OS DESAFIOS E OPORTUNIDADES PARA A CONTRAINTELIGÊNCIA NA ERA DO CONHECIMENTO

Marcelo **Neival** Hillesheim de Assumpção[1]
Gustavo Monteiro **Muniz** Costa[2]

Ocorrências significativas na História Geral delimitaram os cinco períodos nos quais a história da humanidade é dividida, a saber: Pré-História, Idade Antiga, Idade Média, Idade Moderna e Idade Contemporânea. Tais períodos, classificados para fins didáticos e por convenção, revelam panoramas da existência humana com características próprias e com foco principal na perspectiva de intelectuais europeus.

O período em que vivemos, a Idade Contemporânea, iniciou-se em 1789, ano da Revolução Francesa, e estende-se até a atualidade. Este período, em particular, revela uma fase tão significativa de mudanças e evoluções na humanidade que já poderia ter sofrido nova divisão e categorização.

A delimitação de tais períodos é algo relativamente recente, surgido somente após a Idade Média. É possível que, face às profundas mudanças geopolíticas, sociais e comportamentais ocorridas nos últimos anos, historiadores e especialistas, daqui a alguns anos, estabeleçam o fim da Era Contemporânea e definam que atualmente vivemos sob a Era do Conhecimento.

O marco que separará essas Eras caberá aos futuros estudiosos, podendo definir a Queda do Muro de Berlim, o fim da União Soviética, ou mesmo o ataque às Torres Gêmeas, como a data limítrofe, face às profundas e irreversíveis mudanças ocorridas na geopolítica mundial devido a estes acontecimentos.

As alterações nos relacionamentos entre os entes privados e estatais no mundo, devido ao uso da rede mundial de computadores (*internet)*, e aos meios de tecnologia da informação (MTI), causaram uma mudança comportamental na humanidade capaz de influenciar o futuro das nações, bem como determinar o resultado de eleições, como ocorreu recentemente nos Estados Unidos da América com a eleição de Donald Trump.

O exemplo da recente eleição presidencial norte-americana demonstrou que o presidente eleito e sua adversária, Hillary Clinton, utilizaram em larga escala meios de comunicação atrelados à *internet* para sua campanha. No entanto, da mesma forma, foram vítimas desses.

Hillary foi acusada e investigada pelo *Federal Bureau Investigation* (FBI), a polícia federal norte-americana, por comprometer a segurança do país ao usar e-mails particulares, para enviar mensagens oficiais enquanto ocupava o cargo de Secretária de Estado de Barack Obama. Partidários de ambos postavam, incessantemente, em redes sociais fotos e notícias distorcidas ridicularizando, ofendendo ou mesmo manipulando informações contra os adversários. Já sobre Trump, pairam acusações de ter sido beneficiado por ações de *hackers* russos

1 Oficial de Infantaria do Exército Brasileiro, Academia Militar das Agulhas Negras, Pós graduado em Ciências Militares, Escola de Comando e Estado-Maior do Exército - mnha31@yahoo.com.br
2 Oficial de Cavalaria do Exército Brasileiro, Academia Militar das Agulhas Negras, Pós graduado em Ciências Militares, Escola de Comando e Estado-Maior do Exército - gustavommuniz@gmail.com

que o teriam favorecido na disputa do pleito, algo que, mesmo que se comprove ser inverídico, permanecerá desgastando a figura do presidente eleito (GUILHERME, 2016).

As vulnerabilidades surgidas com a Era do Conhecimento ficaram muito bem evidenciadas com os milhares de documentos confidenciais norte-americanos vazados num sítio na *internet*. Edward Snowden, ajudado por um ex-militar, Bradley Manning, entregou milhares de documentos diplomáticos e confidenciais a Julian Assange, fundador da organização chamada *Wikileaks*, que os divulgou seletivamente na *internet*. Comprovações de grampos telefônicos contra inúmeros líderes mundiais a até, recentemente, acusações de que a *Central Intelligence Agency* (CIA) é capaz de monitorar os telefones de qualquer cidadão no mundo, demonstraram que nem mesmo a maior potência global é capaz de possuir sistemas de segurança orgânica que impeçam o vazamento de informações e comprometam os seus ativos (BATISTA, 2017).

Por outro lado, foram justamente os meios de tecnologia da informação empregados no contraterrorismo, atividade da segurança ativa da Contrainteligência, que identificaram e localizaram o terrorista mais procurado do mundo, Osama Bin Laden. Após um dos membros da Al-Qaeda ter dito breves palavras suspeitas, por poucos segundos, usando um celular descartável e num local remoto do Paquistão, é que foi possível iniciar o processo de localização daquele líder terrorista (OWEN, 2012).

O fato é que a revolução tecnológica iniciada há algumas décadas, aliada à propagação em escala global das informações e dos "saberes", já gerou um consenso mundial em chamar o período em que vivemos de Era do Conhecimento. Como dificilmente se conseguirá, em um mundo globalizado, consenso no meio acadêmico acerca do fato histórico que marca o início deste período, é bem provável que continuemos "situados" na Idade Contemporânea por um bom tempo.

Independentemente da denominação histórica e acadêmica que se queira atribuir a este período em que vivemos, é preciso reconhecer que a atividade de Inteligência Militar, tanto no ramo da Inteligência quanto no ramo da Contrainteligência, tem passado por constantes desafios frente ao mundo da Era do Conhecimento. Desafios estes que têm colocado à prova justamente a atividade cujo fulcro é a gestão do conhecimento, além da proteção do mesmo**.**

Definiu-se como objetivo geral dessa pesquisa analisar o que é a Era do Conhecimento, quais suas características principais e como elas afetam à atividade de Contrainteligência. A partir de então, traçou-se objetivos específicos que eram a identificação dos desafios, impactos, oportunidades dessa Era e, se possível, realizar a integração dos conhecimentos obtidos, apresentando, como contribuição, as premissas direcionadoras para esse ramo da Contrainteligência.

Dessa forma, realizou-se uma pesquisa de abordagem qualitativa, exploratória quanto aos objetivos e utilizando-se de procedimentos bibliográficos, apoiado em literaturas atuais, fatos recentes e análises de especialistas acerca de um tema pouco estudado e consolidado. Os conhecimentos obtidos nas diversas fontes consultadas foram então integrados às experiências profissionais dos pesquisadores do presente estudo, resultando em um trabalho que reflete a importância atribuída ao desempenho da atividade de Contrainteligência, em um mundo no qual a proteção das informações parece se tornar a cada dia mais difícil.

Diante deste cenário, o tema apresentado, Os Desafios e Oportunidades para a Contrainteligência na Era do Conhecimento, foi dividido em cinco capítulos, com a introdução, conclusão e mais três

capítulos inerentes ao desenvolvimento. No capítulo dois, o leitor será apresentado a algumas das características principais da Era do Conhecimento. No terceiro capítulo estão identificados alguns dos impactos e desafios dessa Era. Já o capítulo quatro integra os conhecimentos apresentados anteriormente, sugerindo quatro premissas gerais e direcionadores para a Contrainteligência e elencando algumas das novas oportunidades a esse ramo da Inteligência. Por fim, a conclusão mostra as limitações desse trabalho e as necessidades de novos estudos sobre o tema.

1. AS CARACTERÍSTICAS DA ERA DO CONHECIMENTO

Dentre as 100 maiores invenções da humanidade elencadas no livro homônimo (PHILBIN, 2015), mais de 60% delas foram criadas entre o final da segunda metade do século XIX e o início da segunda metade do século XX. O Museu de Ciência de Londres elegeu em 2009 as 10 maiores invenções da humanidade, dentre as quais todas ocorreram nesse mesmo período, com exceção do telégrafo e da máquina a vapor (BBC, 2009). Antes de 1970, o homem já havia criado a televisão, o satélite, o telefone, o rádio, o avião, a bomba atômica, a energia nuclear, a penicilina, o cloro, o computador e a Arpanet, predecessora da internet. Daí em diante, a tecnologia aprimorou as criações já existentes, como os carros autônomos, o ônibus espacial, submarinos de propulsão nuclear, os celulares, os computadores portáteis, os smartphones e a própria internet.

A corrida armamentista ocorrida no período da Guerra Fria entre os Estados Unidos da América (EUA) e a ex-União das Repúblicas Socialistas Soviéticas (URSS) impulsionou o desenvolvimento científico-tecnológico mundial a partir do investimento de governos e empresas por eles contratadas, com destaque para a corrida aeroespacial e o Programa Guerra nas Estrelas do governo de Ronald Reagan nos EUA (LOBO, 2015). No entanto, foi o acesso da população à tecnologia dos telefones portáteis, bem como o uso da internet por pessoas comuns para a troca de e-mails, pesquisas, transações financeiras e demais utilidades, até então limitadas pela baixa capacidade de transmissão de dados, que resultaram nas mudanças mais significativas de nossa Era.

Os principais meios de comunicação hoje são os meios de tecnologia da informação (MTI), conectados à *internet* e, muitas vezes, integrados em uma rede social *online*, as quais permitem que a ligação entre usuários e telespectadores ocorra sem o intermédio dos grupos de mídia. Seja por meio de aplicativos ou programas criados para interação entre usuários, como *Instagram*, *Twitter*, *Whatsapp*, *Telegram* e *Facebook,* seja por sítios da *web* disponíveis para postagens de vídeos, opiniões, artigos, imagens e qualquer outra forma de comunicação por pessoas comuns, como *Youtube*, *blogs* e *Daily Motion*. Praticamente, não existe mais sociedade alheia ou que não esteja sob as influências da Era do Conhecimento.

O resultado dessa mudança foi a transformação da sociedade de um estado simples, controlável, previsível, lento, estável e baseado em instituições sólidas para um ambiente complexo, fora de controle, imprevisível, rápido, instável e pautado sobre o indivíduo, capaz de mudar rumos inteiros de nações por meio de um ato único, isolado e independente (GUIMARÃES, 2016).

Esse dinamismo e rapidez com que as informações são transmitidas entre uma fonte e milhões de destinatários possibilitaram que notícias, propagandas, difamações e quaisquer outras formas de informações possam trafegar por intermédio dos meios de comunicação sem nenhum filtro ou confirmação prévia, causando efeitos que muitas vezes não podem ser mitigados ou solucionados oportunamente.

O dicionário Oxford elegeu o termo "pós-verdade" como a palavra do ano de 2016, definindo-o como "um adjetivo que se relaciona ou denota circunstâncias nas quais fatos objetivos têm menos influência em moldar a opinião pública do que apelos à emoção e às crenças pessoais." (OXFORD, 2016).

Esse neologismo denota a importância em bem se compreender e estar preparado para os desafios da Era do Conhecimento, onde a verdade pode facilmente ser substituída por distorções e mentiras que serão capazes de moldar, alterar ou mesmo influenciar comportamentos com uma velocidade inédita, principalmente aquelas feitas sob o prisma das Operações Psicológicas.

Nas eleições presidenciais brasileiras em 2014 diversos boatos, mentiras e inverdades circularam nas redes sociais, fora do alcance da fiscalização do Tribunal Superior Eleitoral (TSE) e sempre à frente da capacidade de reação dos alvos elencados. Porém, muitas dessas "pós-verdades" não eram realizadas por pessoas comuns, mas sim por especialistas em propaganda política detentores de conhecimento e ferramentas afins às aquelas utilizadas nas Operações Psicológicas.

No entanto, constatou-se que, comparando-se com as eleições presidenciais norte-americanas em 2016, o ocorrido no Brasil dois anos antes era apenas uma fase embrionária desse processo de difamação, manipulação de opiniões, disseminação do medo e controle das massas. Ambos os principais candidatos àquela eleição, Donald Trump e Hillary Clinton, utilizaram-se largamente de um meio gratuito, incontrolável, disseminador e, muitas vezes anônimo, para atacar seu adversário: as redes sociais *online*.

Outro fato contundente da Era do Conhecimento é a ligação direta entre a notícia e o usuário, sem necessariamente haver um órgão de imprensa interligando essas duas pontas. Enquanto, há pouco tempo atrás, era absolutamente necessário um fotógrafo, um jornalista, uma câmera ou os próprios meios de imprensa para divulgar uma notícia, como jornais impressos, locutores de rádio ou um cinegrafista, atualmente, a vítima de um bombardeio na Síria consegue transmitir, em tempo real, suas agruras a milhões de expectadores, uma refugiada afegã consegue prestar seu depoimento pessoal e sem censura em uma rede social virtual que será lida por pessoas nos cinco continentes.

Ao mesmo tempo, transações financeiras bilionárias ocorrem entre hemisférios sem que os envolvidos sequer se vejam. Forças Armadas em todo o mundo desenvolvem e aperfeiçoam suas defesas cibernéticas e, principalmente, suas capacidades de realizarem ataques nessa nova dimensão do combate.

Hoje, um bombardeio aéreo sobre uma usina elétrica pode ser substituído por invasões à rede que distribui a energia aos usuários, economizando meios, vidas e ainda assim atingindo os mesmos fins militares definidos pelo atacante.

Porém, um fato peculiar ao período de transição entre as Eras está ocorrendo: grande parte dos líderes e pessoas com poder de decisão, seja na esfera governamental, civil ou militar, possui mais de quarenta anos de idade. Assim, são pessoas que, em sua maioria, tiveram suas formações acadêmicas ocorridas ainda sob as características da Era Contemporânea, quando havia maior previsibilidade e controle das informações. Já os mais jovens, que estão familiarizados com as novas tecnologias desde a infância, não possuem a maturidade e experiência profissional para adequar o uso dessas novas capacidades às realidades comportamentais da humanidade.

Exemplo dessa imaturidade dos jovens é o grande número de comprometimento de informações e exposições indevidas a que eles mesmos se submetem, variando desde divulgações de conteúdo íntimo privado até ao vazamento de informações sigilosas de governos. Esses atos comprometem

desde a própria honra e dignidade pessoal, com reflexos que podem perdurar a vida inteira para a família, podem colocar em risco a segurança nacional, quando movidos por idealismos temporais e sem reflexão das consequências (como o grupo *Anonymus,* especializado em atacar governos).

Quanto à falta de adaptação dos decisores sobre as atuais ferramentas da Era do Conhecimento, por exemplo, é fato que mensagens trocadas em grupos de *Whatsapp* chegam aos chefes nos diversos escalões sem o prévio filtro e análise dos órgãos assessores. Essas informações não trabalhadas e sem uma adequada técnica de análise prévia acabam por influenciar decisões.

Durante as Olimpíadas do Rio de Janeiro em 2016, inúmeras denúncias anônimas espalhavam-se em grupos daquele aplicativo em uma progressão geométrica, anunciando mochilas suspeitas e ou outras formas de ameaças à população, todas infundadas, mas que nos primeiros dias resultaram no acionamento de equipes diversas, para checar os locais *in loco*, antes mesmo da análise dos dados difundidos. Obviamente, diante da incapacidade de cobrir as inúmeras denúncias com as equipes de operações, constatou-se que as informações difundidas em grupos de rede social deveriam, antes de qualquer coisa, ser previamente analisadas para uma posterior tomada de decisão dos chefes.

A grande maioria dos países no mundo sequer possuem leis adaptadas às dificuldades e peculiaridades dessa Era. Crimes cibernéticos, ofensas trocadas por meio de redes sociais, vazamento de conteúdos pessoais, propagação de mentiras e difamações, clonagem de dados financeiros ou comprometimento de investigações policiais e processos judiciais ainda não recebem o tratamento civil e criminal específico que merecem, sendo enquadrados em tipificações penais mais genéricas, seja pela incapacidade dos órgãos investigativos atenderem à infinita e crescente demanda dessa sorte, seja pelo próprio vácuo legal existente.

Portanto, entender a Era do Conhecimento, esse "ser vivo" altamente mutável e incontrolável, buscar compreender suas características, desafios, ameaças e, ao mesmo tempo, identificar as oportunidades que ora se apresentam é uma obrigação de todos aqueles que têm a responsabilidade de liderar e conduzir suas instituições.

2. OS IMPACTOS E OS DESAFIOS QUE A ERA DO CONHECIMENTO TRAZ À CONTRAINTELIGÊNCIA

Diante do que foi abordado até este ponto no presente estudo, já é possível perceber que a Era do Conhecimento enseja desafios imensuráveis para todas as atividades humanas, em particular, para as ligadas à segurança das instituições e à proteção do conhecimento. Fica a indagação: como resguardar as instituições e proteger a informação em um contexto global em que a transparência e a instantaneidade na transmissão de dados parecem ser as palavras de ordem e encontram um ambiente virtual totalmente voltado para isso? Como tal contexto tem refletido na atividade de Contrainteligência?

Nos últimos anos foi recorrente o caso de terroristas e combatentes de países invadidos por exércitos estrangeiros postarem vídeos em *sites*, com o fito de realizar Operações Psicológicas contra os países invasores.

Durante a campanha dos EUA no Iraque (2003 a 2011), um *sniper,* que foi apelidado de Juba, deixou dezenas de soldados estadunidenses mortos ou feridos após disparos precisos que eram filmados por outro insurgente que, logo após, postava os vídeos destas ações na *internet* utilizando, principalmente, o site *Youtube* (CARROLL, 2005).

Tais vídeos tiveram um alcance mundial, influenciando a opinião pública dos EUA e do

mundo, em prol do fim da guerra. Além disso, abalou o moral das tropas norte-americanas, de uma forma que a Contrainteligência daquele país, com suas Contra-Ações Psicológicas, não puderam evitar (CARROLL, 2005).

Da mesma forma, os vídeos postados na internet pelo grupo terrorista Estado Islâmico do Iraque e do Levante (ISIS) mostrando decapitações de soldados e de jornalistas de várias nacionalidades nos últimos anos têm causado grande comoção junto à opinião pública mundial, propagando sua causa, causando terror em seus inimigos e levando empresas como *Facebook* e *Twitter* a reverem seus procedimentos de controle sobre o conteúdo publicado em seus sites (ALMEIDA, 2015).

Para complicar ainda mais a situação, apoiadores do ISIS criaram o *Khelafabook,* mídia social com uma interface muito semelhante à do Facebook e disponível em vários idiomas, inclusive em português, e que tem tido um alcance global, haja vista o número de curtidas em suas publicações (ALMEIDA, 2015).

A internet vem sendo usada como o principal vetor para o recrutamento de novos terroristas para o ISIS, que tem sido bem sucedido em angariar simpatizantes de todas as idades, nacionalidades e gêneros ao redor do mundo, com seus vídeos caracterizados por uma produção visual impactante e com grande apelo emocional, dignos de grandes produtores midiáticos.

Segundo Costa (2016, p. 2):

> Hoje, a atuação do Estado Islâmico passa por práticas como os twitter bombs (militantes utilizam as hashtags mais populares do Twitter nas postagens relacionadas ao EI, aumentando a visibilidade de seus conteúdos) e chega aos vídeos criados por seu braço midiático, estruturado em torno de dezenas de produtoras audiovisuais coordenadas principalmente pela Al Hayat Media Center, divisão de mídia responsável pela marcação da temática, estética, duração e cronograma de distribuição dessas produções.

Tais recursos tecnológicos têm colocado à disposição de grupos terroristas ferramentas de propaganda, recrutamento e Operações Psicológicas que dispensam o emprego de recursos vultosos e não expõe a grandes riscos os homens que desempenham tais tarefas, além de dificultar sobremaneira as medidas de Contraterrorismo e Contra-Ações Psicológicas.

A propaganda de guerra realizada por intermédio de panfletos jogados de aeronaves em territórios inimigos e que custaram a vida de muitos pilotos parece ter ficado em um passado longínquo na história da humanidade. A propaganda na Era do Conhecimento pode ser feita de um café na cidade de Paris ou de uma *lanhouse* na periferia de um país asiático.

Ainda com relação à propaganda terrorista por meio da internet, Woloszyn (2013, p. 118) pontua que:

> [...] a própria Al Qaeda já se manifestava, em 2003, depois da invasão do Iraque: "Recomendamos urgentemente que qualquer muçulmano ou outros profissionais disseminem notícias e informações sobre a Jihad por meio de listas de e-mails, grupos de discussão e em seus próprios sites na internet para difundir nossa causa e desencorajar infiéis para a luta contra nossos irmãos."

A internet tem sido utilizada também para habilitar pessoas interessadas em empreender atentados terroristas, instruindo-as na fabricação de bombas, execução de sequestros, destruição de prédios, utilização de armamentos, falsificação de documentos, dentre outros ilícitos. Na atualidade, existem cerca de 6 mil sites ligados a grupos terroristas internacionais que cumprem este papel (WOLOSZYN, 2013).

A dimensão virtual ensejou o surgimento dos "profissionais do ciberespaço", os chamados *hackers*. Tais pessoas se valem de grande conhecimento cibernético e, na maioria dos casos, do anonimato, para realizar toda sorte de ações,

algumas nefastas e ilegais, no ambiente das redes. Com relação ao ciberespaço, Filho (2014, p. 54) cita que:

> [...] é dominado por diferentes agentes (hackers, Insiders etc), com ou sem patrocínio estatal, possuidores de notáveis conhecimentos técnicos, e engajados em diferentes atividades, tais como: espionagem industrial, propaganda, vigilância, censura e sabotagem.

A atuação dos hackers há alguns anos deixou de ser exclusivamente empreendida com fins privados e passou a ser conduzida por nações com finalidades diversas, desde ações de espionagem e de sabotagem, até ataques diretos que passaram a ser qualificados como ataques cibernéticos, a mais nova forma de agressão a ser explorada na disputa entre entes estatais (CLARKE, 2015).

Para exemplificar, podemos citar o caso Guerra do Golfo (1990 a 1991), onde os EUA empregaram um vírus com a finalidade de inutilizar a defesa antiaérea do Iraque. Outro caso, foi o ataque realizado pela Rússia contra a Estônia, em 2007, com a finalidade de causar o caos no país, paralisando bancos, empresas, repartições publicas e provedores de internet (FILHO, 2014).

Neste contexto, Woloszyn (2013, p. 111) destaca:

> Podemos afirmar que estamos diante de nova forma de guerra assimétrica, sem exércitos, tanques e aviões, mas com igual letalidade, na qual hackers e crackers, solitários ou a serviço de estados, exercem, ao mesmo tempo, a função de general e soldado e se utilizam de características especiais oportunizadas por tais tecnologias, como rapidez, instantaneidade na difusão de vírus ou informações, abrangência, invisibilidade, baixo custo, difícil detecção e falta de regulamentação na maioria dos países e organismos internacionais, incluindo a ONU.

Outro fenômeno típico de nossa Era e que desafia frontalmente os prognósticos dos analistas de Inteligência comprometendo a estabilidade das nações e suas instituições, tendo em vista a tempestividade com que ocorre e as suas dimensões, é a mobilização das massas em prol de uma causa, por intermédio das redes sociais. Um exemplo disso foi a Primavera Árabe, uma escalada de revoltas populares em países do mundo árabe que desestabilizou a região, no ano de 2011. O movimento teve início na Tunísia e rapidamente se alastrou por outras nações, depondo os representantes da "velha ordem", ditadores que mantinham seus regimes mediante opressão, mas que de certa forma, traziam estabilidade à região e possuíam uma política externa com certo grau de previsibilidade (CANEPA, 2012).

As massas, coordenadas e motivadas a partir do ambiente cibernético, superaram o medo de se manifestar, em países cuja cultura política oprime as manifestações populares, em particular, de caráter reivindicatório, e foram capazes de derrubar governos e mudar o rumo de suas nações. Castells (2013, p. 7) define:

> Da segurança do ciberespaço, pessoas de todas as idades e condições passaram a ocupar o espaço público, num encontro às cegas entre si e com o destino que desejavam forjar, ao reivindicar seu direito de fazer história – sua história –, numa manifestação da autoconsciência que sempre caracterizou os grandes movimentos sociais.

As manifestações populares mobilizadas pelas redes sociais também encontraram palco no Brasil, no ano de 2013, quando milhões de pessoas em várias cidades do país realizaram protestos, inicialmente, contra o aumento no preço das passagens e, em um segundo momento, por uma grande variedade de temas como os gastos públicos em eventos esportivos internacionais, a má qualidade dos serviços públicos e contra a corrupção política.

As dimensões destas manifestações e o caráter violento de algumas delas pegaram autoridades, órgãos de segurança pública, analistas políticos e os serviços de Inteligência totalmente desprevenidos, impedindo a tomada das ações adequadas com a antecipação necessária.

Outro fenômeno de massas que teve origem no ambiente das redes sociais é o que ficou conhecido como "Pós verdade", já citado no capítulo anterior. Este fenômeno certamente não é novo, entretanto, ao ocorrer no âmbito das mídias sociais, tomou uma dimensão muito maior. Ainda mais em um ambiente onde a profusão de informações em um ritmo acelerado oferece poucas condições das pessoas exercitarem seu pensamento crítico em prol de um juízo mais apropriado acerca de algum assunto. Desta forma, qualquer informação com conteúdo negativo acerca de uma instituição macula sua imagem com enorme repercussão, ainda que não expresse a verdade e seja posteriormente rebatida.

Trazendo mais complexidade ainda ao cenário de incertezas da Era do Conhecimento, observa-se que não somente a efetividade da Segurança Ativa tem sido desafiada. As falhas na Segurança Orgânica também têm, por vezes, tomado um vulto de dimensões globais. Foi o caso das fotos postadas por soldados norte-americanos onde os militares aparecem torturando presos iraquianos na prisão de *Abu Ghraib*, no Iraque, demonstrando uma grave falha dos Recursos Humanos estadunidenses no desempenho de suas funções. Tais imagens comprometeram seriamente a imagem do Exército dos EUA e reforçaram o discurso contra a campanha militar e sua legitimidade (HERSH, 2005).

A postagem de fotos, imagens e gravações de áudio tem sido recorrentes nos últimos anos e tem servido tanto para denunciar esquemas de fraude, crimes e corrupções como para comprometer a imagem de instituições sérias e que são alicerçadas na credibilidade depositada nelas pela sociedade como, por exemplo, as Forças Armadas. Tais fenômenos evidenciam a já citada quebra do monopólio da cobertura jornalística.

Em suma, diante do que foi apresentado até o momento, percebe-se que a Era do Conhecimento trouxe uma evolução tecnológica sem precedentes para a humanidade, proporcionando rapidez no tráfego das informações e conectando as pessoas entre si como nunca antes visto. Entretanto, a proteção do conhecimento e das instituições não acompanhou tal evolução, de tal forma que a eficiência da Contrainteligência encontra-se ameaçada, o que enseja uma revisão de suas técnicas, táticas e procedimentos.

3. OPORTUNIDADES PARA A CONTRAINTELIGÊNCIA NA ERA DO CONHECIMENTO E AS QUATRO PREMISSAS GERAIS E DIRECIONADORAS

Apesar dos inúmeros desafios e impactos que essa nova Era trouxe à proteção da informação e ao trabalho da Contrainteligência, é fundamental identificar as oportunidades inerentes. O ser humano normalmente entende como uma ameaça aquilo que é novo e incompreensível. Porém, foram as ferramentas criadas nesse período que têm sido utilizadas como as principais armas no combate ao terrorismo, uma das maiores ameaças mundiais dos dias de hoje.

Muito embora a Era do Conhecimento tenha facilitado a cooptação, recrutamento e preparação dos terroristas, esse advento facilitou as atividades meio e intermediárias. Ou seja, enquanto um grupo criminoso especializado em roubar contas bancárias pela internet não precisa se expor pessoalmente, um terrorista não conseguirá empreender um ataque utilizando unicamente os MTI e a internet. No máximo poderá usar equipamentos adaptados como drones ou celulares para acionamentos remotos. Mas, em todos os casos, ele será obrigado a cruzar alfândegas, manipular explosivos, adquirir armas, expor-se pessoalmente diante dos alvos que elencou ou mesmo recorrer à internet para preparar-se para o ato, facilitando seu monitoramento.

Existe ainda o conceito de ciberterrorismo. Recentemente, o Brasil definiu o conceito de terrorismo, conforme tipificado no artigo 2º da Lei

número 13.260, de 16 de março de 2016 (BRASIL, 2016, p. 1):

> O terrorismo consiste na prática por um ou mais indivíduos dos atos previstos neste artigo, por razões de xenofobia, discriminação ou preconceito de raça, cor, etnia e religião, quando cometidos com a finalidade de provocar terror social ou generalizado, expondo a perigo pessoa, patrimônio, a paz pública ou a incolumidade pública.

Até os dias de hoje, não foi comprovada nenhuma ação cibernética que tenha resultado no terror social ou generalizado. Todas as ações empreendidas até o presente se enquadram como cibersabotagem ou ciberativismo, neologismos que definem ações deliberadas que resultaram em prejuízos financeiros, interrupções de serviços públicos ou simples divulgação de material propagandístico de grupos anarquistas.

Após o atentado às Torres Gêmeas em Nova Iorque, em 11 de setembro de 2001, o governo norte-americano criou a Comissão Nacional sobre Ataque aos Estados Unidos, também conhecida como Comissão do 11 de Setembro. O relatório final dessa comissão identificou falhas na Contrainteligência da CIA e do FBI, resultando numa revisão da estrutura de Inteligência e na criação do cargo de Diretor Nacional de Inteligência, que coordena e integra o trabalho de dezessete agências de Inteligência daquele país e se reporta diretamente ao presidente (WASHINGTON POST, 2010).

A sinergia do trabalho das agências norte-americanas, mas, principalmente, o uso das novas tecnologias para monitoramento, identificação e eliminação das ameaças resultaram que o país maior alvo do terrorismo mundial, com uma população de mais de trezentos milhões de habitantes e com mais de onze milhões de imigrantes ilegais, que comprova a permeabilidade de suas fronteiras, foi alvo de somente um atentado terrorista vultoso em seu solo desde o ataque às Torres Gêmeas.

Em 2013, dois jovens chechenos residentes nos EUA detonaram duas bombas na maratona de Boston, matando três pessoas e ferindo mais de duzentas. Em menos de 72 horas, um dos autores já havia sido morto e o outro capturado. Os demais ataques foram pontuais e não envolveram emprego de explosivos ou produtos químicos e biológicos, somente armas de fogo, semelhantes a outros crimes perpetrados por atiradores nos EUA, com motivações diferentes do terrorismo.

Em 2015, um casal que jurou fidelidade ao Estado Islâmico (EI) atacou funcionários de saúde em San Bernardino, na Califórnia. No mesmo ano, um americano de ascendência afegã matou dezenas de pessoas em uma boate gay em Orlando, na Flórida. Nesse caso, a polícia não conseguiu confirmar se a motivação era terrorista ou problemas psicológicos, pois suspeitou-se que o atirador era gay e tinha medo de assumir sua condição (FOLHA, 2015).

Neste contexto, todos os ataques terroristas cometidos nos EUA foram empreendidos por americanos ou estrangeiros residentes no país, sendo somente no da maratona de Boston onde houve o uso de explosivo improvisado, confirmando a eficiência das novas tecnologias no controle de suas fronteiras e no monitoramento dos materiais e insumos que podem ser utilizados na fabricação de explosivos e produtos químicos ou biológicos com fins terroristas.

Nesse mesmo período, o governo norte-americano destituiu o Taleban do poder no Afeganistão, desarticulou a Al Qaeda, eliminou inúmeros líderes terroristas, inclusive Osama Bin Laden, e mantém um monitoramento constante das ameaças terroristas no mundo, como se exemplifica com os ataques aéreos de mísseis contra líderes e posições do Estado Islâmico no Oriente Médio.

Já na Europa, onde está a maioria dos países mais ricos do mundo e que, consequentemente, possuem os recursos necessários à aquisição, desenvolvimento e emprego das novas tecnologias, também se verifica a vantagem das

medidas contraterroristas sobre as ameaças. As vulnerabilidades européias são imensamente maiores que as norte-americanas, graças à permeabilidade de suas fronteiras, à proximidade geográfica de "países-refúgios" de terroristas e à sua própria configuração populacional com milhões de muçulmanos, o que facilita o homizio dos radicais islâmicos. No entanto, muito embora um ataque na Europa tenha um grande impacto midiático e o fato de que esses países também se configuram como alvos dos terroristas, os números de atentados e de vítimas européias representam menos de 1% do total mundial.

Em 2016, o continente foi palco de quatro ataques, todos com grande repercussão mundial. Eles ocorreram em Bruxelas, Berlim, Nice e Rouen, na França, com um total de 134 (cento e trinta e quatro) vítimas fatais (WIKIPEDIA, 2017). Já até maio de 2017, foram dois em Paris, um em Londres e um em Estocolmo, com um total de 11 (onze) mortos (SUNDAY EXPRESS, 2017). De setembro de 2001 a 30 de abril de 2017, a Europa e a Rússia, somadas, sofreram 293 (duzentos e noventa e três) ataques praticados por muçulmanos (THE RELIGION OF PEACE, 2017). A fonte registra que a grande maioria foram ações isoladas, inclusive contabilizando crimes comuns perpetrados por muçulmanos, enquanto houve, a nível mundial, mais de trinta mil ataques no mesmo período. Somente em 2016, o sítio The Religion of Peace contabilizou 2.479 (dois mil quatrocentos e setenta e nove) ataques praticados por islâmicos, com mais de vinte e um mil mortos no mundo.

No Brasil, a Operação HASHTAG desarticulou um grupo que planejava realizar ataques terroristas durante as Olimpíadas do Rio em 2016. Alguns brasileiros, utilizando-se das novas tecnologias, juraram lealdade ao EI e iniciaram os planejamentos, para realizarem ataques pontuais e indiscriminados durante os jogos olímpicos. E foi justamente a ação dos órgãos de Inteligência brasileiros no monitoramento do uso da internet pelos suspeitos que possibilitou a prisão desses elementos, antes mesmo que executassem um atentado.

Portanto, infere-se que o trabalho silente e eficaz realizado pelas agências de inteligência no uso das novas tecnologias para a segurança ativa é fundamental para sobrepujar a larga escalada do terrorismo mundial.

Ainda sobre as oportunidades, a dinâmica na análise de informações e os novos sistemas de obtenção de dados potencializaram as capacidades dos profissionais encarregados das medidas de Contraespionagem e Contra-Ações do público interno. Pessoas que há pouco tempo poderiam roubar informações ou mesmo cometer crimes utilizando-se de seus cargos estão sob um maior risco de serem detectadas antes que causem prejuízos institucionais, graças às novas tecnologias de varredura de ambiente, bloqueadores de celulares, interferidores de gravação e toda sorte de medidas eletrônicas para proteção das informações.

No campo da segurança orgânica, a segurança das áreas a instalações ganhou um importante advento no controle e monitoramento do acesso de pessoas graças às novas tecnologias. Atualmente, programas de computadores aliados às imagens geradas por câmeras de monitoramento possuem 97% de eficácia na identificação de um rosto, ao passo que há seis anos esse índice de acerto era de 27%. Já a capacidade de monitoramento de uma pessoa frente a um monitor é reduzida a menos de 50% após 18 minutos, chegando a quase zero após uma hora olhando para as telas do sistema (VILICIC, 2017). Portanto, *softwares* modernos de monitoramento instalados em alfândegas, aeroportos, áreas de acesso restrito ou mesmo nas ruas potencializam a capacidade de detecção e neutralização das ameaças.

Assim, da análise dos inúmeros desafios e impactos apresentados no capítulo anterior e as oportunidades acima elencadas, verifica-se que as instituições que possuem ativos de interesse sempre se constituirão em alvos e devem estar perfeitamente adaptas à nova Era em que vivem.

Nesse interim, é fundamental identificar, de forma macro e sem descer ao nível tático de procedimentos pontuais, quais são as principais premissas que devem nortear as ações de Contrainteligência na Era do Conhecimento. E, como proposta deste presente trabalho, identificou-se quatro premissas gerais e direcionadoras:

Primeira premissa: diversas medidas de Contrainteligência atuais tornar-se-ão obsoletas em pouco tempo. Isso significa que, assim como testes antidopings e sistemas antivírus de computadores estão sempre reagindo às ameaças depois que surgem, as medidas de Contrainteligência voltadas à segurança orgânica ou à segurança ativa estarão constantemente sendo alvos de técnicas e táticas que as sobreponham. Portanto, manuais, regulamentos, regras de uso, recomendações profissionais e toda sorte de procedimento interno de uma instituição deverão estar sob constante revisão, auditoria e aprimoramento.

Segunda premissa: a Contrainteligência nunca será capaz de analisar os dados na mesma velocidade com que estes são propagados. Enquanto uma simples foto pode chegar instantaneamente a milhares de pessoas, analisá-la, confirmar sua veracidade e transformar esse dado em um conhecimento, sempre demandará um tempo bastante superior ao que se levou para que fosse difundida. Assim, muito embora o decisor por vezes tenha necessidade de reagir ou decidir baseado em uma informação não confirmada, os chefes devem estar cientes que decisões baseadas em informações sem prévia análise colocam em risco a própria organização.

Terceira premissa: a segurança da informação depende diretamente do controle sobre os meios de tecnologia da informação, já que são a ferramenta indispensável ao encaminhamento de um dado. Uma vez enviado um arquivo, foto, vídeo ou qualquer outra informação perde-se o controle sobre eles, pois não existe criptografia ou qualquer ferramenta que garanta a perfeita inviolabilidade do mesmo. Portanto, qualquer forma de controle e proteção sobre a informação deve ocorrer sobre os MTI e o seu acesso à internet. Proibição de celulares, bloqueadores de sinal telefônico, uso de computadores fora da rede e da internet e proibição de filmagem e fotografias são apenas alguns exemplos do controle sobre a ferramenta para a proteção dos ativos.

Quarta premissa: os encarregados das medidas de Contrainteligência devem ser afeitos às novas tecnologias ou assessorados por especialistas capazes de usar esses meios com a mesma desenvoltura que aqueles que se dedicam ao seu mau uso. Relegar esta atividade apenas aos métodos empregados na Era Contemporânea seria semelhante à tentativa dos alemães de deterem com metralhadoras os blindados ingleses na Batalha de *Somme*, durante a 1ª Guerra Mundial. Portanto, o emprego de especialistas em MTI na Contrainteligência e o constante acompanhamento desses profissionais que trabalham em outras áreas são fundamentais para a segurança dos ativos de uma organização.

Portanto, da análise das diversas fontes bibliográficas, que permitiram apresentar nos capítulos anteriores as características, os desafios e os impactos da Era do Conhecimento, com as oportunidades elencadas nessa parte do trabalho, comprovaram que a metodologia empregada foi adequada aos objetivos propostos, que conduziu a uma integração de todos os conhecimentos sob as quatro premissas gerais e direcionadoras.

4. CONCLUSÃO

É inquestionável que a velocidade e a profundidade das mudanças comportamentais, sociais, econômicas e científico-tecnológicas ocorridas nos últimos vinte anos ensejarão mais mudanças de extremo significado e impacto em todas as atividades desenvolvidas pelo ser humano, além de abrirem espaço para uma mudança pelo meio acadêmico na classificação da Era em que vivemos.

Conforme apresentado, a Era do Conhecimento não se caracteriza pela invenção de novas tecnologias, mas por um aprimoramento substancial dos meios de comunicação, apoiados sobre uma capacidade de transmissão instantânea de dados e financiado principalmente pelo mercado consumidor, não mais pelos governos.

Um futuro breve nos reserva novas tecnologias ainda mais impactantes. Especialistas da área de tecnologia afirmam que em dez anos não usaremos mais smartphones, que óculos de realidade virtual mudarão a forma como interagimos com o mundo e que a velocidade de transmissão de dados dos domicílios saltará de megabytes por segundo para gigabytes. O ciberterrorismo e outros crimes utilizando a *internet* se tornarão mais comuns. Pessoas mal intencionadas possivelmente poderão assumir o controle de trens, metrôs, carros e caminhões autônomos e toda sorte de meios que possam ser empregados para causar morte, pânico e terror.

Atualmente, a gestão e a proteção do conhecimento, o ativo mais precioso de nossa Era, se tornará o grande desafio da humanidade. O sucesso desta empreitada, em particular da Contrainteligência, será um dos aspectos que determinará o papel de cada uma das nações neste mundo, cada dia mais conectado.

Esse presente estudo integrou conhecimentos diversos, reunindo os desafios, impactos e oportunidades para o ramo da Contrainteligência e integrou-os sob a forma de quatro premissas gerais e direcionadoras: leis, manuais e regulamentos deverão estar sob constante revisão, auditoria e aprimoramento; chefes devem estar cientes que decisões baseadas em informações não analisadas colocam em risco a própria organização; todo controle e proteção da informação deve ocorrer sobre os MTI; e a atividade de Contrainteligência não pode prescindir de especialistas em MTI, bem como esses profissionais de outras áreas devem estar sob constante acompanhamento.

A atuação da Inteligência, em seus dois ramos, dentro do ciberespaço, agora é uma imposição, tendo em vista ser este o ambiente onde a maioria das informações trafega e o ciberespaço se tornou a quinta dimensão do combate, ao lado das dimensões: terrestre, aquática, aérea e espectral magnética. Desta forma, as Forças Armadas de todo mundo devem se adequar a esta realidade sabendo que a dimensão cibernética não pode ser encarada como paralela às demais citadas, mas como uma dimensão que permeia e condiciona todas as outras. Assim, é mister novos estudos para auxiliar em uma adequação técnica e tática das tropas militares, não apenas na atividade de Inteligência mas em todas as funções de combate.

O presente estudo optou por utilizar somente conhecimentos disponíveis em fontes abertas, como forma de ampliar a sua possibilidade de leitura. Isso, no entanto, também se configura em uma limitação, pois não utilizou dados de conhecimento classificados ou sob restrição de acesso, o que restringe a sua abrangência metodológica quanto ao procedimento, bibliográfico.

Outras limitações presentes nesse trabalho dizem respeito ao nível que se decidiu focar a integração dos conhecimentos, com premissas gerais e direcionadoras, ou seja, sem pontuar ações, procedimentos e normas que devem ser estabelecidas de acordo com o cliente ou instituição objeto de análise.

Portanto, é difícil imaginar um país que pretenda desempenhar um papel de protagonista no cenário mundial e que não esteja focado em se adequar à realidade da Era do Conhecimento. Da mesma forma, é difícil imaginar Forças Armadas que pretendam ser a garantia deste mesmo país e que não estejam preparadas para fazer um bom uso das oportunidades que a Era do Conhecimento traz à gestão da informação ou que não saibam proteger adequadamente seus ativos.

REFERÊNCIAS

ALMEIDA, Reginaldo Rodrigues de. Estado Islâmico: à distância de um clique. Janus 2015-2016. Integração regional e multilateralismo, p. 12-13, 2016.

BATISTA, Henrique Gomes. CIA controla celulares, PC e até Smart TV. 2017. Caderno Mundo. O Globo. Rio de Janeiro, 2017.

BBC NETWORK. Um siglo de exhibir inventos. Redacción BBC Mundo. Londres, Inglaterra. Disponível em: <http://www.bbc.com/mundo/ciencia_tecnologia/2009/06/090610_museo_ciencias_rec.shtml>. Acesso em: 21 abr. 2017.

BRASIL. Lei número 13.260, de 16 de março de 2016.

CANEPA, Beatriz. Mundo árabe em mutação. Atualidades. Editora Abril. São Paulo, 2012.
CARROLL, Rory. The Guardian. Elusive sniper saps US morale in Baghdad. Disponível em: <https://www.theguardian.com/world/2005/aug/05/iraq.usa>. Acesso em: 21 abr. 2017.

CASTELLS, Manuel. Redes de indignação e esperança: movimentos sociais na era da internet. Tradução Carlos Alberto Medeiros. Editora Zahar. Rio de Janeiro, 2013.

CLARKE, Richard A.; KNAKE, Robert K. Guerra Cibernética: a próxima ameaça à segurança e o que fazer a respeito. Rio de Janeiro, 2015.

COSTA, Ana Carolina. Propaganda do terror: A Relação Entre a Produção Audiovisual do Estado Islâmico e a Experiência Visual do First Person Shooter. Congresso Internacional Comunicação e Consumo. 2016

FILHO, Oscar Medeiros; NETO Walfredo Bento Ferreira e GONZALES Selma Lúcia de Moura. Segurança e defesa cibernética: da fronteira física aos muros virtuais. Editora UFPE. Recife, 2014.

FOLHA DE SÃO PAULO. Motivos de atirador para matar em boate gay nos EUA se confundem. Jornal Folha de São Paulo, São Paulo 2016. Disponível em: <http://www1.folha.uol.com.br/mundo/2016/06/1782214-motivos-de-atirador-para-atacar-boate-gay-em-orlando-se-confundem.shtml>. Acesso em: 28 abr. 2017.

GUILHERME, Paulo. Hackers russos ajudaram Trump a ser eleito nos EUA, diz CIA. Tecmundo, 2016. Disponível em: <https:/tecmundo.com.br/amp/ataque-hacker/112637-hackers-russos-ajudaram-Trump-eleito-eua.htm>. Acesso em: 07 abr. 2012.

GUIMARÃES, Ricardo. Thymus-Natura: Contexto de Mundo. Vídeo (11min03s). Disponível em: <https://www.youtube.com/watch?v=NHqV5YIvA2A&list=>. Acesso em: 01 abr. 2017.

HERSH, Seymour M.; Peter FRIEDMAN. Chain of command. Harmondsworth: Penguin, 2005.

LEIGH, Davis. Wikileaks: a Guerra de Julian Assange contra os Segredos de Estado / David Leigh, Luke Harding. Tradução Ana Resende. Verus. Campinas, 2011.

LESACA, Javier. Fight against ISIS reveals power of social media. Brookings Institution, 2015.

LÓPEZ, José Maria Álvarez-Pallete. A morte do telefone. Revista VEJA, Edição 2529, ano 50, nº 19, 10 de maio de 2017. São Paulo, 2017.

LOBO, Carlos Eduardo Riberi. O Programa "Guerra nas Estrelas" e o Governo Reagan. Revista de História, Política e Cultura, v.1, n.1, Julho, São Paulo, 2015.

NEVES, Eduardo Borba; DOMINGUES, Clayton Amaral. Manual de metodologia da pesquisa científica. Rio de janeiro, 2007.

OWEN, Mark. Não há dia fácil: um líder da tropa de elite americana conta como mataram Osama Bin Laden. Editora Paralela. São Paulo, 2012.

OXFORD, Dictionaries. The Word of the Year 2016 is... English Oxford Living Dictionaries. Disponível em: <https://en.oxforddictionaries.com/word-of-the-year/word-of-the-year-2016>. Acesso em: 01 maio. 2017.

PHILBIN, Tom. As 100 Maiores Invenções da História. Uma classificação cronológica. – 1 Ed – Algés, Portugal. DIFEL, 2015.

SUNDAY EXPRESS. Terror Attack Timeline: 2017. Londres, Inglaterra [2017]. Disponível em: <http://www.express.co.uk/news/world/693421/Terror-attacks-timeline-France-Brussels-Europe-ISIS-killings-Germany-dates-terrorism>. Acesso em: 07 maio. 2017.

THE RELIGION OF PEACE. List of Islamic Terror: 2016. Disponível em: <https://www.thereligionofpeace.com/attacks/attacks.aspx-?Yr=2016>. Acesso em: 07 maio. 2017.

VILICIC, Felipe. Ela já está entre nós. Revista VEJA, Edição 2520, ano 50, nº 10, 08 de março de 2017. São Paulo, 2017.

WOLOSZYN, André Luís. Ameaças e desafios à segurança humana no séc. XXI: de gangues, narcotráfico, bioterrorismo, ataques cibernéticos às armas de destruição em massa / André Luís Woloszyn. - 2 Ed. - Rio de Janeiro: Biblioteca do Exército; Salto (SP): Schoba, 2013.

WASHINGTON POST. Top Secret America. Washington, Estados Unidos da América: Washington Post Journal, [2010]. Disponível em: <http://projects.washingtonpost.com/top-secret-america/articles/a-hidden-world-growing-beyond-control/>. Acesso em: 01 maio. 2017.

WIKIPEDIA. Terrorism in Europe. Wikipedia Group, [2017]. Disponível em: <https://en.wikipedia.org/wiki/Terrorism_in_Europe>. Acesso em: 07 maio. 2017.