Geopolitica da Vigilância: Globalização e Guerras Híbridas[1]

Pedro Vidal Diaz[2]

Resumo: A globalização da vigilância em comparação com casos geopolíticos e a produção de hegemonia com suas linhas de fuga analisadas na figura do hacker Esse artigo busca traçar a globalização da vigilância como forma de manutenção e exercício de um poder global e geopolítico que utiliza-se da manipulação de bolhas informacionais e tecnológicas para efetuar a antiga estratégia de “enganar, dividir e conquistar”, mas que sempre produz suas linhas de fuga, analisadas aqui, na potência do hacker, tanto pela tecnologia social como em resposta às estratégias de militarização da vida. Buscarei, com noções de Deleuze, Guattari e Lazzarato, apresentar casos históricos concretos de conflitos e estratégias internacionais, onde a vigilância se desenvolve na produção globalizada do capitalismo contemporâneo, traçando um diálogo da cibercultura como Paul Virilio, Berardi e Eugênio Trivinho junto ao campo da Ciência da Informação e seus autores como Sandra Braman, Armand Mattelart.

Palavras-chave: Vigilância, geopolítica, ciberwar, informação, hacker

1 Artigo apresentado no IX Simpósio Nacional ABCiber – PUC São Paulo -8, 9, 10 DEZEMBRO 2016.

2 Mestrando em Ciência da Informação no IBICT/UFRJ-RJ. Email: pedrovdiazz@yahoo.com.br

> *Agora somos um império e, quando agimos, criamos nossa própria realidade. E enquanto vocês estão estudando essa realidade – judiciosamente, como o farão – nós iremos agir novamente, criando outras novas realidades, as quais vocês podem estudar, e isso é como as coisas irão se desenrolar. Somos atores da história (…) e vocês, todos vocês, vão limitar-se a estudar o que fazemos* (Suskind, 2004).[3]

Desde os primeiros dias que se seguiram ao atentado de 11 de setembro, Bush prevenira: "os Estados Unidos iam se lançar em um novo tipo de guerra, uma guerra que requer de nossa parte uma caça ao homem internacional"[4]. O que a princípio soava simplesmente como um slogan pitoresco de um caubói texano fora depois convertido em doutrina oficial e internacional de Estado, com especialistas, planos e armas bélicas junto ao desenvolvimento de sistemas info-digitais de vigilância aprovando o Patriot Act[5]. Em uma década constitui-se uma forma não convencional de violência de Estado que combina as características dispares da guerra e de operação policial que encontra sua unidade conceitual e prática na noção de

3 (Suskind, Ron. "Faith, Certainty and the Presidency of George W. Bush", 17/10/2004). (Embora não seja atribuída, muitos acreditam que elas foram ditas no verão de 2002 por Karl Rove, um importante assessor do presidente George W. Bush.)

4 "*President Speaks at FBI on New Terrorist Threat Integration Center*", 14 fev. 2003. In: CHAMAYOU, G. *Teoria do Drone*. 2014. p. 30.

5 USA PATRIOT Act é o acrônimo "*Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act*" de 2001 (em português algo como "Ato de Unir e Fortalecer a América Providenciando Ferramentas Apropriadas e Necessárias para Interceptar e Obstruir o Terrorismo").

caça militarizada ao homem globalizado que agora, após quinze anos, ainda se intensifica em um segundo projeto de lei, o Cyber Patriot Act (CISA). A primeira tarefa não é mais imobilizar ou aniquilar o inimigo e sim identificá-lo e localizá-lo. Isso envolve todo um trabalho de detecção generalizada com o uso intensivo das novas tecnologias que combinam vigilância aérea, informacional, vídeos e gravações, interceptando sinais e traçados sócio-cartográficos. A topografia das conexões é uma extensão da prática generalizada da análise de redes sociais utilizadas para desenvolver os perfis dos indivíduos de grande interesse ou valor traçando fóruns sociais e ambientes que ligam os indivíduos uns aos outros em "nódulos-chaves" estratégicos. A expansão da "Nuvem" como campo de agenciamento conectivo e virtual.

Os "dotcoms" no começo da internet global pela década de 1990 foram laboratórios para a formação de novos modelos de produção e Mercado, mas no final o Mercado estava sufocado por monopólios e exércitos de auto-empreendedores e pequenas iniciativas dispersas que finalmente foram sujeitados à precárias formas de emprego em um tipo de cognitariado. As corporações acabaram por tomar a liderança na nova economia de rede ("net-economy") e aliaram-se com os grupos dominantes da velha oligarquia, bloqueando e pervertendo o próprio projeto de globalização. O Neoliberalismo produziu sua própria negação: a dominação de monopólios e a ditadura de Estados-militares. A promessa ao qual estava implícita a nova economia virtual oferecia grandes recompensas e participação nas fortunas econômicas do novo sistema. Mas aí veio o "Bug do Milênio", o "data-crash", o colapso do novo milênio 2000, iniciando novas condições de terror e controle na modernidade intensiva. A imaginação social estava carregada de expectativas apocalípticas no mito do tecno-colapso global que levou ondas midiáticas e especulativas aterrorizantes por todo o globo. Nada aconteceu naquela noite de 'milênio, mas a psique global tremeu e fraquejou à beira do abismo (BERARDI, 2014, p. 160).

> A profusão cotidiana de informações – alarmantes para uns, apenas escandalosas para outros – molda nossa apreensão de um mundo globalmente não inteligível. Seu aspecto caótica é a névoa de Guerra por trás da qual ele se torna inatacável. É por meio de seu aspecto ingovernável que ele é realmente governável. É aí que está a malícia. Ao adotar a gestão da crise como técnica de governo, o capital não se limitou apenas a substituir o culto do progresso pela chantagem da catástrofe, ele quis reservar para si a inteligência estratégica do presente, a visão de conjunto sobre as operações em curso. E é isso que é importante disputar com ele. Trata-se, em material de estratégia, de voltarmos a estar dois passos à frente em relação à governança global. Não há uma "crise" da qual é preciso sair, há uma Guerra que precisamos ganhar! (Comitê Invisível, 2016:19).

Com o avanço da propaganda nos anos 1920 e, posteriormente, com o advento da televisão, uma máquina valorativa cada vez mais bem-organizada se desenvolveu, da qual o Google, Apple e Facebook podem ser considerados a nova fronteira de interesse. Em 2014, a Comissão Federal de Comunicação dos EUA propuseram o fim da neutralidade da rede dando aos grandes pagadores (Amazon, Google, Facebook e Netflix) o acesso rápido de uso, enquanto que usuários ordinários ficam para trás no jogo mercadológico financeiro (MIRZOEFF, 2015, p. 7). Isso mostra o deslocamento constante da fronteira, buscando e criando outros territórios de expansão e imperialização arbórea do capital de investimento. O novo 'celeiro do mundo' é o mercado informacional emergente em uma "economia de Mercado informacional" e transborda na vigilância gerenciadora de toda uma diplomacia internacional. Criam-se bolhas de valoração e exploração para aliviar e compensar as despesas investidas em outras bolhas financeiras, predando assim, toda a especulação ativa de áreas de economia real, não-financeiras. Com isso, marcam a intensificação e uso de um tipo de corrupção ideológico e totalitário que mobilizam governos, infraestruturas e ideologias a corresponderem à uma forma organizacional, supranacional e trans-estatal de produção e valoração financeira/econômico, (principalmente depois da quebra da bolha do mercado imobiliário nos Estados Unidos em 2008), transferindo investimentos para o setor tecnológico do "Vale do Silicone"[6]. Tal escalonamento emergente levou às denúncias feitas por vazamentos de documentos e registros desde o caso do Wikileaks junto ao soldado Manning quanto ao analista de sistemas ex-contratado pela CIA/NSA, Edward Snowden e que não sabemos todos os desdobramentos de tais operações.

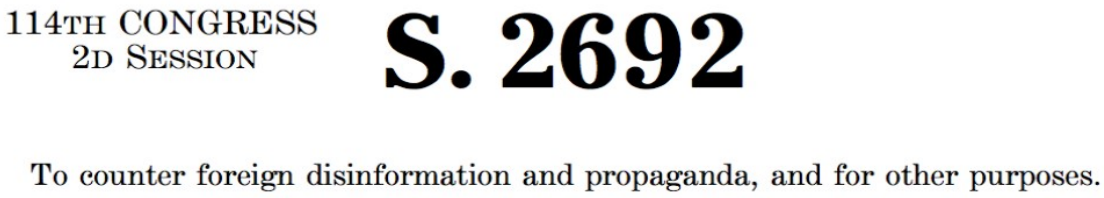
> "É alarmante que as capacidades de vigilância desenvolvidas nas mais avançadas agências de espionagem no mundo estão sendo empacotadas e exportadas em volta do mundo por lucro. A proliferação de tais capacidades de vigilância intrusivas é extremamente perigoso e impõe uma ameaça real e fundamental para os direitos humanos e a democratização" afirma o pesquisador Edin Omanovic oficial da Privacy International. Cf.: https://theintercept.com/2016/10/17/how-israel-became-a-hub-for-surveillance-technology/.

6 Por exemplo a biografia de Ruth Porta: vice-presidente do banco Morgan Stanley durante a crise de 2008, mudando para a presidência da Alphabet In., subsidiaria da Apple onde produz material interativo e didático educativo. Ela é membra do Comitê de Consulta de Empréstimos do Tesouro dos Estados Unidos, na banca do Fundo de Investimentos da Universidade de Stanford, na banca dos diretores do Conselho de Relações Exteriores, na banca do Clube de Seguros Econômicos de Nova York e do Comitê de Bretton Woods assim como membra do Conselho de Consulta do Centro Fiscal Hutchins e da Instituição de Política Monetária e Fiscal. Cf.: *Financial Oligarchy and the Crisis* – Entrevista do Professor do MIT Simon Johnson com Harvey Stephenson. Grand Cayman, Ilhas Cayman, 20 Janeiro, 2010.

A ideia desse arquivo-geral que garantisse antecipadamente a rastreabilidade retrospectiva de todos os itinerários e de todas as gêneses busca a capacidade de estocagem, indexação e análise que os sistemas atuais não possuem: O principio de arquivamento total ou de um filme de todos eventos e vidas (CHAMAYOU. 2014. p. 33). A vigilância info-óptica, não se limita à vigília em tempo real. Ela se redobra como uma função de gravação e arquivamento produzindo uma cartografia temporal dos acontecimentos para que se possa rastrear em uma topografia cronológica, rastreando sua genealogia de ameaças e seus possíveis desdobramentos – "Se uma cidade pudesse ser vigiada de uma só vez, os carros-bombas poderiam ser rastreados até seu ponto de origem" (Idem). Segundo um analista da Air Force:

> Hoje, analisar imagens capturadas pelos drones é uma atividade entre trabalho social e ciências sociais. O foco esta na compreensão dos 'esquemas de vida' e nos desvios desses esquemas. Por exemplo, se uma ponte normalmente cheia de gente se esvazia de repente, isso pode significar que a população sabe de uma bomba ali. Agora vocês estão começando a fazer um trabalho de estudo cultural, estão observando a vida das pessoas. (In.: CHAMAYOU, 2015, p. 37)

Um desses órgãos de apoio à estratégias info-tecnológicas, trata-se de um órgão ultra-secreto, ligado à NSA, chamado *Sinio Council*, que estuda as dinâmicas de cada país, com objetivo de promover interferências que atendam os interesses econômicos e políticos dos Estados Unidos, em especial do governo e das corporações norte-americanas. Uma lei promulgada neste ano de 2016, o *"Countering Information Warfare Act of 2016"* afirma esta tendência acirrada da militarização da diplomacia e da globalização para "*contrariar propaganda e desinformação estrangeira, e para outros propósitos*":


114TH CONGRESS
2D SESSION

S. 2692

To counter foreign disinformation and propaganda, and for other purposes.

A racionalidade política subjacente a esse tipo de prática é a da medida de segurança para o social que não é destinada a punir mas somente preservar a sociedade contra o risco que ela corre em seu seio na presença de seres perigosos[7]. Daí o imperativo categórico para potências

7 No Brasil, a primeira iniciativa desenvolvida fora a criação do '*Centro de Defesa Cibernética*' (CDCiber) onde teve como primeira missão o monitoramento de rede da Rio+20, a conferência das Nações Unidas sobre Desenvolvimento Sustentável, que aconteceu no mês de Junho de 2012 e foi um ambiente comum para ataques

globais de perpetuar um sistema de "global information dominance". A hegemonia cultural se confunde com o exercício do softpower, o poder de sedução e o recuo das estratégias que recorrem à força e à coerção (MATTELART, 2005, p.9).

As grandes empresas de Tecnologia da Informação (TI) estão cada vez mais a frente dos poderes estatais de coordenação e controle do tráfego informacional global. A supervia informacional junto ao portal da web estão enquadrando uma nova hierarquia na Data-esfera e pavimentando um caminho para uma cartografia especifica da internet de redes. O processo de (des) mapear nos convida a uma nova relação espacial na era das redes globais, de altas frequências de comércio, cabos submarinos e rotas automatizadas e contra esse fundo constitutivo, uma nova medida de crítica pode se tornar tão simples como o atraso latente da transmissão entre servidores e terminais (o 'lag' ou o tempo de Ping). Baseado em um "comando de Ping", esse projeto faz a manutenção dos 193 países da ONU de acordo com o tempo de resposta em relação à seus 'sites' governamentais, definindo suas distâncias e presenças virtuais na rede, como expressado geograficamente por Mark Graham:

Mark Graham e Stefano De Sabbata, feito com "Natural Earth" - Oxford Internet Institute, Agosto de 2013.

O aspecto central da doutrina da "global information dominance" é justamente a segurança e a defesa. Conceitos como "netwar" e "cyberwar"[8], exprimem os componentes da dita "sociedade do conhecimento", a "noopolítica" como fronteira da "nooguerra". Trata-se aqui de controlar agendas de prioridades de tal forma que se imponham naturalmente à outros

vindo de hacktivistas. O evento fora a prova de fogo para a estrutura de defesa contra ataques cibernéticos do país que reunia cerca de cem chefes de Estado e de governo.

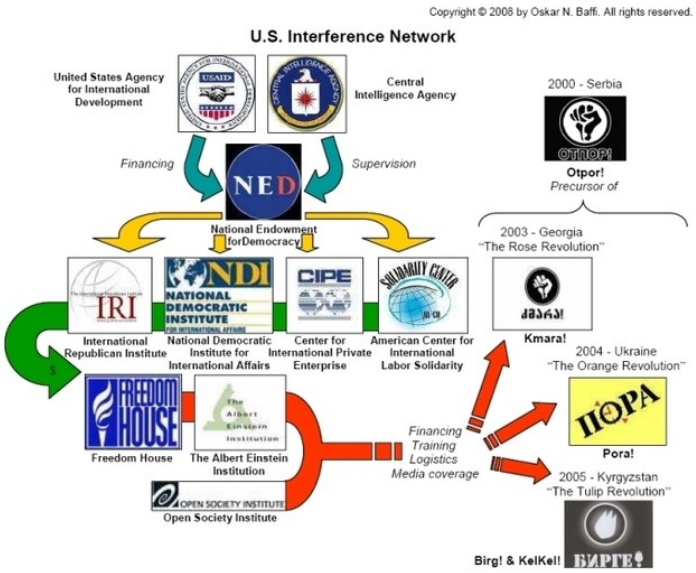
8 A netwar é feita contra os novos inimigos que recorrem às redes: os cartéis da droga, os ativistas, os terroristas, etc. A cyberwar aplica-se às novas formas da guerra tornadas possíveis graças ao domínio das tecnologias da inteligência, da vigilância e do reconhecimento. (MATTELART, 2005. p.10. Disponível em: http://www.gepicc.ufba.br/enlepicc/. Acesso em: 27/06. 2016.)

países, conduzindo-as a aceitar as normas e instituições conforme os interesses hegemônicos. Nessa lógica de segurança baseada na interceptação preventiva de indivíduos perigosos, a guerra toma forma de vastas campanhas de execuções e perseguições extrajudiciais. O 'Predator' ou 'Reaper' – (aves de rapina e ceifador da morte) são nomes de veículos não tripulados (VANTS ou DRONES) e indicam literalmente a representação de suas funções e propósitos.

O controle portanto, é de curto prazo e de rotação rápida, mas também contínuo e ilimitado. "O homem não é mais o homem confinado em instituições" e sim o homem endividado e rastreado por sistemas info-vigilantes de indexação e cobrança em 'extituições' de gerência e controle - "Pobres demais para pagar a dívida, numerosos demais para o confinamento" (DELEUZE, 1992a, p. 220). O controle não só terá que enfrentar a dissipação das fronteiras, mas também a explosão dos guetos e favelas em seus movimentos de contra-ação e resistência. Se na sociedade disciplinar a normalização constituinte era muito pautada pela palavra de ordem, na sociedade de controle torna-se o algoritmo, a cifra, o código ou a senha de passagem entre a o controle e a fluidez de circulação (bens, pessoas, informação, etc). A especialização tecno-social de controle se engendra por dentro, se especializa, se condensa e articula novas formas de interação e existência, constituindo-se também como agenciamento desse devir-hacker que estamos permeando. O lado totalitário do hackeamento é produzido como vigilância, manipulação informacional e subjetiva da opinião pública jogadas em camadas aparentemente confusas e desconectadas, escondendo os verdadeiros intuitos estratégicos de poder e controle em guerras chamadas de 4ª geração[9], guerras não-lineares ou Guerras Híbridas, esbarrando e transbordando o desenvolvimento aplicado das teorias do caos, incerteza e complexidade na era pós-keynesiana (FILHO&ARAÚJO, 2000).

> A violência é, doravante, parte essencial da instalação do projeto econômico global, ou melhor, da "representação do mundo" (shaping the world). Seu instrumento comum: o domínio do tempo eletrônico, a observação e a escolha do público alvo em tempo real. Timely knowledge flow: a divisa da nova doutrina militar sobre o network-centric war desde a guerra do Afeganistão é também a dos estrategistas da economia (MATTELART, 2005, p.12).

9 O termo "guerra de quarta geração" vem sendo empregado para designar o conflito multidimensional, envolvendo ações em terra, no mar, no ar, no espaço exterior, no espectro eletromagnético e no ciberespaço. Nesse contexto estratégico, o "inimigo" pode não ser um Estado Nacional, mas um grupo terrorista ou outra organização criminosa qualquer.



Rede de financiamento cultural e criação de 'líderes' de oposição em diferentes países (Revoluções coloridas como as indicadas no gráfico de Oskar N. Baffi, 2008.

O processo onde pessoas são postas como alvo em listas da morte ("Kill Lists") e ultimamente são assassinadas por ordens de alto escalão em segredo e sem provas ou processos jurídicos e transparentes. Listas de vigias que monitoram pessoas pelos bastidores e classificam-as em listas, atribuindo números processados e indexados, ganhando sentenças de morte sem aviso prévio em um campo de batalha global sem limites ou fronteiras. Uma doutrina toda sendo desenvolvida nos termos "find, fix, finish" (encontrar, decidir, finalizar) combustadas após o marco de onze de setembro (9/11)[10] como engenharia social do terror, do medo e decepção. A guerra sem fronteiras está finalmente refinada e institucionalizada. Seja através do uso de drones, mísseis de longo alcance, incursões noturnas, manipulação midiática e informacional dos fatos e em novas plataformas e estratégias ainda não totalmente relevadas, o que vemos através de vazamentos, 'hacks' e até por pesquisas mais específicas, é que a normalização do assassinato e guerra sigilosa é um componente central na geopolítica contemporânea, principalmente na doutrina de contra-terrorismo dos Estados Unidos[11].

10 CF.: FUERZA, Zander. "Masters of Deception: Zionism, 9/11 and the War on Terror Hoax", 2013.

11 Em setembro de 2009, o Gen. David Petraeus publicou uma ordem executiva chamada "Joint Unconventional Warfare Task Force" que habilita as bases para forças militares conduzirem ações clandestinas e expandidas no Iêmen e também em outros países. Permite forças especiais 'americanas' a entrar em qualquer país, aliado ou inimigo, para "construir redes que podem penetrar, atrapalhar, derrotar e destruir a Al' Qaeda e qualquer grupo militante, assim como preparar o ambiente para futuros ataques por forças militares americanas ou locais. Disponível em NY Times, 24 de Maio, 2010: http://www.nytimes.com/2010/05/25/world/25military.html?_r=0

Referências Bibliograficas:

BERARDI, Franco. *AND: Phenomenology of the End – Cognition and sensibility in the transition from conjuntive to connective mode of social communication*. N-1. Aalto University, Helsinki, 2014.

BRAMAN, S. *Information, policy, and power in the informational state. In Change of state: Information, policy, and power.* Cambridge, MA: MIT Press. 2006.
CHAMAYOU, Grégoire. *Teoria do Drone*. Tradução Célia Euvaldo, São Paulo: Cosacnaify, 2015.
DELEUZE, Gilles; GUATTARI, Felix.. *Postscript on the Societies of Control*. Outubro, vol. 59, 1992a.
_____. Mil platôs: *Capitalismo e esquizofrenia*, vol. 3. São Paulo: Editora 34, 1996.
ECO, Umberto. *Apocalípticos e Integrados*. 1ª ed. LUMENS, Paris,1968.
GONZALEZ DE GOMEZ, Nélida. Regime de Informação. Inf. & Soc.:Est., João Pessoa, v.22, n.3, p. 43-60, set./dez. 2012.
GRUPPI, L. 1978. *O conceito de hegemonia em Gramsci*. Rio de Janeiro: Graal. LACLAU, E. 1993.
MATTELART, Armand. *Sociedade do conhecimento e controle da informação e da comunicação*. In: Encontro latino de economia política da informação, comunicação e cultura. 5, Salvador, 2005. p.1-22. Disponível em: http://www.gepicc.ufba.br/enlepicc/. Acesso em: 1 jun. 2007.
MIRZOEFF, Nicholas. *Control, Computer and Execute: Debt and New Media, The First Two Centuries*. In.: "You are not a Loan: Debt and New Media". Org.: Wendy Chun e Anna Fisher, *New Media, Old Media*, Nova Yorj: Routledge, 2015.
TRIVINHO, Eugênio. *A Dromocracia Cibercultural*. Ed. Paulus, 2007.
WARK, Mckenzie. *A Hacker Manifesto*. Harvard University Press, 2004.