AS NOVAS TECNOLOGIAS: UM ENSAIO SOBRE O FIM DA SEGURANÇA INTERNACIONAL COMO CONHECEMOS.

NEW TECHNOLOGIES: AN ESSAY ON THE END OF INTERNATIONAL SECURITY AS WE KNOW IT.

Bruno Celidonio[1]

RESUMO
Este artigo pretende, através de uma análise das novas tecnologias que surgem diariamente no mercado, estudar as atuais formas de controle e de vigilância internacionais e entender como estas inovações repercutem na segurança não apenas das informações no âmbito internacional, mas também dos próprios governos dos países, apontando, com isso, exemplos contemporâneos de falhas e perigos deste novo sistema comunicacional.

PALAVRAS CHAVE
Informação; segurança; novas tecnologias; vigilância.

ABSTRACT
This article intends, through an analysis of the new technologies in the market, to study current forms of control and international surveillance, also how those innovations repercute in the security of not only the international information, but on the countries governments themselves, demonstrating as contemporary examples failures and dangers of this new communication system.

KEYWORDS
Information; security; new technologies; surveillance.

Introdução

Existem mais de setenta formas de agressões cibernéticas: Anonymizer; ARP cache poisoning; Backdoor; Backscatter; The Blues- Bluebugging, Bluejacking and Bluesnarfing; Buffer overflow; Bullying in Cyberspace; Click fraud; Computer trespass; Cookie Manipulation; Copyright infringement; Crap-flooding; Cyber Stalking; Cyber Terrorism; Cyber Warfare; Data Diddling; Data Leakage; Defamation; DOS / DDOS; DNS poisoning; Easter Eggs; Email Spoofing; Encryption use by terrorists; eShoplifting; Financial Crimes; Fire Sale; Fire Walking; Foot-

1 Mestre em Comunicação Social pela Pontifícia Universidade Católica do Rio Grande do Sul, Bacharel em Relações Internacionais pela ESPM-SUL, Bacharel em Direito pela Universidade Federal de Pelotas. brunocelidonio@gmail.com

> printing; Fraud; Online Gambling; Google based hacking; Griefers; Hactivism; Hijacking; Identity Fraud; Impersonation; Joe – Job; Key stroke Logging; Logic Bomb; Lottery Scam; Mail Bombing; Malware; Nigerian 419 Fraud Scheme; Packet Sniffing; Phishing & Spoofing attacks; Piggy backing; Piracy of Software; Pod Slurping; Poisoning the Source; Pornography; robots.txt file; Port scanning; Rootkits; Salami Theft; Sale of Illegal Articles; Scavenging; Smishing; Social Engineering; Spambot; SQL Injection; Stealware; Time Bomb; Trojan; URL Manipulation; Virus Attack; Web defacement; Vishing; Wire – Tapping; Worm; XSS Attack; Y2K; Zero Day Attack; Zeus; e Zombie. (SHAH, 2013)

A resumida listagem acima de formas de invasão (ou agressões cibernéticas) representa apenas as mais simples (e talvez hoje arcaicas) maneiras de se invadir um espaço virtual de segurança através de computadores. Ao alcance de um clique, qualquer pessoa que se aprofunda no mundo *hacker* pode se utilizar destas "armas" para burlar códigos e obter informações restritas de pessoas, empresas ou governos.

O advento de novas tecnologias criou uma chamada "arte moderna" de espionagem, fazendo com que a vigilância e a invasão chegasse a novos patamares, cujos rumos nem mesmo Pierre Lévy (2009) poderia prever em seus ensaios sobre cibercultura, ou seja, o estreitamento da comunicação e a sua rapidez fez com que a tecnologia que se introduziu na vida cotidiana também repercutisse no âmbito da segurança nacional. Aparatos que até então seriam voltados para aproximar o virtual do real, tendo seu principal uso comercial voltado para lazer e ações profissionais, como um *e-mail* ou um *google glass*, hoje fazem com que o que parecia apenas possível em um futuro distópico seja um perigo iminente. A possibilidade de se usar um óculos como tela para comunicação, transportar dados, filmagem e fotografias, em tempo real e de fácil compartilhamento, acaba por mudar a forma de se tratar de segurança e de sigilo da informação, e aquilo que antes era de se imaginar como sendo um *gadget* digno de um filme ficcional do espião britânico James Bond, hoje é extremamente plausível de ser usado não apenas por um repórter que queira registrar um fato quando ele ocorre, mas também por qualquer cidadão munido da mesma tecnologia para seu lazer cotidiano ou, ainda, um sujeito que queira registrar acontecimentos políticos e dados sigilosos de forma a passar despercebido.

E é graças a rapidez com que estes novos aparatos tecnológicos se tornam cada vez mais inseridos ao corpo e aos utilitários cotidianos, como celulares, óculos ou relógios, que transformam um homem comum em uma espécie de ciborgue moderno, se tornando em uma potencial ameaça à segurança internacional.

De Anonymous até Hillary: nenhum governo está a salvo.

Ao passo que a modernidade trouxe novas tecnologias digitais de comunicação, modelos mais sofisticados e precisos de comando exerceram um controle até então desconhecido pela sociedade, através primordialmente

da vigilância, esta que, entretanto, também ofereceu novas oportunidades de resistência a este mesmo controle. Em referência a este assunto, ao tratar do que chama de "sociedade de controle", Deleuze (1992) explica que este se situaria em um patamar superior ao que entende por disciplina, e esta, por sua vez, sucederia a soberania. Galloway (2004), avançando em uma linha temporal neste assunto, ao tratar de um momento essencialmente cibernético como o contemporâneo, analisa que tecnologias digitais de comunicação seriam ferramentas fundamentais da sociedade de controle, e a internet seria sua maior expressão, fazendo dos *hackers*, portanto, atores políticos.

E com o avanço ininterrupto da digitalização das informações e seu uso contínuo, todos são passíveis de controlar e ser controlados o tempo todo, através de rastros de navegação ou programas de ciber vigilância, visto que a sociedade está, constantemente, inserida em um fluxo de redes, seja na academia, no comércio, no transporte, nas telecomunicações, em seu lazer ou no próprio uso da computação. Qualquer que seja a atividade exercida na sociedade atual, suas redes irão gerar dados ou padrões comportamentais passíveis de serem rastreados.

Então como impedir este rastreio?

O próprio controle pode operar através de bloqueio de conteúdos, através do que se entende por "protocolo", no que tange às informações confidenciais, os segredos de Estado e principalmente as questões que envolvem softwares, linguagens de programação e padrões de rede. Assim, seriam criadas recomendações ou regras técnicas que definiriam o modo como "tecnologias específicas são acordadas, adotadas, implementadas e usadas pelas pessoas no mundo" (GALLOWAY, 2004, p.7), como ocorre na simples navegação da internet, em que se torna necessário aceitar um protocolo, ou seja, o conjunto TCP/IP (*Transmition Control Protocol/Internet Protocol*).

Galloway (2004) porém explica que tal controle se tornaria ilusório, já que este ambiente também incitaria uma resposta, uma forma de romper essas amarras, o que se observa no ativismo *hacker*, este que visa furar bloqueios indesejáveis, acessar e liberar informações de interesse público, ter acesso a privacidade do usuário, criptografar comunicações e desenvolver softwares livres das amarras das grandes corporações.

E se de um lado Levy explicitava em seu clássico *Hackers: Heroes of the computer revolution* (2010) que as informações devem ser totalmente livres e o uso de computadores, dado ao seu caráter revolucionário, ser tão universal quanto possível, bastaram alguns e-mails serem expostos para que, em 2010, o caos fosse disseminado entre os governos das grandes potências mundiais, naquilo que Galloway (2004) irá chamar de hipertrofia de controle, ou seja, investidas contra o controle cibernético. É nesse ambiente que o *WikiLeaks*

encontrou seu espaço, burlando controle governamental e protagonizando o caso *Cablegate*, entre polêmicas diplomáticas e intensos debates referentes à liberdade de imprensa.

Ironicamente, a principal forma encontrada pelo grupo para a manutenção das suas informações foi justamente o canal usado para obtê-las. Sabendo que a proteção das suas fontes de informação é algo primordial para a sobrevivência da organização, foi através da própria internet que se promoveu a entrega de documentos governamentais sigilosos, uma vez que a maioria dos países ou impõe poucas restrições jurídicas ou não possuem qualquer regra no que tange ao uso do ciberespaço. Ainda, como forma de assegurar a sua própria segurança, foi usada criptografia em dados compartilhados de forma a não poderem ser rastreados e, consequentemente, revelados os remetentes, blindando com o anonimato quem contribuísse para o projeto (DOMINGOS; COUTO, 2011). O movimento *Anonymous*, portanto, é o principal exemplo internacional de uso das novas tecnologias criando um problema internacional, já que empreendeu em ações digitais diretas de rompimento do controle como forma de protesto aos atos de governos e corporações internacionais, resultando em uma ação compartilhadas por uma rede de grupos e indivíduos dispersos mundialmente, de difícil identificação.

Este não foi o último caso envolvendo o *wikileaks*. O medo de novos ataques da organização acabaram por expor ação, nas últimas eleições americanas de 2016, da então candidata Hillary Clinton referente a e-mails sigilosos e privados, de quando foi Secretária de Estado (2009-2013). Erroneamente e sem permissão do governo, a candidata se usou de uma conta particular de e-mail para trocar cerca de 61 mil mensagens de conteúdo secreto do governo norte-americano, o que o Jornal New York Times tratou à época como um risco para a segurança nacional, por ficar vulnerável, por exemplo, ao ataque de *hackers* como os *Anonymous*. O medo e a fragilidade da potência econômica de serem invadidos e terem seus dados expostos, ficou clara. Até os Estados unidos estavam vulneráveis aos ataques de *hackers*.

E no que tange ao cenário internacional, os resultados não foram diferentes.

Assim, a principal consequência do WikiLeaks (sem se aprofundar aqui nas constantes crises diplomáticas que se sucederam), foi a inovação no uso da informação enquanto arma política capaz de promover transformações (OLIVEIRA, 2012), uma vez que o movimento conseguiu, de fato, evidenciar o completo despreparo dos Estados, quer seja por sua diplomacia, que seja por suas legislações, em relação a informatização do conhecimento na política internacional.

Um passo para o futuro: as novas tecnologias e a privacidade da informação.

Em 18 de dezembro de 2011 foi exibido pelo Channel 4, canal de televisão britânico, "Toda a sua história" (*The Entire History of You*), terceiro e último episódio da primeira temporada da série antológica de ficção científica britânica *Black Mirror*. O episódio em questão tratava de uma realidade em um futuro ficcional, onde parte das pessoas possuía implantado atrás de suas orelhas um *nano chip*, capaz de registrar tudo o que havia sido feito, visto ou ouvido. Desta forma, o *device* permitiria que as memórias fossem gravadas, buscadas e reproduzidas ou na própria visão da pessoa, ou em uma tela de televisão ou computador. Três anos depois da obra ficcional ir ao ar, em 2014, a empresa Google, em parceria com o laboratório farmacêutico Novartis, anunciou a criação de uma lente de contato inteligente desenvolvida para controle da diabetes. Uma vez colocado no olho, o dispositivo usava lágrimas para monitorar a quantidade de glicose presente no sangue. Em 2016, a empresa transnacional Samsung registrou patente na Coreia do Sul de uma lente de contato inteligente que teria câmera fotográfica e outros comandos ativados por piscadas oculares do usuário.

O que antes seria ficção, hoje parece tomar forma de realidade. Próteses se misturam a artefatos, pequenas cápsulas contém em seu interior nanotecnologias, microchips substituem cartões de crédito, e um clique parece, aos olhos de um usuário de *device* como um *google glass*, um longo caminho a percorrer para se tirar uma simples foto. Para Lévy (1996), olhar para estas tecnologias como um grande avanço pode representar uma miopia frente ao que ainda está por acontecer.

> No final das contas, as biotecnologias nos fazem considerar as espécies atuais de plantas ou de animais (e mesmo o gênero humano) como casos particulares e talvez contingentes no seio de um continuum biológico virtual muito mais vasto e ainda inexplorado. (LÉVY, 1996, p. 27)

Parece indiscutível que os *wearable devices* estão cada dia mais comuns entre usuários e consumidores, estes que usam *smartwatches*, *smart glasses* ou *wearable fitness Trackers*, produtos que há poucos anos não passavam de futurismos, mas que agora, no presente, são uma das certezas de oferta no mercado. Este fenômeno, muito ligado à convergência de tecnologia, ocorre também na convergência de meios, como ligados as roupas, artigos esportivos ou de lazer, e que não parecem poder ser paradas, já que

> a convergência das tecnologias de rádio, dos microprocessadores e dos dispositivos eletrônicos digitais pessoais está levando ao conceito de ubiquidade no qual dispositivos inteligentes, móveis e estacionários, coordenam-se entre si para prover aos usuários acesso imediato e universal a novos serviços, de forma transparente, que visam aumentar as capacidades e habilidades humanas. (ARAÚJO, 2003, p.45)

Porém mesmo sendo cada vez mais presente no cotidiano, não se pode dizer que seu conceito seja algo facilmente disseminado ou reconhecido pelo usuário comum. Como distinguir um *device* comum daquele que foi produzido para se mimetizar aos artefatos cotidianos?

Como forma de responder a esta pergunta, entende-se por *wearables* as novas tecnologias criadas para serem usadas o mais próximo do corpo possível, como se fossem peças de roupas inteligentes ou acessórios, o termo significaria portanto "tecnologias para vestir" (SUMRELL, 2014). Atualmente, e devido ao empenho das empresas de tecnologia em desenvolver novos dispositivos neste formato, a maioria dos *wearables* disponíveis está limitada a relógios inteligentes ou dispositivos esportivos, porém a gama é mais ampla (e útil), inclusive saindo do usuário comum e se adaptando à interesses de empresas e governos.

No que tange à privacidade pessoal, entretanto, esta é uma das maiores preocupações de usuários. O crescimento e aprimoramento destes dispositivos, combinados à vida cada vez mais *online*, trazem riscos de que a identidade e privacidade sejam invadidas por sistemas que, despercebidos, captem informações dadas como sigilosas ou que interfiram nos diferentes níveis de direitos individuais. A segurança, em adição a estes riscos, é outro fator de fácil invasão. A falta de regras e normas sociais que exijam a total transparência e padronização sobre quais dados poderiam ser coletados por tais dispositivos, como seriam usados, e como os usuários poderiam manter o controle sobre sua privacidade ainda são expectativas e passam por discussões diárias nos órgãos reguladores responsáveis. Assim, existe a necessidade de soluções que possam gerar proteção à privacidade, tanto em dispositivos não-vestíveis quanto em *wearables*, para que todos os tipos de dispositivos conectados possuam um controle de privacidade independente do tipo de dispositivo ou de nível de conexão. (SUMRELL, 2014)

Ainda neste sentido, não se pode questionar o avanço de *wearables* apenas no que tange à segurança e privacidade do cidadão comum. Segredos empresariais e a segurança nacional podem ser alvo destes recursos que, ao passarem despercebidos ou se tornando um simples aparelho de uso irrestrito, criam a necessidade de um novo olhar sobre a forma de se precaver ou, até mesmo, coibir seu uso. Em outro tópico, uma vez estes aparatos presentes, devido à facilidade que os mesmos possuem de se conectar à rede, é impossível prever a rapidez que uma informação levaria para chegar a seu destino, senão em tempo real. Assim, e tentando entender o fenômeno, Ark & Selker (1999) identificaram quatro grandes aspectos que, através das novas tecnologias, poderiam afetar pessoas e governos no que se refere à sua segurança e privacidade: a crescente disponibilidade de novos dispositivos de informação; a mobilidade dos usuários; a distribuição da computação pelo ambiente; e a simplificação da comunicação entre indivíduos, entre indivíduos e coisas, e entre coisas.

A introdução e popularização de múltiplos aparatos móveis de informação, como GPS, livros eletrônicos, consoles portáteis para jogos e, especialmente, smartphones, representam a mobilidade do hardware e a facilidade de se estar armado de instrumentos tecnológicos de informação compartilhada entre seus usuários. Araújo (2003), por sua vez, inclui outros pontos importantes, como o fato de as aplicações seguirem os usuários em movimento; a informação pode ser acessada por meio de múltiplos dispositivos heterogêneos, que apresentam visões diferentes da aplicação e interagem entre si; o ambiente e os dispositivos trocarem informações e responderem às mudanças percebidas; e algumas tarefas serem executadas de maneira autônoma, reduzindo ou eliminando a necessidade de intervenção humana.

A tecnologia toma, conforme disposto, força autônoma conforme seus avanços. Mais que um serviço, cada vez mais está inerente ao cotidiano e nos mais diferentes focos, e por isso não causa espanto a criação dos dispositivos móveis cada vez menores ou a tendência de crescimento e disseminação de dispositivos *wearables.* A tecnologia passa a ser tão próxima do usuário que se confunde com quem a usa, faz parte de cada momento, cada interação entre pessoas, e cria, conforme o já mencionado por Galloway (2004), novas oportunidades de rastreio e controle.

Em tempos passados, avanços tecnológicos eram quase sempre pensados para impactarem o processo de guerra. Hoje, particularmente no que tange ao poderio militar, o domínio da tecnologia desenvolveu-se de forma significativa, e os novos modelos tecnológicos fazem com que modernos soldados estejam, por exemplo, transportando e captando informações em veículos aéreos não-tripulados (drones), de forma portátil, sem precisar se infiltrar no território inimigo fisicamente. *Smart watches, smart glasses, health monitoring bracelets*, muito embora hoje sejam *gadgets* comuns, podendo ser comprados em qualquer loja de eletrônicos, podem ser somados às novas inovações de caráter militar, como a pele artificial (*wearable* com sensores, comandos e armas embutidos em um tipo de roupa) e microcomputadores portáteis, estes que já estão sendo discutidos para utilidades militares específicas.

Em artigo publicado em maio de 2015 no Diário do Exército de Libertação do Povo (PLA), uma espécie de informativo específico para militares chineses, a repórter Jiang Yijun Tong Zujing alerta, porém, para os riscos destes dispositivos inteligentes, em especial relógios, monitoramento *fitness* e óculos serem usados pelos militares em ação, uma vez que "no momento em que um soldado coloca um dispositivo que pode gravar áudio e vídeo de alta definição, tirar fotos e processar e transmitir dados, é muito possível para ele ou ela ser rastreada ou revelar segredos militares".

Entretanto, o *Google Glass* já é uma realidade e um dos dispositivos mais falados nos últimos tempos em relação à sua aplicabilidade para as forças

de defesa. Militares modernos estariam assim possuindo, através do *gadget*, dispositivos inteligentes que deixariam suas mãos livres, tendo a capacidade de gravação, transmissão e computação em tempo real. Ainda, espera-se que as tecnologias baseadas na realidade aumentada possam se combinar a este *gadget*, de forma a criar um ambiente muito mais realista e imersivo. E dentre estas várias novas idéias que estão sendo discutidas em relação às tecnologias portáteis militares, os desenvolvimentos em campos como nanotecnologia e biotecnologia ajudam no crescimento do domínio das tecnologias portáteis de guerra.

É um novo tempo de transmissão de informações. E também é o somatório de novas tecnologias e novas formas de se dispor segurança internacional no âmbito das relações internacionais contemporâneas.

A vigilância e a nova fragilidade da segurança internacional.

Não é possível falar de globalização sem fazer referência à internet e a dinâmica por permitir modos novos e mais interativos de se comunicar. O tema proposto de segurança da informação, particularmente a internacional, é tópico constante no âmbito da sociedade globalizada. A segurança internacional, sempre foi objeto da política internacional, da política externa de cada Estado, e suas novas vertentes não passam despercebidas.

O assunto está intimamente relacionado ao estado de vigilância, muito bem teorizado por Giddens (1984), quando ensina que a vigilância seria a codificação de informações importantes para a administração de uma população, mais a direta supervisão desta população por representantes governamentais e empresariais, que hoje se tornariam mecanismos de integração. Assim, um Estado se usa da vigilância para reunir informações sobre determinado país ou população, com intuito de possibilitar o poder de informação e seu controle geral. Para o autor, estas sociedades modernas são, ao fim, sociedades de informação.

> A vigilância é o poder de conhecer sem ser conhecido, de ver sem ser visto. [...] toda vigilância é totalitária, pois não permite que suas vítimas tenham voz na maneira como ela opera, e não devemos permitir que o aspecto benigno geral de seus usos mascare este fato (FISKE, 1996: 46 e 241).

Estas informações, hoje, encontram novos desafios. A transmissão de informações via *gadgets*, *e-mails* e *wearables* não podem ser enfrentadas por um Estado através apenas de sua força militar, método mais comum dos países enfrentarem suas ameaças à segurança. Martins (1998) concorda com este ponto de vista, de que a nova tecnologia introduziu uma mudança qualitativa nas relações internacionais, já que os conflitos entre potências claramente não mais podem ser resolvidos pelo conflito militar. As investidas militares não são capazes

de impedir novos dilemas internacionais, incluídos aqui a ofensiva cibernética e a possibilidade de qualquer cidadão ser o transmissor das informações.

> Certamente, a vigilância hoje é mais descentralizada, menos sujeita a restrições espaciais e temporais (localização, horário do dia, etc.), e menos dirigida do que nunca pelos dualismos entre observador e observado, sujeito e objeto, indivíduo e massa. O sistema de controle é desterritorizalizante (BOGARD, 2006: 102).

Tais assuntos, somados ao crescente medo do terrorismo internacional e o compartilhamento de informações sigilosas são, segundos novos autores de relações internacionais, "novas ameaças" à segurança de países, e estão tomando lugar das "velhas" ameaças. Governos devem, portanto, atentar não apenas aos perigos militares e também se concentrarem em medidas para enfrentar diferentes desafios ao bem-estar de suas nações. (KENNEDY apud VILLA; REIS, 2006)

> Após a Guerra Fria o terrorismo tornou-se mais evidente (perceptível) à Nações, sendo que suas formas operacionais e objetivas também adequaram- se frente à realidade cibernética global. Hoje não são necessários tantos suicidas dogmáticos para concretizar o intento criminoso terrorista, como no quinquênio passado. Os ataques às ciber-redes dos Estados aterrorizados por esses grupos estão cada dia mais comuns e sofisticados, sendo tal fenômeno globalmente conhecido por ciberterror(ismo). O combate ao ciberterror é (talvez) nosso maior desafio enquanto sociedade pré-globalizada. (SILVA JR, 2013)

Não tratando fundamentalmente aqui do terrorismo internacional em si, mas a invasão a dados e seu fácil compartilhamento, propõe-se um exemplo de como este assunto resulta na necessidade de ser analisado.

A entrada em um país sob regime autoritário e, consequentemente, fechado frente ao cenário político internacional, representa o desafio de obter informações e compartilhá-las. A Coréia do Norte, por exemplo, é um destes países. No ano de 2009, duas jornalistas americanas foram presas e condenadas a 12 anos de trabalhos forçados por terem entrado ilegalmente no país e tentado fazer registros em foto e vídeo, sendo necessária a intervenção direta do ex-presidente Bill Clinton para conseguir a libertação de ambas (PIRES, 2013, pág. 69). No ano seguinte, uma equipe de documentaristas para o programa à cabo "Não Conta lá em Casa", do canal brasileiro Multishow, entrou no mesmo território, com vistos de turismo, para obter imagens para o programa, que se fundamenta basicamente em registrar países de difícil acesso e mostrar a realidade existente nos mesmos. Para tal, necessitavam burlar a constante presença de "guias" do governo, que impediam qualquer questionamento sobre a dinâmica política-autoritária do país ou registro de locais ou situações consideradas proibidas. Usando do

"jeitinho brasileiro", os participantes obtiveram regalias e conseguiram, de forma discreta, realizar filmagens e fotografias através de celulares e câmeras nos mais inóspitos lugares do país, como o palácio do governo norte-coreano (PIRES, 2013). Caso nesta época fossem usados alguns dos novos aparatos, como o *google glass*, tais registros seriam mais simples de serem feitos e, automaticamente, de terem as informações compartilhadas, sem nem ao menos chamarem a atenção dos "guias".

Rosenau (1990) indica um ponto importante neste tópico para o cenário das relações internacionais atuais, que ajuda a entender estes fenômenos tecnológicos. Tomando como foco a pós-industrialização, o avanço e o desenvolvimento de tecnologias eletrônicas garante a facilidade de transmissão de registros, além de um rápido movimento de pessoas, produtos e informações pelo mundo desterritorializado (ou global). Em um âmbito mais amplo, caso estes registros fossem direcionados para obter informações referentes ao sistema político do país, ou para obter outros dados de pertinência para um governo, o uso de um *device* como *google glass* ou, futuramente, uma lente de contato inteligente, traria facilidade para todo o processo, afetando diretamente a segurança nacional daquele país. Assim, a entrada em um país como a Coréia do Norte, usando um aparato tecnológico de rápido compartilhamento de informações permitiria que, bastando um comando, registros fossem compartilhados em rede de forma imediata, sem grandes dificuldades e, ainda, burlando a percepção de que o aparato é, em realidade, um *device* tecnológico, não um simples óculos ou lente de correção visual. Seria então, até o presente, a forma mais tecnológica além da mais eficiente de espionagem internacional.

Assim, como evitar esta facilidade de acesso e transmissão de informações no cenário internacional? Existiria possibilidade de se coibir ou criar formas de impedir o uso destes aparatos? Como regular o uso de um *wearable*, ou até mesmo percebê-lo, caso em um futuro próximo o mesmo se aproximasse cada vez mais com uma lente comum?

São questionamentos importantes, para qualquer país interessado por buscar respostas. O avanço é latente, e cada vez mais será difícil se identificar novas tecnologias em um dispositivo móvel ou *wearables*. Ainda que estes aparatos sejam apenas um dos problemas a serem observados, as novas tecnologia são muito mais amplas que apenas tratar aqui de *devices*, e não tardará para existirem outras novas que também adicionem ao tema novas problemáticas a serem tratadas e analisadas de forma a reduzir, coibir, ou até mesmo proibir a transmissão de informações consideradas de segurança por cada país, já que a velocidade das inovações tecnológicas guardam novidades inimagináveis e, assim como seu uso traz benefícios, certos cuidados deverão ser tomados no que se refere à segurança individual e entre países. Para tanto, governos correm

contra o tempo, tentando criar novas regras de segurança, leis e penalidades para crimes cibernéticos. Mas o caminho ainda é longo.

Considerações Finais

A idéia inicial deste estudo não foi chegar em respostas sobre segurança e como solucionar possíveis problemas derivados dos avanços das novas tecnologias. Teve-se como intuito analisá-los e exemplificá-los e, assim, levantar questões sobre os mesmos, quando relacionados com a segurança e o processo de vigilância entre países.

Para a estabilidade da nova ordem internacional e as investidas tecnológicas, inclusive para que sejam criados os pressupostos de uma ordem cosmopolita e moderna (Thompson, 1998), faz-se necessário o tratamento privilegiado das questões referentes a cibercultura e a facilidade de transmissão de informações. O novo papel das tecnologias e sua inserção quase irrestrita em lugares e objetos cotidianos resultarão em diversas mudanças sociais, seja em um simples e-mail ou em um wearable, tendo em vista as diversas possibilidades de serviços e suporte a serem desenvolvidos. Tais fatores, porém, encontrarão resistência com as inúmeras questões que pairam sobre estas tecnologias. O cenário necessita de fortes pesquisas e acordos envolvendo diversos setores, especialmente em áreas da computação e governamental, porém é fulcral que estes estudos tenham como enfoque, especialmente, no que isto implicaria no âmbito social, econômico e ético de uma sociedade que, cada vez mais, se encontra conectada e dependente das mesmas tecnologias que afrontam o cenário internacional.

REFERÊNCIAS BIBLIOGRÁFICAS

ARAÚJO, R.B. de. **Computação ubíqua:** princípios, tecnologias e desafios. In: Anais de

XXI Simpósio Brasileiro de Redes de Computadores. 2003. pp. 45-115. Disponível em: <https://im.ufba.br/pub/MAT570FG/LivroseArtigos/045_AraujoRB.pdf.>. Acessado em 02/07/2014.

ARK, W. S. & SELKER, T. ***A look at human interaction with pervasive computers***. In: IBM Systems Journal, Vol.38, No.4, 1999, pp.504-507.

BLACK Mirror. ***Toda a sua história.*** Direção: Brian Welsh. 2011.

BOGARD, William. ***Surveillance assemblage and lines of flight***. In: *Theorizing surveillance*, Ed. David Lyon, 97-122. Portland: Willan, 2006.

DELEUZE, Gilles. **Post-scriptum sobre as sociedades de controle.** In: Deleuze, Gilles. Conversações. São Paulo: Editora 34. p.223-230. 1992.

DOMINGOS, J. A.; COUTO, S. P. **WikiLeaks**: Segredos, Informações e Poder. Bauru: Editora Idea, 2011.

FISKE, John. **Media matters**. Minneapolis: University of Minnesota Press, 1996.

GALLOWAY, Alexander. **Protocol**: how control exists after decentralization. Cambridge: MIT Press. 2004.

GIDDENS, Anthony. ***The constitution of society:*** *outline of the theory of structuration*. Cambridge: Polity Press, 1984.

G1. **Samsung registra lente de contato 'smart' com câmera ativada a piscadas.** Abr. 2016. Disponível em: <http://g1.globo.com/tecnologia/noticia/2016/04/samsung-registra-lente-de-contato-smart-com-camera-ativada-piscadas.html>. Acesso: em 17 de ago. 2017.

LÉVY, Pierre. **Cibercultura**. (Trad. Carlos Irineu da Costa). São Paulo: Editora 34, 2009.

_____. **O que é o virtual?**. São Paulo: Editora 34, 1996.

MARTINS, Luciano. **A condição de "país emergente" no contexto das transformações globais.** In: X Fórum Nacional, Rio de Janeiro, 11 de maio de 1998. MATHEWS, Jessica.

Segurança internacional redefinida. Diálogo, Vol. XIII, n. 2, 1993, p. 3.

OLHAR DIGITAL. **Conheça a lente de contato inteligente do Google.** Jul. 2014. Disponível em: <https://olhardigital.com.br/noticia/conheca-a-lente-de-contato-inteligente-do-google/43069>. Acesso em: 19 ago. 2017.

OLIVEIRA, D. S. G. **O Poder da Informação na Política Internacional:** A WikiLeaks e a Revolução na Tunísia [dissertação]. Lisboa, 2012.

PIRES, André Fran. **Não conta lá em casa:** uma viagem pelos destinos mais polêmicos do mundo. Rio de Janeiro: Record, 2013.

ROSENAU, James N. ***Turbulence in worlds politics***. Princeton: Princeton university press, 1990.

SHAH. Aaushi,. RAVI. Srinidhi,. ***A to Z of Cyber Crime***. Asian School of Cyber Laws. 2013. Livro disponível em: <http://ensaiosjuridicos.files.wordpress.com/2013/06/122592201- cybercrime.pdf>. Acessado em 12/06/2014.

SILVA JR, Nelmon J. **Espionagem & Filosofia**. Disponível em: <http://www.egov.ufsc.br/portal/sites/default/files/espionagem_filosofia_silva_jr.pdf>. Acessado em 12/06/2014.

. **Ciber terror e ciber guerra.** disponível em:<http://ensaiosjuridicos.wordpress.com/2013/06/25/ciber-terror-ciber-guerra-nelmon-j-silva-jr/>. Acesso em 09.07.2014.

SUMRELL, Mariano. **Os *wearables* são a evolução da tecnologia móvel**. Disponível em: <http://canaltech.com.br/coluna/mobile/Os-Wearables-sao-a-evolucao-da-tecnologia-movel/>. Acessado em 12/06/2014.

THOMPSON, Janna. ***Community Identity and world citizenship***. In: *Archibugi.* HELD E KOHLER. CIT, 1998.

VILLA, Rafael Duarte; REIS, Rossana Rocha. **A segurança Internacional no pós-guerra fria:** um balanço da teoria tradicional e das novas agendas de pesquisa. In: Revista Brasileira de Informações Bibliográficas em Ciências Sociais, n. 62, São Paulo, 2. Sem./2006, pp. 19-51.

ZUJING, Jiang. **Evitar o vazamento do "equipamento de desgaste inteligente.** Disponível em: <http://www.81.cn/jfjbmap/content/2015-05/10/content_110417.htm>. Acessado em 12/08/2017.

Recebido em março de 2017.
Aprovado em abril de 2017.