se por Função, o propósito inicial da tecnologia, dito de outra maneira é o que responde à pergunta: para o que essa tecnologia foi pensada e desenvolvida? Por disfunção, aquilo que leva a tecnologia a operar de maneira inesperada; e por distopia, o que a disfunção da função inicial de determinada tecnologia possibilita fazer. Tendo como referência a notável expansão tecnológica que vem ocorrendo no século XXI e os inúmeros casos de grande repercussão onde a tecnologia foi utilizada para fins de espionagem, sabotagem e controle, por governos, agências e ativistas, pretende-se analisar os diversos elementos que compõem esse cenário, assim como suas implicações político-sociais.

Palavras-chave: Tecnologia, ciberguerra, hacking, distopia.

ABSTRACT

This work presents an analysis about the mutations of technology, conceptualized as function, dysfunction and dystopia. Understanding Function, the initial purpose of technology, put another way is what answers the question: what has this technology been designed and developed for? By dysfunction, what causes the technology to operate unexpectedly; and dystopia, which the dysfunction of the initial function of a given technology makes it possible to do. Taking as reference the remarkable technological expansion that has been taking place in the 21st century and the innumerable cases of great repercussion where the technology has been used for espionage, sabotage and control by governments, agencies and activists, we intend to analyze the various elements that make up this scenario, as well as its socio-political implications.

Keywords: Technology, cyberwar, hacking, dystopia

SUMÁRIO

1 INTRODUÇÃO **9**

2 PROBLEMATIZAÇÃO **10**

3 OBJETIVOS **27**

4 PROCEDIMENTOS DE PESQUISA **28**

5 CRONOGRAMA **29**

BIBLIOGRAFIA **30**

1. INTRODUÇÃO

Assistimos diariamente como a tecnologia vai se expandindo e se tornando cada vez mais parte da vida do ser humano. Nesse contexto, não estamos, portanto, falando apenas da tecnologia enquanto motor do Capitalismo — como na revolução industrial; trata-se ao invés disso da tecnologia implantada em cada lar, presente no cotidiano; a tecnologia enquanto meio de consumo remoto, lazer e trabalho; a tecnologia enquanto extensão das faculdades humanas. Dessa maneira, este trabalho pretende estudar como a tecnologia pode e está sendo aplicada no século XXI para se alcançar fins políticos muitas vezes com ambições ou claros propósitos totalitários. A tecnologia aplicada à guerra, ao ativismo, ao terrorismo moderno. Além disso — do uso direto e explícito da tecnologia nos contextos citados— o presente trabalho tem como foco a tecnologia em seu funcionamento anormal, quando subvertida por meio de uma disfunção (um bug no código fonte, lógica incorreta etc), situação na qual, um relógio, um smartphone, uma geladeira, um televisão ou qualquer outro dispositivo conectado à internet podem ser utilizados contra a liberdade de um usuário, ou mesmo e uma nação.

2. PROBLEMATIZAÇÃO

Uma vez disseminada nos lares, indústrias e instituições, a tecnologia supre demandas ao passo que também cria dependências e riscos, que muito além dos prejuízos financeiros, afetam diretamente a liberdade de expressão, a neutralidade e mesmo a liberdade propriamente dita do indivíduo. E isso vem sido feito há muito tempo na história da internet, pra ser exato desde seu nascimento, embora só tenha ganhado destaque — a ponto de se tornar assunto do dia a dia — com o advento dos indivíduos e grupos que denunciaram o uso de disfunções em tecnologias largamente utilizadas por cidadãos (dispositivos, aplicativos, gadgets) ou específicas (usinas, power grids, etc) para fins de espionagem e sabotagem. Dessa maneira o presente trabalho pretende contribuir com a literatura a respeito da discussão sobre tecnologia, mais especificamente no contexto do hacking, tema estrutural desta trabalho.

Do controle à Distopia

Usarei a expressão “distópicas” para me referir às sociedades que situam-se num momento histórico caracterizado pela exponencial oferta tecnológica e pelo fácil acesso por parte dos consumidores à essas tecnologias ou ao produto delas. Desta maneira, tem-se não somente a tecnologia aplicada nos meios de produção, como estrutura e motor de expansão do Capitalismo — embora também o seja— , mas a tecnologia plantada em toda parte enquanto objeto de socialização, educação, trabalho e consumo remoto. Diante disso estamos falando de sociedades tecnologicamente distópicas, ou seja, sociedades que podem ser vigiadas e controladas em sua conformação coletiva ou individual, por meio de sua superfície tecnológica que a compõe.

Vale ressaltar que o conceito de distopia como aqui pretendo analisar se distancia um pouco de seu sinônimo de antiutopia. Isso porque a antiutopia representa a antítese da utopia, uma utopia negativa, onde aparentemente as coisas não aconteceram como esperado. Nesse caso, os aspectos negativos da tecnologia, tendem a ser relativizados ou se transformam em meros medos etéreos que circulam pelo imaginário social. Mas as disfunções, as imperfeições, os bugs e até mesmo recursos legítimos (com potencialidades distópicas) raramente passam despercebidos pelos grupos que atuam para agências de espionagem — sobretudo nas grandes potências hegemônicas —, regimes ditatoriais e muito menos pelas empresas que suportam esses regimes servindo-os com as melhores tecnologias (para as piores práticas).

Além disso existem aqueles agentes, isolados ou em grupos organizados, que devido àquelas práticas (o uso da tecnologia para fins de controle e manipulação), revidam contra os fornecedores, uma vez que esses aparatos servirão de mecanismo de repressão nas mãos de agentes a serviço de uma um regime totalitário a fim de espionar, controlar e incriminar ativistas, jornalistas, dissidentes e o que mais for considerado uma ameaça contra esse regime.

O terrorismo no século XXI se tornou um excelente álibi para qualquer prática, inclusive terrorismo, e não por acaso se tornou o mantra das agências de inteligência. Mas as agências não existiriam sem os indivíduos especializados em encontrar, explorar vulnerabilidades e criar novas ferramentas a partir delas. E aí mora um dos principais dilemas: hackers extremamente hábeis que se num momento representam a força tarefa, o cerne de uma agência, em outro podem também utilizar esse poder contra os interesses das agências.

Os grupos organizados e agentes sempre estiveram presentes no território da internet desde os primórdios e estão de certa maneira emaranhados na própria história dela. No entanto, ganharam grande repercussão no século XXI agindo contra empresas que desenvolvem as tecnologias; como é o caso da empresa italiana Hacking Team e do hacker Phineas Fisher, do grupo The Shadow Brokers contra a NSA, assim como de Julian Assange com o Wikileaks e os vazamentos de documentos da NSA por Edward Snowden. São inúmeros os casos de grande repercussão, assim como aqueles pouco conhecidos do grande público.

Mutação e Processo

Adotarei aqui os termos *mutação* e *processo* de uma perspectiva e num contexto que embora não seja exatamente novo, vale a pena ter suas particularidades ressaltadas. O termo *mutação* tem por objetivo abarcar as formas que a tecnologia pode assumir quando subvertida – usada de maneiras não planejadas segundo seu design, sendo o design a fase do processo de de produção onde a razão de ser da tecnologia é concebida e documentada. E *processo* trata dos estágios pelos quais a tecnologia passa a fim de se aprimorar ou se adequar ao ciberespaço. E como “tecnologia” pode soar um pouco vago, aqui o termo será empregado como sendo o produto, o meio como ele é disponibilizado e como os usuários o adquirem e usufruem dele. Dessa forma tecnologia é o aplicativo da rede social presente no dispositivo móvel, notebook, smart tvs e também o meio, a internet. E para que não fique a impressão de

estarmos contrapondo a internet às tecnologias concretas e que, portanto, estamos falando de coisas abstratas simplesmente por serem transmitidas, processadas e armazenadas no meio eletrônico-digital, é importante ter em mente que usinas nucleares, *powergrids*, plantas hídricas e infraestrutura crítica de muitos países são controladas por algoritmos, assim como satélites, marca-passos, computadores pessoais, smartphones e ao que tudo indica – com a Internet das coisas (IoT) –, em breve tudo à nossa volta. E questões ainda mais complexas se pensarmos na biotecnologia. O que um bug numa tecnologia inserida em nosso corpo poderia causar, por exemplo? e num sistema crítico baseado em inteligência artificial? São perguntas urgentes que visam dar luz não somente ao que o uso esperado dessas tecnologias (função) pode acarretar por si mesmos, mas também qual o impacto de uma eventual disfunção.

A proposta é adotar a perspectiva sociológica, sem, no entanto, abrir mão dos aspectos técnicos e culturais dos agentes. Portanto, a análise pretende-se sociológica, utilizando-se, no entanto, de signos, objetos, conceitos e do vocabulário das mais diversas áreas que compõem o que é denominado *hacking*, sendo o hacker a figura central das sociedades distópicas, uma vez que está envolvido tanto nos procedimentos de pesquisa de novas vulnerabilidades (disfunções), como também nas ações que serão realizadas por meio delas (eventos distópicos). Aqui ele será referenciado como *agente ativo* das mutações que serão apresentadas. Sendo que nem todo agente é um *hacker*, mas todo *hacker* é necessariamente um agente. Como será apresentado mais adiante, sua importância se dá tanto na resignificação da tecnologia quanto no combate ao uso promíscuo dela.

A gênese dos Agentes

O Cenário de Risco é um conceito muito empregado na segurança da informação, sendo um dos mais populares na área de desenvolvimento seguro de software. Trata-se de um esquema para se simular o risco, impacto e a criticidade de uma ameaça ou de uma vulnerabilidade em relação ao um ativo (computador, recurso, dados pessoais, etc). O primeiro componente desse cenário é *agente de ameaça* que através de um vetor de ataque explora uma fragilidade de segurança (disfunção), podendo causar (a depender da eficácia e da existência dos controles) diversos tipos de impacto (estados distópicos). Daqui vem a ideia de *agente* como aplicada no presente trabalho. Faço essa distinção, tendo vista que Pierre Bourdieu utiliza o termo *agente* para se referir aos indivíduos que articulam suas posições

sociais dentro do espaço social, para ele *um espaço virtual teórico.* Embora seja possível tratar as duas concepções como intercambiáveis, é importante, dado o contexto, enfatizar de onde a tirei.

Dessa maneira, o agente de ameaça traz consigo toda sua bagagem simbólica, seu léxico, seu mindset, suas ferramentas e habilidades técnicas e sociais. Poderíamos considerar, por exemplo, que mesmo no âmbito virtual, os hackers que descobrem e exploram vulnerabilidades e sistemas, *agentes de ameaça ativos*, portanto, são em última análise pessoas reais agindo através de um espaço virtual (literalmente virtual), portanto indivíduos, e assim, também agentes como os entende Bourdieu. No entanto, processos trabalhosos tendem a ser delegados à máquina que irá interpretar e executar os algoritmos pensados e implementados pelos agentes. Neste caso estaríamos falando de algoritmos que embora criados e/ou operados por indivíduos reais (em termos materiais) podem assumir grande parte do trabalho e até mesmo tomar decisões com relativa complexidade, e ao que tudo indica, tendem a se tornar cada vez mais autônomas, aplicando conceitos de Machine Learning, Inteligência artificial, Redes Neurais e outras ainda por surgir das intersecções ou limitações destas. Nesse caso já estaríamos falando de máquinas com considerável autonomia e capacidade não só para tomar decisões complexas como também para criar novos agentes de ameaça de maneira completamente autônoma e que tendem a um aperfeiçoamento contínuo. Assim, estaríamos entrando num terreno nebuloso onde o aspecto físico do agente se esgarça. Logo a correspondência com o conceito de agente, como encontrado em Bourdieu, deixaria de existir, se esse fosse o objetivo deste trabalho. Contudo, aqui também o agente (seja ele uma pessoa ou um sistema autônomo à serviço do primeiro) estará sempre articulando suas posições sociais dentro do espaço social e virtual, o que muda é o meio pelo qual isso se dá.

O propósito deste trabalho é — com base no que foi exposto — analisar os estados da tecnologia, que apresento como *função, disfunção e distopia*. Analisar *estados*, implica que o objeto da análise sejam as formas possíveis [mutações] e não os estágios necessários [processos]. O primeiro se refere às possíveis formas que a tecnologia (ou a experiência que o usuário tem com ou a partir dela) podem assumir no ciberespaço, e não que seja intrínseco à tecnologia passar por esses três estágios. Como será apresentado mais adiante, os estágios da tecnologia também culminam em distopia, ou seja, a tecnologia agindo segundo sua função original. Na verdade eles são eventos indissociáveis dos estados, além do que, resulta neles, daí o foco da análise ser nas mutações.

Por *função* devemos entender o motivo de ser da tecnologia segundo seu design. Ou segundo a ideia que se faz dela ou a experiência que se tem com ela, por exemplo, a função de uma smart tv é permitir que eu acesse não só o conteúdo televisionado, mas também aquele transmitido por meio da internet; e para tal, instala-se aplicativos, acessa-se a internet etc. Por Disfunção devemos entender alguma condição da função inicial da tecnologia que a faça funcionar de maneira anormal ou a impeça de funcionar: uma vulnerabilidade em um software ou no hardware de uma smart tv a impede de funcionar normalmente e/ou permite outras ações não esperadas, que afetam a privacidade do usuário ou a integridade dos seus dados. E por fim, a Distopia, que significa tudo aquilo que é possível realizar por meio de uma disfunção. Por exemplo: No vazamento Valt7 a primeira parte do vazamento de documentos da CIA pelo Wikileaks (2015), foi revelada a existência de uma ferramenta que conseguia atacar alguns modelos de smart tvs da Samsung e transformá-las em aparatos de vigilância, que fazia o aparelho entrar num modo denominado *fake-off*, ao mesmo tempo que utilizava os recursos de áudio e vídeo para vigiar o usuário. A isso, denomino Distopia no presente trabalho. E aqui, embora a ferramenta tenha sido batizada pelo(s) agente(s) de “weeping angel”, personagem da série Doctor Who, outro paralelo da ficção científica que podemos relacionar é a obra 1984 de George Orwell. No livro, os cidadãos assistem e são assistidos pela teletela, um aparelho utilizado pelo grande irmão para vigiar as pessoas. E o mesmo se dá no caso da ferramenta da CIA. A diferença aqui é na ficção os aparelhos são produzidos para esse fim, enquanto na realidade do século XXI, qualquer que seja a finalidade de determinada tecnologia, ela ainda poderá ser subvertida para se fazer algo mais. Esta é a síntese do que considero como estados/mutações da tecnologia. Síntese porque embora consiga esboçar a ideia, a mesma não pode ser esgotada sem considerar todos os componentes que compõem esses cenários.

Características da Função Distópica

É Importante ressaltar a importância dos conceitos de utopia e distopia para a literatura de ficção científica e a influência desse gênero nas invenções tecnológicas. Dentre as inúmeras obras relevantes, podem ser citadas 1984 de George Orwell, Admirável Mundo Novo de Aldous Huxley e Nós de Zamiátin, sendo muitas vezes utilizadas como sinônimos de distopia, representando verdadeiros arquétipos da ficção distópica. E mais do que o conceito de distopia em seu espectro amplo de “utopia negativa”, vale ter em mente o conceito de

distopia como empregado nessas duas obras, onde a distopia só é negação se contrastada com a expectativa utópica dos indivíduos, das massas, uma vez que parece atender perfeitamente aos anseios totalitários. Em outras palavras: Nada deu errado se deu tão certo para os que esperavam que desse errado. Aplicando a tríade *função, disfunção, distopia*: Se a disfunção possibilita o que sua função não permite ou não deveria permitir por design, a tecnologia é ressignificada, e, portanto, estamos falando de algo diferente, que embora tenha dado errado (segundo sua função) deu certo segundo a *Função* da sua *Disfunção,* e a isso denomino *Distopia* no presente contexto. Além disso, a característica que torna a *Distopia* um instrumento, ou melhor, um aparato tão eficiente para suportar ações arbitrárias é seu falso aspecto de irrealidade. Por se dar no âmbito eletrônico, cria-se uma abstração onde tanto o ato perpetrado pelo agente quanto a consequência desse ato são impregnados de irrealidade e pairam como ideias absurdas normalmente associadas à ficção científica, sobretudo no cinema – de onde também vêm os estereótipos dos hackers. E nesse caso, a tecnologia cumpre uma função que foge ao protocolo, uma Função Distópica. Os paralelos possíveis (e esperados) entre o conceito de distopia como empregado na literatura de ficção científica e o que aqui emprego é exatamente aquele explorado por George Orwell em 1984: A tecnologia utilizada como ferramenta de controle, seja do Estado, instituições e corporações a fim de instituir e manter o totalitarismo, afinal “a tendência natural de todos no poder é querer mais poder e controle, e é preciso de vigilância para isso”[1].

Na literatura de ficção científica – como ocorre em 1984 – a sociedade é vigiada por meio de tecnologias especialmente criadas com essa finalidade, de onde deriva o termo Big Brother, hoje sinônimo de controle, vigilância e manipulação. Na obra em questão, as teletelas são um tipo de tecnologia de telecomunicação bidirecional que ao mesmo tempo transmitem a programação oficial do governo e filmam o que acontece na frente do televisor. E a diferença aqui nesse contexto de distopia com o que proponho analisar é o fato de não se tratar de uma disfunção que possibilita uma função distópica, mas de um aparato pensado para essa finalidade. É evidente que na sociedade contemporânea existem empresas (agentes) que se ocupam do desenvolvimento de aparatos tecnológicos pensados exclusivamente para o controle, vigilância e manipulação da sociedade, não só existem como são bem conhecidas e representam um objeto de estudo importante. A questão é que no âmbito digital, para servirem

1 O hacker Phineas Fisher em entrevista à motherboard sobre o hacking da empresa italiana de espionagem Hacking Team.

a tal propósito – controle, vigilância, manipulação –, os aparatos tecnológicos contemporâneos não precisam sê-lo por design. Winston Smith estava consciente que estava sendo vigiado pelo grande irmão diretamente pela teletela enquanto assistia à programação. Portanto, não foi necessário uma disfunção nas funções da teletela para permitir o controle que se obtêm por meio dela.

Uma mutação tecnológica do tipo função-distopia é constituída de propriedades que inviabilizam e/ou subvertem. A propriedade que se limita à subversão é aquela onde uma disfunção no design original de um artefato tecnológico, não inviabiliza sua função, criando ao invés disso uma nova função não documentada nas especificações do artefato. Por outro lado, a propriedade que inviabiliza é acionada intencionalmente quando se tem por ação ou efeito sabotar, interromper ou causar indisponibilidade. Uma mutação tecnológica do tipo função-distopia também pode se apresentar acionando as duas propriedades ao mesmo tempo, criando uma nova função (que estende sua atuação) e adicionalmente possibilitando uma ação ou efeito (intencional) que leva à indisponibilidade da informação ou do sistema.

Fatores Implícitos e Explícitos

Os estágios da tecnologia dizem respeito ao processo pelo qual a tecnologia passa a fim de atender aos anseios dos usuários ou mesmo para se adicionar novos recursos (criar novos anseios). Dessa maneira, ao longo dos tempos as redes sociais foram agregando funcionalidades, como a integração com outros serviços, uso de webcam, comandos de voz, dupla autenticação, reconhecimento de rostos em fotos. O volume de dados que circula nas redes sociais ganha uma proporção cada vez mais assombrosa, o que por sua vez exige tecnologias específicas, como Big Data, para não só armazenar como também cruzar esses dados e tirar algum valor, seja direcionar propagandas, produtos e/ou aprimorar os próprios algoritmos para tornar a experiência do usuário final ainda mais “agradável” e, pode-se dizer, torná-lo cada vez mais confiante ao fornecer os seus dados. Não por acaso conceitos como Googlismo e Dataísmo foram forjados para se tratar do tema. E evidentemente que quanto mais o usuário interage, mais personalizada se torna sua experiência e mais abstrata se torna a forma como tudo isso se dá. Aqui reside um fator distópico explícito uma vez que pode ocorrer justamente por meio das funcionalidades que constituem a experiência do usuário com o sistema. Assim, operar um sistema via comando de voz oferece uma conveniência que pode

ocultar fatores obscuros como o fato de o aparelho permanecer em escuta durante todo o tempo, gravando e enviando os dados do usuário para servidores ao redor do mundo[2]. Conforme o usuário se entranha no meio digital e se torna parte do fluxo de dados, faz-se necessário transferir certa autoridade aos algoritmos. O escritor Israelense Yuval Noah em seu intrigante Homo Deus: Uma breve história do amanhã, capta esse ponto com muita clareza:

> A transferência da autoridade de humanos para algoritmos está acontecendo a nossa volta, não como resultado de uma decisão governamental, e sim devido a uma inundação de escolhas mundanas. Se não tivermos cuidado, o resultado disso poderia ser um estado de polícia orwelliano, que constantemente monitora e controla não somente todos os nossos atos, mas até mesmo o que acontece dentro de nossos corpos e cérebros (NOAH 2017).

Fenomenologia de uma Função Distópica

Por natureza essa nova função – derivada de uma disfunção – atua de forma promíscua, contra o usuário ou não. Por se dar no meio eletrônico digital, as ações executadas por meio dessa nova função tendem a uma discrição por obscuridade. E a falta de materialidade das consequências, ao menos de imediato, são ignoradas, ou melhor, desacreditadas. E a discrição das operações somada à percepção fictícia é uma característica fundamental de uma Função Distópica, como demonstram os casos analisados mais adiante.

A disfunção identificada viabiliza uma nova função ou funcionalidade não documentada no design original, que por sua vez viabiliza operações distópicas: situações onde o indivíduo — ou o coletivo — pode ser vigiado de forma imperceptível por meio da tecnologia. Essas tecnologias são carregadas com o usuário no dia a dia, estão presentes no ambiente de trabalho, nas casas, e se tornam cada dia mais indispensáveis às grandes cidades (inteligentes) e à indústria. Portanto, certas disfunções permitem a criação de *Funções Distópicas*. Trata-se de um tipo de distopia especialmente interessante, uma vez que mesmo depois de divulgado, revertido, exposto e analisado (ao nível binário num diálogo direto com a máquina), ainda persiste seu caráter fictício (de ficção científica). O aspecto imaterial dessa distopia, distancia o usuário, tanto em relação ao seu impacto social, quanto do entendimento de seu funcionamento do ponto de vista técnico.

2 https://www.wired.com/2017/02/smart-tv-spying-vizio-settlement/

No século XXI são abundantes os casos de aparatos que cumprem uma Função Distópica. E dada a natureza e o contexto em que esses aparatos atuam é evidente que não seriam tornados conhecidos do grande público (não técnico, sobretudo) não fosse pela ação de hackers e whistleblowers, pessoa que expõe informações ou atividades consideradas ilegais, antiéticas ou incorretas praticadas por organizações públicas ou privadas. Embora o termo whistleblower remonte a 1970, geralmente associado ao ativista civil Ralph Nader, o mesmo se popularizou a partir de 2007 com o advento do Wikileaks, sendo hoje diretamente associado à figura de Julian Assange, fundador e líder do serviço global de denúncias. Da mesma maneira, whistleblower se refere àqueles que tornaram esse serviço possível através das suas ações, como Edward Snowden, Chelsea Manning dentre outros considerados violadores da lei federal aprovada em 15 de Junho de 1917 conhecida como *Espionage Act*.

Dentre esses casos, ou como pretendo tratar aqui, “eventos”, tomarei como base de análise, alguns dos mais significativos no século XXI (até o momento). E sabendo que esses mesmos eventos, agora significativos, tendem a se tornar em breve obsoletos, pretendo analisar esses eventos pelo que representam em termos finalidade, e de impacto técnico, político e social. Posto isso, considero significativos o caso da *cyberweapon STUXNET*, o caso do comprometimento da empresa italiana de espionagem *Hacking Team (Phineas Fhisher)*, o caso do vazamento da *NSA (Edward Snowden)*, o vazamento do arsenal da *NSA* (grupo *The Shadow Brokers: TSB*) e os vazamentos da CIA (Wikileaks). Esse último é especialmente interessante por abarcar vários outros vazamentos isolados, assim como é importante por esboçar alguma inteligência em relação ao cenário no qual nasceu o STUXNET, o que implica uma responsabilização política embaraçosa envolvendo dois países que há tempos já não mantém relações diplomáticas ou minimamente cordiais.

No dia 07 de Março de 2017, o Wikileaks deu início a uma série de publicações sobre as atividades da Agência Central de Inteligência dos Estados Unidos da América, CIA. À data era publicado o que foi designado como “*Year Zero*”, a primeira parte do que foi apelidado como “*Valt7”*, a maior publicação de operações de inteligência da história. Na primeira parte da análise, Julian Assange chama a atenção para o fato de que a crescente sofisticação das técnicas de vigilância reforça os paralelos com a obra de George Orwell, 1984, o que não é exatamente algo novo. No entanto, enfatiza Assange, "Weeping Angel", desenvolvido pela *Embedded Devices Branch (EDB)* da CIA, é certamente a realização mais emblemática, uma vez que infesta Androids, IPhones, Smart TVs, transformando-as em microfones encobertos. E embora essa observação seja aparentemente ofuscada pelo teor da divulgação em si, na

realidade ela é fundamental, uma vez que aponta a obsolescência da ideia de distopia em relação aos aparatos utilizados no século XXI por potências que se confundem com o próprio conceito de democracia.

Weeping Angel é o nome de um personagem do episódio “Blink”, décimo episódio da terceira temporada da série Britânica Doctor Who. Numa pesquisa realizada à época o Weeping Angel venceu com 55% dos votos como o personagem mais assustador da série. Em 2012 em outra votação realizada pela Radio Times, o personagem venceu novamente com 49.4% dos votos e ainda em 2014 a revista Doctor Who elegeu “Blink” como um dos melhores episódios de todos os tempos, ficando o primeiro lugar para o episódio “The Day of The Doctor”. Aqui temos uma intersecção crucial para a consolidação do que chamo de fenomenologia de uma função distópica, uma vez que trata-se de um híbrido de aspectos técnicos – como a função se dá e opera no meio eletrônico-digital – e fenomenológicos – como as ações e consequências dessas ações (dinâmicas de eventos, ou seja, as interações entre agentes e funções) são percebidas (ou não) pelos agentes afetados.

Assange dá a exata proporção do que o *Valt7* representa ao dizer que a quantidade de páginas publicadas somente na primeira parte do "Vault 7" (Year Zero) já eclipsa o número total de páginas publicadas nos primeiros três anos dos vazamentos de Edward Snowden. Ao que consta na análise do Wikileaks, a primeira parte integral da série, "Year Zero", é composta por 8.761 documentos e arquivos de uma rede isolada de alta segurança, situada dentro da CIA. Esse vazamento expõe o escopo e a direção do programa global de hacking da CIA, seu arsenal de malwares e dezenas de ataques munidos de 0-days (falhas não divulgadas) contra uma ampla gama de produtos de empresas americanas e europeias, contabilizando várias centenas de milhões de linhas de código. No entanto, ao fazer essa alusão, Assange procura tão somente dar uma base comparativa que possa ressaltar a dimensão desse vazamento. O Valt 7 não anula a importância das operações, ferramentas e estratégias reveladas por Edward Snowden em relação à NSA.

Outro evento relevante trata-se do vazamento do The Shadow Brokers (TSB), grupo de hackers que em 2016 iniciou uma operação de vazamento das ferramentas (cyber weapons) criadas e operadas pelo Equation Group, o grupo de elite da NSA, descrito como um dos mais avançados grupos de hackers[3] de que se tem notícia (até a data). O primeiro vazamento

3 A divisão de inteligência da empresa Russa Karspersky Lab, que primeiro analisou operações realizadas pelo grupo da NSA por meio das suas plataformas de malware foi quem atribuiu o nome de Equation Group devido à forte afinidade do grupo de elite com algoritmos criptográficos, métodos de obfuscação e outras técnicas avançadas. Equations Group Questions and Answers: https://securelist.com/files/2015/02/Equation_group_questions_and_answers.pdf (Acessado em 23 de Abril de 2017)

realizado pelo grupo (TSB) foi realizado em Março de 2016 e o segundo em Abril de 2017. Embora normalmente o TSB seja tratado como um “grupo” de hackers, o mais adequado nesse contexto de agências e leaks, é tratar este e qualquer outro “grupo” como uma entidade, uma vez que pode tratar-se tanto de um grupo quanto de um indivíduo agindo isoladamente. De acordo com a análise realizada pela Karspersky Lab o Equation Group atua com suas plataformas de malware, EquationDrug plugins, GrayFish modules e EquationVector discretamente há cerca de 14 anos, operando por toda a internet com absoluta discrição.

Em Segurança da informação diz-se que a informação pode ser transmitida, armazenada e processada, constituindo estes os três estados da informação. Todos esses estados sofrem de ameaças e vulnerabilidades muito particulares. Dessa maneira se a informação que está sendo transmitida do cliente para o servidor, ou vice-versa, trafega por canais passíveis de monitoramento promíscuo de seu ponto de origem ao destino, é importante garantir que somente pessoas autorizadas possam acessá-la pelos meios autorizados, o que requer que os dados não estejam legíveis descriptografados para um potencial agente no meio do caminho. Se um sistema espera por design que a informação que ele está enviando como resposta a um pedido legítimo seja acessada somente pelo agente que originou o pedido, poderíamos entender isso como sendo sua *função*.

Se um agente não autorizado consegue de alguma maneira (utilizando seu arsenal) acessar essa informação, ocorre uma *disfunção da função (DF)*, e as consequências dessa subversão, ou seja, o que um agente de ameaça pode realizar a partir de DF, vão constituir uma Distopia, ou estado distópico, seja na forma de espionagem, controle, fraudes ou mesmo incriminação, afetando a liberdade ou mesmo a vida do alvo.

Ecossistema

Esse novo aparato cujo design cumpre uma Função Distópica, existe numa espécie de realidade alternativa dentro do ciberespaço, como uma singularidade computacional. E por se tratar de uma singularidade, esse aparato atua em um limbo fora do alcance das legislações, regras e princípios aos quais estariam submetidos os aparatos tecnológicos dedicados, por design, à mesma função.

São denominados agentes todos os envolvidos com desenvolvimento, subversão, aplicação/operação de aparato de Função Distópica. Sendo assim temos como agentes os

desenvolvedores, engenheiros, designers responsáveis pela produção de uma determinada tecnologia (hardware/software); hackers que irão identificar as falhas e subverter o design original atribuindo uma função específica à disfunção identificada, e também aqueles que irão aplicar ou operar essa Função Distópica (indivíduos, governantes, grupos terroristas).

Quanto ao conceito de disfunção, é importante ressaltar a ligação direta com o hacking, e com as agências de inteligência, uma vez que os hackers constituem o exército virtual das grandes hegemonias, como apontado por Rogério da Costa em seu artigo sobre sociedades de controle:

> Por outro lado, da mesma forma que o terrorismo é uma consequência do terror imposto pelo Estado, a ação não localizada dos *hackers*, produzindo disfunções e rupturas nas redes, parece ser o efeito que corresponde adequadamente aos novos modos de atuação do poder. (COSTA, Rogério da. Sociedade de controle. São Paulo Perspec., São Paulo , v. 18, n. 1, p. 161-167, Mar. 2004 . Available from <http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0102-88392004000100019&lng=en&nrm=iso>. access on 27 Nov. 2018. http://dx.doi.org/10.1590/S0102-88392004000100019.)

No contexto das ciências da computação, *artefato* é o produto das atividades realizadas por uma pessoa ou por uma equipe no contexto de desenvolvimento de software ou de um sistema. Na Arqueologia o Artefato é entendido como sendo um objeto ou mesmo os fragmentos desse objeto que podem fornecer indicações sobre o indivíduo que o concebeu, sobre a época e o ambiente no qual ele estava inserido. Nas ciências experimentais o artefato é o resultado de uma experiência que não poderia acontecer naturalmente e que foi causado por um método de experimentação errado. Em processamento de sinais artefato é qualquer elemento que não existe no sinal original (input), mas que aparece no sinal processado (output), como resultado de imperfeições no processamento. Sendo assim, emprego *artefato* como sendo o resultado (esperado ou não) de um processo realizado por agentes, sejam eles agentes de função (AF) ou disfunção (AD/oper).

Os agentes da função (A*f*) podem ser associados diretamente com a primeira definição de artefato, sendo dessa maneira os responsáveis pelo desenvolvimento do software/sistema que será instalado ou embarcado nos diferentes tipos de dispositivos, o que vai de smartphones pessoais a usinas nucleares. Dessa maneira trata-se de uma correlação direta. No

entanto, o correto é tratá-lo como um agente duplo, uma vez que ele está associado à definição de artefato da ciências da computação da mesma maneira como está às demais definições. Em relação às definições das ciências experimentais e processamento de sinais, a correlação com o agente é ainda mais direta, uma vez que o AF é responsável não só pela função, mas também pela disfunção já que a primeira é condição *sine qua non* para a segunda. Por outro lado, os agentes da disfunção (AD) estão diretamente relacionados aos quatro tipos de definições de artefatos.

Dessa maneira, para usar um termo ainda mais apropriado, eles podem ser definidos como agentes polimórficos, uma vez que assumem formas variadas dentro do cenário de uma Função Distópica. Eles personificam os agentes da função por meio da programação de computadores. Eles identificam a Disfunção plantada pelo A*f* enquanto A*D* e atribuem a ela uma nova função, que não poderia existir naturalmente, mas somente em decorrência de uma experimentação errada, como nas ciências experimentais. Da mesma maneira, a Função Distópica atende a propósitos que não seriam possíveis a priori, ou seja, a função possibilitada não existe no design inicial, mas somente em decorrência de imperfeições, assim como no processamento de sinais. E por último, no contexto da Arqueologia, podemos dizer que a forma como um algoritmo é concebido pode revelar informações sobre agentes da função que o escreveram, sobre suas motivações e o meio onde o conceberam. cabe ao A*D*, em seu polimorfismo, atuar nessa arqueologia da disfunção. E através disso, tal qual o arqueólogo em campo, ele vai desenterrando os artefatos, desvendando modos de pensar, falhas de lógica que denunciam bugs cognitivos. Assim, ambos os agentes estão também relacionados à definição de artefatos da arqueologia.

Os cenários representam a configuração resultante da ação dos agentes sobre os artefatos e a consequente confecção de aparatos, o que pode resultar ou não num evento que leva a uma Função Distópica. Os eventos são formados das ações dos agentes (protocolares ou operadores) num cenário onde o aparato tecnológico cumpre uma Função Distópica.

Evento é qualquer ocorrência observável em um sistema ou na rede. Essa é uma definição de Incident Handling, aŕea da segurança da informação dedicada aos incidentes de segurança, que em sua grande maioria ocorrem devido a vulnerabilidades (disfunções). A da natureza das operações distópicas na sociedade de controle do século XXI (sobretudo aquelas orquestradas por/para o Estado) é serem discretas. Aqui usarei *evento* como sendo uma ocorrência observável ou não de uma ação possibilitada por uma disfunção. Essa disfunção,

como dito, não conduz necessariamente a uma Função Distópica, e nem tão pouco é condição para que ela exista, uma vez que o aparato pode ser dedicado por design a propósitos distópicos (Hacking Team). No entanto, são evidentes as vantagens em se ressignificar o design, uma vez que o aparato atuará de maneira promíscua, constituindo um evento singular, onde a obscuridade do processo resguarda a ação dos agentes, esconde os artefatos resultantes da disfunção e, portanto, viabiliza a Função Distópica.

Agentes da Distopia

O hacker é um agente indispensável nos eventos originados de disfunções. E por isso, suas habilidades podem levá-lo a ser tratado com terrorista ou salvador da pátria a depender do seu empregador. Alexander Galloway em seu trabalho Protocol: *How Control Exists after Decentralization*, captou esse ponto com muita clareza no capítulo 5 intitulado *Hacking*:

> Hoje existem duas coisas geralmente ditas sobre hackers. Eles são ou terroristas ou libertários. Historicamente a palavra significava um funileiro amador, um autodidata que pode tentar uma dúzia de soluções para um problema antes de sair um sucesso. Aptidão e perseverança sempre eclipsaram o conhecimento rotineiro na comunidade de hackers. Hackers são o tipo de tecnófilo que você gosta tem em torno de uma pitada, por tempo suficiente, eles geralmente podem rachar qualquer problema, ou pelo menos encontrar uma solução alternativa. (Galloway, 2004, p.151)

E esses tecnófilos são indispensáveis em direções opostas, não apenas enquanto agente ativo que subverte o design da tecnologia, mas também como agente que subverte o sistema político e denuncia o emprego do aparato para finalidades obscuras que favorecem agentes do poder econômico, político ou religioso. E disso resultam aparentes paradoxos, como hackers agindo por uma organização que espiona ou fornece aparatos para espionagem e manipulação de jornalistas, dissidentes e opositores políticos. Mas essa afirmação só poderia representar uma contradição se existisse alguma homogeneidade entre os hackers, o que não há; ou se ao contrário do aspecto anárquico, inerente ao hacking, esses agentes se submetessem de livre e espontânea vontade a algum tipo de código de ética imutável, o que não acontece. O que não significa que não estejam eles também submetidos aos mesmos protocolos que governam a internet. Agentes contra-procoloco implicam na existência e eficácia de protocolos de controle, que constituem a internet.

Os vírus de computador, pirataria de software, o domínio técnico para a subversão e sabotagem podem ser considerados formas de resistência nas sociedades de comunicação e controle, maneiras de quebrar os circuitos, burlar a lógica. Essas formas de resistência atentam contra as propriedades da segurança da informação, afetando direta ou indiretamente o que se convencionou como tríade CIA: Confidencialidade, Integridade e a Disponibilidade. No entanto, no século XXI, foram tornados públicos casos onde os agentes da disfunção, são – ou atuam para – os maiores interessados na manutenção do controle, ou ao menos a isso se designam. Sendo assim, como podemos atribuir uma função de resistência para atos de subversão dos agentes dentro das sociedades de comunicação, se os agentes que atuam diretamente para possibilitar o controle das sociedades empregam as mesmas práticas subversivas? O que explica essa aparente contradição é justamente ambos os agentes estarem submetidos aos mesmos procedimentos, às mesmas regras, sejam agências de espionagem, sejam hacktivistas que atuam contra essas agências, sejam sujeitos isolados. Esses procedimentos constituem os protocolos, do ponto de vista das RFC's (*Request For Comments*), mas, sobretudo como desenvolvido por Alexander R. Galloway. Ao apresentar sua tese sobre como o controle existe após a descentralização, Galloway enfatiza que o protocolo é a razão do sucesso e que ele não se resume ao que os usuários podem ver, pelo contrário, os protocolos são a base sem a qual nada do que utilizamos hoje em termos de tecnologia existiria, e tão pouco é possível se opor a ele:

> Se opor ao protocolo é como se opor à gravidade — não há nada que diga que isso não pode ser feito, mas tal busca é certamente equivocada e no final não prejudica muito a gravidade. Enquanto o controle costumava ser uma lei da sociedade, agora é mais como uma lei da natureza. Por causa disso, resistir ao controle tornou-se muito desafiador (Galloway, 2004, p.147)

Ressalta ainda que “[..] uma razão para o seu sucesso é o alto custo para se empreender contra aqueles que ignoram o uso global de tecnologias específicas”. (Galloway, 2004, p.147)

Acontece que os agentes (agências/ativistas) lutam contra os protocolos exatamente por que uma vez subvertidos podem oferecer recursos para os quais o aparato não foi projetado originalmente. E isso exatamente por que essas ações estariam sujeitas a uma série

de burocracias e penalidades às quais os agentes não estão aptos ou interessados em cumprir ou justificar em prol de objetivos questionáveis ou resultados incertos.

Propriedades-Objetivos

Esses objetivos estão intrinsecamente relacionados à tríade CIA citada anteriormente. As propriedades da segurança da informação delineiam as variantes de disfunção que por sua vez estão atreladas aos objetivos dos agentes. A confidencialidade é a propriedade da segurança da informação que garante que *somente usuários autorizados mediante autenticação e controle de acesso poderão acessar determinada informação.* Sendo assim, uma disfunção num artefato tecnológico que afete a confidencialidade pode permitir que pessoas não autorizadas (mediante um processo de autenticação e autorização) acessem informações sensíveis ou críticas de um sistema ou usuário.

A integridade é a propriedade que garante que a informação processada, armazenada ou transmitida pelo aparato tecnológico não sofreu alteração indesejada, atestando que toda e qualquer adulteração foi permitida com base num processo de autenticação e autorização aos quais estão atrelados processos de identificação e responsabilização. Nesse caso uma disfunção que afete a Integridade possibilita, potencialmente que a informação seja modificada por um agente não autorizado, que poderá ser rastreado ou não, a depender dos demais controles implementados no aparato afetado.

Por fim, a disponibilidade garante que a informação processada, armazenada ou transmitida pelo aparato tecnológico estará disponível sem obstrução indesejada. Uma disfunção relacionada com essa propriedade pode permitir que um agente cause a indisponibilidade da informação ou do sistema, o que caracteriza os ataques de DoS (*Denial of Service*) ou DDoS (*Distributed Denial of Service*), normalmente associados a formas de protesto que se utilizam da sabotagem. Em 2010 o Wikileaks divulgou o que foi conhecido como *United States diplomatic cables leak, uma série de* 251.287 cabos (comunicação via submarino, via cabos) somando 261.276.536 palavras, tornando o Cablegate "o maior conjunto de documentos confidenciais a serem liberados para o domínio público", segundo o Wikileaks. Tão logo os documentos foram publicados, corporações como Mastercard, Amazon, Paypal, BankAmerica, Swiss bank PostFinance e visa suspenderam as doações para o Wikileaks. Em retaliação, a operação Payback foi executada pelo Anonymous em Dezembro

de 2010. PayPal, PostFinance e Mastercard sofreram poderosos ataques de DDoS, um tipo de ataque que tem por objetivo afetar a disponibilidade dos serviços e que retirou do ar todos os sites de algumas dessas empresas.

Dessa maneira, observa-se que o polimorfismo das disfunções mantém um vínculo estreito com as respectivas propriedades da segurança afetadas, embora suas possibilidades não se restrinjam a elas, o que caracteriza a Função Distópica.

3. OBJETIVOS

O presente trabalho tem como objetivo analisar as *disfunções* tecnológicas e suas implicações sociais, políticas e econômicas na sociedade de controle do século XXI. Por *disfunção* devemos entender *a tecnologia operando de uma maneira inesperada, segundo seu design (função).* Operar de maneira inesperada é possível quando a *disfunção* presente em determinada tecnologia não inviabiliza sua função (propósito inicial) mas, ao invés disso, produz novas funções, que por serem produto de um desvio, atuam de modo invisível, possibilitando operações não documentadas em suas especificações — e que portanto, não sofrem influência de leis, regras, ou preceitos morais. Uma disfunção pode ser originada por diversos fatores, como vulnerabilidades decorrentes de implementação (bugs no código fonte), abuso de funcionalidades, ou mesmo backdoors (funcionalidades ocultas plantadas durante o desenvolvimento do software, por exemplo). Portanto, o termo disfunção no contexto tecnológico, extrapola seu significado de mero defeito em sua função e adquire um caráter extensivo, ou seja, aquilo que a tecnologia possibilita quando funcionando de modo subvertido.

3.1 Geral

Com isso pretende-se fornecer uma teoria — baseada em casos reais e em consonância com a literatura relacionada ao tema — de como a terceira guerra vem acontecendo diante dos nossos olhos pelo meio eletrônico-digital. Para tal é preciso levar em conta além dos estados da tecnologia, os atores, cenários, contextos e aparatos que serão analisados.

3.2 Específicos

Os estados da tecnologia são aqui tratados como função, disfunção, distopia. Sendo que inicialmente, a tecnologia é apresentada aos usuários segundo sua função apenas. Quando ocorre uma disfunção torna-se possível realizar novas funções não previstas no design original da tecnologia; que por sua vez podem conduzir a um estado distópico, aqui conceituado como um estado em que é possível rastrear, vigiar, incriminar, possibilitando, portanto, um controle completo e ao mesmo tempo revestido de um aspecto irreal, abstrato por se dar no meio digital.

4. PROCEDIMENTOS DE PESQUISA

A pesquisa busca dialogar com a literatura existente sobre o tema, citada nas referências bibliográficas, e sobretudo com o conceito de Protocolo como apresentado por Alexander Galloway em seu trabalho *Protocol How Control Exists After Decentralization*. Vale ressaltar que trabalhos nessa linha, são raros senão inexistentes no Brasil. E frequentemente se tratam ou de análises puramente sociológica que não contemplam os aspectos técnicos fundamentais para se compreender o problema, ou análises puramente técnicas que não dão conta ou não têm a pretensão de expôr o impacto político-social — inerente ao objeto.

Embora balizado por excelentes trabalhos que direta ou indiretamente discutem o tema, a pesquisa pretende analisar também alguns casos reais amplamente divulgados, como por exemplo, Julian Assange e o Wikileaks; Edward Snowden; grupos hacktivistas (Shadow Brokers, Phineas Phisher, Anonymous, Lulzsec), assim como aqueles que atuam para agências de espionagens, como o Equation Group (Grupo de hackers que atuam para a NSA) e o Fancy Bear (ao que tudo indica até o presente momento, grupo associado ao governo Russo). Esses agentes são responsáveis tanto pelo estado distópico (aquele alcançado através da aplicação da disfunção na função), como também pela divulgação dos cenários, eventos e contextos possibilitados pelo estado distópico (whistleblower) — casos onde temos uma ruptura com os sensores e agências. Além disso, são considerados agentes (passivos) aqueles responsáveis pelo estado inicial da tecnologia, ou seja, responsáveis pela função inicial, aquela que dá o sentido de existir da tecnologia.

Os procedimentos de pesquisa terão como foco analisar casos conhecidos de grande repercussão, como os citados acima, e demonstrar como todos se encaixam na tríade que denomino Função, Disfunção, Distopia no presente trabalho. Além disso é escopo deste trabalho, analisar como ocorre e qual o efeito dessa interação entre ficção científica e realidade no contexto da guerra, terrorismo e ativismo no século XXI.

Cronograma de Atividades 2018

Atividades	Mar	Abr	Mai	Jun	Jul	Ago	Set	Out	Nov
Pesquisa do tema	X								
Definição do tema	X								
Pesquisa bibliográfica		X							
Coleta de Dados			X						
Apresentação e discussão dos dados									
Elaboração do projeto			X	X	X	X	X		
Entrega do projeto									**X**

Bibliografia

GALLOWAY, Alexander. **Protocol: How Control Exists after Decentralization.** MIT Press, 2004.

LÉVY, Pierre. **Cybercultura**. Editora 34; Edição: 3 (1 de Janeiro de 1999).

WIKILEAKS; **Projeto Vault 7.** Part I:Year Zero - 23 de Março de 2017.