Guerra Hibrida e Ciberconflitos: Uma Análise das Ferramentas Cibernéticas nos Casos da Síria e Conflito Rússia-Ucrânia

Alane Costa Pinheiro[1]
Augusto Ferreira do Nascimento Barbosa[2]
Caroliny dos Santos Marinho[3]
Deywisson Ronaldo Oliveira de Souza[4]
Fernando Henrique Casalunga[5]
Matheus Guerra Guedes[6]

Resumo

Este artigo enfoca às ciber ameaças aos Estados e os seus desafios frente a uma nova modalidade de conflitos. A preocupação central foi descrever e analisar as ciber ações relacionadas a dois casos específicos: o conflito Rússia -Ucrânia e a utilização das redes sociais no caso da Síria. Retrata-se o cenário no qual o ciber conflito entre Rússia e Ucrânia se desenvolveu e apresenta-se atores não-estatais envolvidos no conflito. Já no cenário da Primavera Árabe, buscou-se analisar o papel das mídias sociais como ferramenta de poder, com uma ótica especial para o caso da Síria e as manifestações que ocorrem até hoje. A metodologia foi qualitativa, instrumentalizada por análise de conteúdo. Evidenciou-se a importância da guerra cibernética em um teatro de operações moderno, servindo a "Primavera Árabe" como evidência da capacidade que o ciberespaço tem de mobilizar grandes números de pessoas, por todo um território, em relativo curto espaço de tempo. O conflito Rússia-Ucrânia mostra como táticas de guerra cibernética podem ser usadas como um multiplicador de forças e como meio de ataque e negabilidade, se utilizada de forma coordenada por um Exército.

Palavras-chave: Defesa Cibernética; Ciberconflitos; Guerra Híbrida; Síria; Rússia-Ucrânia; Primavera Árabe.

Introdução

O campo da "segurança e defesa cibernética" refere-se ao conjunto de desafios ligados aos sistemas informacionais que, cada vez mais, crescem em importância para a segurança interna e externa dos países. É possível conceber o conceito de ciberguerra como uma inovação na forma de se fazer a guerra. Em Arquila e Ronfeldt (1993), fica evidente a importância dessa dimensão, ao se comparar a relevância da ciberguerra para o século XXI com a importância que a blitzkrieg[7] atingiu no século XX. A ciberguerra se estende

[1] Graduanda em Ciência Política na Universidade Federal de Pernambuco (UFPE).
[2] Graduando em Ciência Política na UFPE.
[3] Graduanda em Ciência Política na UFPE.
[4] Professor Substituto do Departamento de Ciência Política da UFPE e Doutorando em Ciência Política.
[5] Graduando em Ciência Política na UFPE. Bacharel em História pela Universidade Estadual Paulista Júlio de Mesquita Filho (UNESP).
[6] Graduando em Ciência Política na UFPE.
[7] Blitzkrieg é a expressão utilizada para designar a "Guerra relâmpago": estratégia de guerra utilizada pela Alemanha na segunda Guerra Mundial contra países europeus que devido ao seu ataque surpresa e brutal não

primeiramente no aspecto de busca do conhecimento sobre o inimigo, no sentido de compilar e reter a maior quantidade de informação sobre o outro, permitindo uma espécie de monitoramento do oponente. "Significa tentar saber tudo sobre um adversário enquanto este não sabe nada sobre nós mesmos. Significa virar o equilíbrio de informação e conhecimento ao nosso favor" (ARQUILLA; RONFELDT, 1993, p. 30), permitindo, no futuro, o emprego de menos trabalho e capital em ofensivas com o oponente. É indispensável, ainda, caracterizarmos o chamado "cyberwarfare" como uma posição estratégica e tática instrumental empregada para afetar diretamente o inimigo.

Já o conceito de cibersegurança consiste em adotar medidas para proteger as operações de um sistema de computador ou a integridade de seus dados frente a uma ação hostil. Fundamentalmente, sua definição abrange a segurança e a capacidade de sobrevivência das funções que operam para além do ciberespaço, mas que ainda dependem de um servidor de computador, no qual as informações estão ligadas (CHOUCRI; CLARK, 2011).

Um conceito que também precisa ser abordado é o de Guerra Híbrida. Diferentes definições cercam esse tipo de guerra, e muitos estudiosos afirmam que ela não é um novo tipo de guerra, mas sim um arsenal de recursos e ferramentas que aumentam ao longo do tempo. Neste artigo compreendemos a definição expandida por Hunter (2014), que a entende como "campanhas sofisticadas que combinam, em baixo nível, ações convencionais e operações especiais; mais ações virtuais e espaciais ofensivas; e operações psicológicas que usam as mídias sociais e tradicionais para influenciar a percepção de populares e a opinião pública internacional". Esse modelo de confronto pode ser considerado como mais eficaz, visto que busca objetivos políticos, podendo dispensar uma grande extensão de uso das forças armadas e violentas, fazendo uso de outras ferramentas (LIMNELL, 2015). É possível compreender, então, que o foco tem se estendido cada vez mais para além das ações entendidas como "convencionais".

Com essas definições podemos adentrar brevemente em questões que se constituem como abertura para algumas das principais formas de ataques: a) a dependência de sistemas de redes nacionais e internacionais a sistemas virtuais e de web, aumentando a exposição à ataques estatais e não estatais; b) a vulnerabilidade de Estados em relação a uma maior capacidade organizacional de forma horizontal, por parte da população, pelas redes sociais. Esses pontos serão desenvolvidos nas seções seguintes, com abordagens contextuais de acontecimentos de dois casos específicos: o recente conflito entre Rússia e Ucrânia e o papel da guerra cibernética; e o uso das mídias sociais na Primavera Árabe, especificamente no conflito Sírio, como estratégia militar irregular de guerra híbrida. O artigo também aborda, brevemente, a atual relação dos Estados frente as ameaças cibernéticas e a possibilidade de uma nova modalidade de conflitos.

1. O Conflito Cibernético e as Vulnerabilidades dos Estados

O conceito de guerra cibernética deriva de duas importantes teorias militares. A primeira, diz respeito a capacidade que essa forma de conflito tem para obrigar o inimigo a se render através da indução de paralisia estratégica para atingir fins desejados; e a segunda refere-se ao cumprimento deste objetivo sem emprego de força física (CLAUSEWITZ, 1984, apud LIMNELL, 2015 p.521).

Já o campo da "segurança e defesa cibernética" refere-se ao conjunto de desafios ligados aos sistemas informacionais que, cada vez mais, crescem em importância para a

---

permitia que a tropa inimiga tivesse tempo para se reorganizar. Essa estratégia permitiu a conquista de vários países europeus pelos alemães.

segurança interna dos países. O desenvolvimento de capacidades de defesa das estruturas críticas - hidrelétricas, reatores nucleares, sistemas bancários, transporte, etc.- impõe a necessidade de se manter atualizados estudos a respeito do ambiente cibernético, com intuito de entender como são afetados os computadores atacados e infectados por *malwares*[8].

Conforme aponta Kenneth Geers (2015), neste novo cenário, os combatentes se modificaram. Os novos engenheiros de combate são agora especialistas em desenvolvimento de software, a infantaria se converteu em invasores de rede, e as armas passaram a ser computadores municiados com *malwares*. Os ciberataques aumentam o campo de ação da guerra, confundindo as redes de comando e controle dos adversários, e vêm se tornando cada vez mais úteis para os Estados. Sendo assim, uma simbiose entre hackers e Exército pode resultar em estratégias de invasão mais rápidas e eficazes.

É importante a observação sobre a vulnerabilidade de setores estratégicos da infraestrutura aos ataques cibernéticos, representando, inclusive, um problema para o controle das fronteiras dos Estados. A questão recai sobre a problemática de que os sistemas vitais para a sobrevivência dos Estados, como os de abastecimento energético, financeiro, industrial e de transportes, que hoje estão conectados e são geridos pela internet, foram projetados em um período anterior a própria popularização da rede. Sinalizando a fragilidade com que as defesas destes sistemas foram idealizadas, quando comparadas à diversificação das novas ameaças. A preocupação com a evolução da guerra cibernética e o futuro da era digital tornou-se de extrema importância para os Estados. Refletindo tal problemática, reitera-se o alto grau de complexidade em que se desenrolam os ciberconflitos na era da informática.

Nesse contexto, o interesse no "kinect cyber conflict" - conflito-ciber-físico - aumentou. O termo refere-se a uma classe de ataques cibernéticos que podem causar danos físicos diretos ou indiretos, por meio da exploração de sistemas de informação vulneráveis. Normalmente, estas ameaças cibernéticas são descritas como ataques contra infra-estruturas críticas ou redes industriais e sistemas de controle. As ameaças são orientadas a causar a interrupção temporária, total ou parcial de certos serviços ou sistemas (APLLEGATE, 2013 apud LIMNELL, 2015 p.523). Entretanto, enquanto mais países desenvolvem capacidades de operacionalização no campo virtual, mensurar a capacidade de infringir danos a terceiros por meio de ataques cibernéticos, continua sendo um problema de difícil resolução (INTERNATIONAL STUDIES, apud LIMNELL, 2015, p.524).

Ao estimar as capacidades cibernéticas militares - análise de intenções estratégicas, tecnológicas e políticas - as doutrinas disponíveis revelam algumas informações sobre a alocação de recursos sobre como a organização financeira dos investimentos de um determinado Estado se desenvolve em relação à capacidade de atuação no ciberespaço. Embora isso seja uma clara indicação de movimento e incentivo à atividade da ciberguerra, os dados acerca dos incentivos financeiros estatais são, normalmente, vagos e de difícil acesso. Ou seja, os dados sobre a alocação de recursos do Estado para a tecnologia de defesa cibernética chegam a existir, mas são pouco explicativos ou transparentes. Contudo, Segundo Limnell (2015), diversos Estados tem anunciado a formação de unidades cibernéticas em suas forças armadas, atitude que em si pode ser encarada como parte de uma tendência de reforço

[8] *Malware* é o termo utilizado para designar o software projetado para interferir na funcionalidade do computador ou para degradar a integridade dos dados. Engloba uma gama de códigos de computador maliciosos-vírus, *worms*, *trojans*, *spyware*, *adware*, etc-.Um *Malware* pode ser projetado para abrir uma avenida de acesso a um sistema de computador adversário, e/ou para atacá-lo. Assim, o uso de softwares maliciosos é um instrumento de hostilidade cibernética, não uma categoria separada de ação (KELLO, Lucas, 2013 p.18 tradução nossa).

das capacidades de defesa e ação no ciberespaço. Outros indicadores mensuráveis da atividade cibernética que podem ser encontrados são o recrutamento de peritos cibernéticos, atualizando as ciberestratégias militares, e o nível de sofisticação das parcerias público-privadas entre os Estados (LIMNELL, 2015, p.524).

Contudo, é de suma importância compreender que o aumento de ataques cibernéticos patrocinados pelo Estado pode ser enquadrado dentro de uma percepção de que não há um significativo "preço a pagar" para tais ataques, devido a falta de legislação sobre ações cibernéticas, uma vez que os protocolos para responder às ameaças à segurança nacional patrocinados pelo Estado não são claros para ataques cibernéticos (LIMNELL, 2015, p.525). Porém, os conflitos atuais tornaram-se uma oportunidade ímpar para o desenvolvimento de pesquisas na área, assim como para a criação de um “playbook” - livro do jogo- cibernético.

2. O Conflito Rússia- Ucrânia e o Papel da Guerra Cibernética

A Rússia lidera mundialmente o desenvolvimento de softwares e técnicas na área de cibersegurança (GILES, 2012a). Os diálogos entre Rússia e Ocidente no que tange o ciberespaço são caracterizados por uma incompreensão mútua e aparente intransigência. As normas não são de comum acordo, tal qual a falta de um vocabulário comum e conceitos relacionados dificultam o alcance de acordos (GILES, 2012b).

Conforme salienta o pensamento de Weedon (2015), na Rússia os setores estratégicos desconsideram o termo “cyberwar” - guerra cibernética -, ou mesmo o prefixo ‘cyber’ como um conceito distinto, pelo contrário, os russos enxergam as operações na rede de computadores como ferramentas integradas aos esforços do Estado para manter e/ou ampliar o domínio político e militar em um determinado território. (WEEDON, 2015, p.68). Um importante documento da segurança russa, “Information Security Doctrine of the Russian Federation” (2000), aponta em seu artigo primeiro um conjunto de informações sobre segurança e ciber questões que aprerrogam a intenção de “assegurar os direitos constitucionais e liberdade dos homens e cidadãos para livremente buscarem, receberem, transmitirem, produzirem e disseminarem informação por qualquer meio legal” (Article I, Part 1, apud GILES, 2012b).

No entanto, as recentes ações do Exército russo vêm sendo vinculadas aos ciberataques DDoS[9], que paralisaram os sistemas de computadores na Estônia, em 2007, e atingiram as comunicações e o Banco Nacional na Geórgia, em 2008, marcando o início de uma nova era do ciberconflito (KELLO, 2013). A recente ação militar russa na Ucrânia - 2014-5-, também, foi acompanhada por uma série de ataques da mesma natureza, que infectaram computadores de estações elétricas e derrubaram o fornecimento de energia (GEERS, 2015).

Em vista disto, a guerra Rússia-Ucrânia tem sido tratada amplamente como a crise de segurança mais importante desde o fim da Guerra Fria. O conflito em questão, atualmente, é o maior exemplo do que se convencionou denominar como guerra híbrida, uma espécie de

[9]Um ataque DDoS tem como objetivo tornar um servidor, um serviço ou uma infraestrutura indisponíveis, ao sobrecarregar a largura da banda do servidor ou fazendo uso dos seus recursos até que estes se esgotem. Durante um ataque DDoS, vários pedidos são enviados em simultâneo, a partir de vários pontos da Net. A intensidade deste "fogo cruzado" torna o serviço instável, ou pior, indisponível. (OVH.pt, 2015). Disponível em: <https://www.ovh.pt/anti-ddos/principio-anti-ddos.xml> Acesso em 15.04.2016

conflito que combina estratégias militares, econômicas e políticas para atingir os objetivos de um determinado Estado em território inimigo (LIMNELL, 2015, p.521).

> Basicamente, todos os meios e ferramentas empregados pela Rússia no âmbito da guerra híbrida fazem parte da antiga política externa e de segurança soviética, bem como da história da guerra assimétrica. A única novidade tem sido o alto grau de efetividade, em muitos casos, quase uma coordenação em tempo real de vários meios empregados, incluindo políticos, operações militares especiais e medidas de informação (RÁCZ, 2015, apud LIMNELL, 2015, p. 522, *tradução nossa*).

Embora a Rússia negue ter agido em consonância com estes grupos, a coincidência cronológica entre os ataques cibernéticos e as invasões por terra tornam os argumentos do governo russo de difícil sustentação. Particularmente, no que diz respeito ao conflito Rússia-Ucrânia, os ataques cibernéticos não foram na mesma medida prejudiciais como os perpetrados na Estônia, em 2007, e na Geórgia, no ano seguinte.

Nos três casos, os ciberataques ocorreram poucas horas antes das tropas do Kremlin avançarem sobre as fronteiras destes territórios, com o comprometimento de setores estratégicos, tais como as redes de telecomunicação e distribuição de gás e energia. Desse modo, as defesas desses países tornaram-se permeáveis a um ataque direto. Enfrentando pouca resistência, a Rússia conseguiu invadir os territórios sem incorrer em um grande derramamento de sangue.

De acordo com James Stavridis, Supremo Comandante das Forças Aliadas da Europa – OTAN -, os ataques cibernéticos à Estônia e Geórgia fornecem uma "ideia deste futuro [de conflito]" (MILES, 2012, apud KELLO, 2013, p.24).

O conflito Rússia-Ucrânia foi o resultado de uma tensão política histórica entre os países, que se intensificou quando o ex-presidente ucraniano Viktor Yanukovych recusou-se a assinar um acordo comercial com a União Européia, em novembro de 2013 (MAURER, 2015, p.80). Logo após Yanukovych deixar a Ucrânia, em fevereiro de 2014, tropas russas tomaram o controle dos aeroportos internacionais de Sevastopol e Simferopol. Ao mesmo tempo, as tropas do Kremlin avariaram cabos de fibra óptica e invadiram o sistema operacional da empresa de telecomunicações Ukrtelecom, interrompendo, por completo, o serviço de telefonia e o acesso a internet de usuários da Crimea.

No mês seguinte, enquanto as tropas russas avançavam sobre o território da Crimea, o principal *website* do governo ucraniano foi derrubado por 72 horas; outros sites também foram corrompidos pelos ataques coordenados simultaneamente. Na ocasião, dispositivos móveis de telefonia de membros do parlamento ucraniano também foram hackeados. Apesar do dano causado, os ciberataques foram caracterizados como de baixa intensidade (MAURER, 2015; WEEDON, 2015). A resposta ucraniana ocorreu após a invasão da península. Em março, grupos de hackers pró-kiev intitulados “Cyber Hundred” e “Null Sector” utilizaram uma série de ataques DDoS contra sites de Moscow e do Banco Central russo (MAURER, 2015).

Em maio, um dos grupos pró-Rússia, denominado“CyberBerkut”, assumiu a responsabilidade por violar os sistema central da comissão eleitoral e tentar apagar os resultados da votação presidencial. O grupo obteve, ainda, acesso a documentos confidenciais e passou a disponibilizá-los, periodicamente, em sua página na rede.

Apesar da investida ter causado alguns danos, o serviço de segurança ucraniano – SBU - conseguiu remover o *malware* que havia infectado o sistema e substituir o *software* eleitoral sem grandes problemas para o resultado das eleições (WEEDON, 2015).

Desde sua descoberta, em 2007, o BlackEnergy[10] tem sido constantemente atualizado, devido a sua alta mutabilidade, através da inclusão de novas funções destrutivas, o combate preventivo tornar-se difícil. Os especialistas do F-Secure Labs, empresa finlandesa especializada em cibersegurança, reforçam que ataques do tipo BlackEnergy são largamente utilizados na espionagem de organizações, empresas e grupos industriais. De acordo com o F-Secure, o *malware* BlackEnergy, originalmente desenvolvido e utilizado com fins lucrativos criminais, foi implantado contra organizações governamentais na Ucrânia por um grupo chamado "Quedagh". O relatório conclui afirmando que: "O uso do BlackEnergy para um ataque orientado politicamente representa uma intrigante convergência da atividade criminosa e de espionagem" (MAURER, 2015, P.85).

Em dezembro de 2015, a cidade de Ivano-Frankivsk localizada à oeste da Ucrânia, teve a distribuição de energia comprometida por seis horas devido a um ataque de "BlackEnergy", o *malware* conhecido como KillDisk[11] atingiu os sistemas da usina elétrica e comprometeu o abastecimento de milhares de residências. O ministro ucraniano de Energia acusou à Rússia de estar por detrás dos ataques (TUPTUK; HAILES, 2016). Acredita-se que o *malware* 'KillDisk' está relacionado com o *malware* destrutivo utilizado durante as eleições ucranianas em outubro. Na época, o CERT-UA[12] conectou esse incidente com os ataques Black Energy, e, desde então, empresas da área de segurança cibernética como a Symantec[13] tem analisado estes ataques. Além disso, outras fontes especializadas nesta temática, tal como a iSIGHT[14], reportaram que o *malware* BlackEnergy foi implantado em pelo menos um dos sistemas de energia ucranianos afetados pelo 'KillDisk'(PHSYORG, 2015).

Os principais grupos responsáveis por empregar ciber ataques à Ucrânia em prol da Rússia foram classificados como APT –Advanced Persistent Threat-, siga em inglês que significa 'Ameaça Persistente Avançada'. Para Weedon (2015), a infraestrutura demandada para empreender ataques globais dispersos, pode sinalizar o envolvimento subsidiário do governo russo nas ações destes grupos.

Weedon (2015) ressalta que, desde 2013, a chamada "operação Armagedom" -uma campanha de espionagem cibernética russa que teria como alvo o governo ucraniano- tem ajudado a proporcionar uma vantagem militar para a Rússia nas disputas territoriais com a Ucrânia. Segundo a autora, a Rússia tem um longo histórico de operações que utilizam informações falsas para criar confusão e/ou semear o pânico, provocando condições favoráveis à sua atividade político-militar.

Na era da internet, a tática do Kremlin evoluiu, disseminaram-se informações e propagandas online e a internet passou a ser utilizada pelos russos de maneira intensiva como veículo para confundir seus adversários; os chamados 'backdoors' cibernéticos tornaram-se mais frequentes. Este tipo de tática é utilizada no acesso e divulgação de dados de maneira ilícita. Neste sentido, ressalta-se preparação sistemática do campo de batalha como uma ação consistente do pensamento estratégico russo (HEICKERÖ, 2010, apud, WEEDON, 2015).

---

[10] BlackEnergy é um tipo de *malware* que oferece suporte à servidores *proxy* para obter controle da conta de um determinado usuário. Uma vez adquirida a senha do usuário, o invasor pode agir sem ser detectado e causar danos. (F-SECURE LABS, Blackenergy&Quedagh: The convergence of crimeware and APT attacks, 2014)

[11] O KillDisk é capaz de extrair informações vitais dos sistemas de segurança, além de deletar arquivos do sistema, destruir o hard drive dos computadores e sabotar sistemas de controle industrial causando graves danos aos setores de infraestrutura crítica (PHSYORG, 2015).

[12] CERT-UA, Computer Emergency Response Team of Ukraine, empresa ucraniana especializada em segurança cibernética.

[13]Symantec: empresa especializada em segurança cibernética. Para maiores informações visitar *website,* nas referências.

[14] O iSIGHT Partners é uma empresa global de inteligencia na área de cyber ameaças, para maiores informações visitar *website*, referências.

Os estudos de Weedon (2015), apontam que os grupos estão divididos por categorias. Os membros do chamado "Tsar Team/Sofacy/Pawn Storm" recebem a classificação de APT28. Estes hackers têm por objetivo roubar informações de entidades ligadas aos interesses geopolíticos da Rússia. Conforme aponta o documento divulgado pelo Fire Eye[15], em 2014, o trabalho do APT28, vem recebendo subsídio do governo russo. A atuação se dá através do envio de e-mails carregados de links corrompidos e *malwares* para *download*. Os alvos principais são os governos ocidentais, tendo como objetivo adquirir informações ligadas à política externa e/ou relacionadas com a defesa nacional.

Ainda de acordo com Weedon (2015), há outro importante grupo de ciber espionagem, que de maneira similar ao APT28 tem como objetivo obter informações sigilosas de organizações de segurança governamental e militar, conhecido como APT29. Novamente, os alvos principais são os países do leste Europeu. Um dos *malwares* utilizados é identificado como 'Hammertoss'[16], uma ferramenta de difícil detecção, em grande parte devido a sua capacidade de mimetizar o comportamento dos usuários infectados. A movimentação aparentemente regular do usuário ajuda o *malware* a evadir sua detecção, possibilitando o roubo de senhas e dados pessoais das vítimas. Além disso, o APT29 conta também com os chamados "Dukes"[17], uma coleção de malwares que estão sendo monitorados desde 2007, e já demostraram capacidade para afetar computadores e *smartphones* em diversos países, não apenas europeus como também asiáticos (LAWRENCE; RILEY, 2014, apud WEEDON, 2015; BAUMGARTNER; RAIU, 2015, apud WEEDON, 2015).

Ao analisar o caso Rússia-Ucrânia, Maurer (2015), insere a condição socioeconômica como uma variável de influência no surgimento de grupos de ciber-espionagem, como o "CarderPlanet", na cidade de Odessa, o qual atua manipulando dados de cartões de crédito de norte-americanos e europeus. De acordo com o autor, em um contexto de oportunidades reduzidas, os indivíduos são levados a agir de forma contraventora, sendo o grupo responsável por absorver mão-de-obra tecnicamente qualificada para a ciber-criminalidade (GLENNY, 2009, apud MAURER, 2015, p.83).

Para designar esta gama de atores circulando na esfera cibernética privada, Maurer (2015), utiliza o termo "proxy"[18]. Seus estudos revelam ainda outros grupos *proxies* importantes como o intitulado "Ciber Força Ucraniana", composto por voluntários recrutados através de veículos de mídia social. O grupo é responsável por publicar na rede informações importantes do Ministério do Interior da Rússia. Outro importante grupo denomina-se "CyberForce", uma de suas ações foi atuar no monitoramento de tropas separatistas por meio do uso não autorizado de câmeras de vigilância no leste ucraniano.Também fazem parte desta classificação de *proxies* outros atores, como os grupos de hacktivismo pró-Kiev: "OpRussia"; "Russian Cyber Command"; "Cyber Ukranian Army"; "Cyber Hundrer" e "Null Sector" (MAURER, 2015).

Maurer (2015), sugere, no entanto, que não se observa nos cidadãos ucranianos um forte nacionalismo capaz de mobilizar uma reação técnica coordenada entre os agentes

[15]"A Window Into Russia's Cyber Espionage Operations?"(FIRE-EYE, 2015).

[16]A ferramenta funciona da seguinte forma: checa e recupera comandos através de serviços de confiança na web, como Twitter e GitHub; Usando servidores corrompidos para controlar e comandar (C2); Visitando diferentes páginas do Twitter lidas diária e automaticamente; Usando ataques direcionados, como comunicação após uma data específica ou apenas durante a semana de trabalho da vítima; Obtendo comandos através de imagens que contêm dados ocultos e criptografados. (WEEDON, 2015, p.70 *tradução nossa*).

[17]Em algumas literaturas o grupo "Dukes" recebem a denominação de APT29. Para um aprofundamento sobre suas atuações ver: whitepaper F-secure Labs Trheat intelligence "The Dukes, 7 years of ciberespionage", 2015.

[18]O termo "proxy" enfrenta limitações conceituais importantes, carece de uma definição clara, no relatório da GGE (Group of Governmental Experts) o termo parece caracterisar um ator que flutua entre atores estatais e não estatais, que atua no interstício entre ambos (MAURER, 2015, P.86).

privados “proxy” e o governo ucraniano, “o conflito não parece ter mobilizado os atores não-estatais mais sofisticados com recursos cibernéticos na região” (MAURER, 2015, p.84). Adere a isto o fato de que, segundo as entrevistas coletadas por Mauer na Ucrânia, mesmo que tal conexão fosse possível, o governo ucraniano não seria capaz de coordenar a ação.

Diante do exposto, não obstante a já citada capacidade limitada do governo ucraniano, é importante notar a tomada de posição dos países membros da OTAN no sentido de auxiliar a ciber defesa na Ucrânia, posicionando-se claramente ao lado de Kiev no conflito contra os russos. Tal fato se deu por meio do “Cyber Defence Trust Fund”, o qual investiu em treinamento e melhoria das defesas cibernéticas ucranianas, fortalecendo os laços entre Kiev e o bloco (MAUER, 2015, p.84).

Mediante uma análise qualitativa das fontes primárias e secundárias, a pretensão deste artigo não foi a de especificar criteriosamente quais são os grupos que tem atuado no âmbito da ciber criminalidade, ou mesmo detalhar cronologicamente quais foram os ataques empregados nos conflitos entre Rússia e Ucrânia nos últimos anos, este seria um esforço demasiado longo para um breve estudo.

De tal modo que a preocupação central foi realizar um apanhado geral dos casos e apresentar o cenário no qual o ciber conflito s e desenvolve. Além disso, trazer à luz alguns atores não-estatais que estão indiretamente envolvidos no conflito.

3. A Primavera Árabe e o Papel das Mídias Sociais

A chamada “Primavera Árabe” foi um movimento revolucionário de protestos e de guerras que ocorreram - algumas ainda ocorrem até a data atual - no Oriente Médio e no norte da África. O movimento teve início no final de 2010 tendo como símbolo um jovem tunisiano que ateou fogo ao próprio corpo protestando contra seu governo e as condições de vida de seu país. As manifestações decorrentes acabaram afastando o Chefe de Estado, Ben Ali, do poder, em 2011. O sentimento de rebeldia contra governos ditatoriais no mundo árabe, assim como o aparente sucesso dos manifestantes na Tunísia, serviu com incentivo, e em pouco tempo diversos países da região conviveriam com reivindicações semelhantes.

Os países que foram atingidos por fortes protestos - Argélia, Egito, Jordânia, Iêmen, Líbia, Síria, Iraque, Omã, Djibuti e Barein – se assemelham por terem governos autocráticos, altas taxas de corrupção, grau elevado de desigualdade social, serem regimes fechados, e manterem segurança coercitiva abusiva e privatizações em favor de minorias elitistas (LYNCH, 2011 apud VIEIRA, 2013, p. 3). No total, seis governos foram derrubados, três guerras civis emergiram, e várias mudanças governamentais ocorreram em alguns desses países. A Primavera Árabe teve - e tem - como um movimento em favor da democracia, pela maior parte da população, de proporções gigantescas, uma clara importância política, atraindo o olhar da sociedade internacional e dos países centrais.

3.1 As Redes e a Primavera

Um dos fatores mais relevantes que contribuiu para incentivar, atrair e agregar a população aos atos foi o uso das mídias sociais como meio de comunicação e propagação de informações. A definição de guerra híbrida de Frank Hoffman inclui exatamente “Operações psicológicas que utilizam as mídias sociais para influenciar a percepção popular e a opinião

internacional" no conceito (HUNTER, 2014), algo que é visto claramente no caso dos levantes Árabes.

A internet guarda potencialidades únicas para a geração de mudanças sociais em uma sociedade, pois ela, ao contrário das mídias tradicionais, consegue integrar vários tipos de modalidades de comunicação e conteúdo -Vídeo, imagem, texto, áudio - em um único meio (DIMAGGIO *et al*, 2001). Além dessas funcionalidades conteudistas, tais redes também permitiam a criação de páginas para o debate e discussão de uma temática, as quais permitem a formação de laços comunitários online independentes de identidades geográficas (CASTELLS, 2003 apud REIS, 2011, pg. 8). No caso em questão, essas novas mídias deram poder aos indivíduos para coordenar, comunicar, e difundir as repressões e as censuras do Estado, transformando uma rede hierárquica de comunicação em uma rede mais horizontal (LYNCH, 2014).

A utilização das redes sociais, tais como o Facebook, Twitter, Youtube, foi um dos principais recursos para espalhar notícias de protestos e mobilizar a população. No caso Egípcio a *Fanpage*[19] mais famosa era a "We Are All Khaled Said". Ela foi criada após o assassinato do estudante Khaled Said, e denunciou a tortura da polícia Egípcia contra a população, e incentivou, por meio de fotos e vídeos, as manifestações contra as ações violentas do governo Mubarak. O foco inicial da página era falar sobre as brutalidades do regime totalitário, e sobre direitos humanos universais. Porém à medida que os movimentos em outros países ganharam maior destaque, a página passou a dar apoio aos manifestantes de outros países, como a revolução na Tunísia. Adiante, a página teve importância significativa para espalhar, incentivar e organizar os protestos de 25 de janeiro e que deu início à derrubada do governo. As páginas da rede tiveram um relativo sucesso neste contexto devido ao seu caráter horizontal e pessoal entre as pessoas:

> [...] A cobertura era colaborativa, ou seja, não havia uma equipe contratada com o objetivo de realizar vídeos e fotos das manifestações, mas sim uma rede de internautas que produziam individualmente seus conteúdos, os publicavam online e chegavam à Fan page […] (REIS, 2011, p. 13-14).

Comparando-se com 2010, nos primeiros 3 meses de 2011 houve um crescimento de 30% na utilização do Facebook nos países Árabes. Países com manifestações civis mais impactantes tiveram um aumento exponencial do uso da rede, com exceção da Líbia (ARAB, 2011).

A tabela 01 demonstra o aumento da utilização do Facebook, de maneira total, em 9 países da região.

Tabela 01: Crescimento no Número de Usuários do Facebook de 5/1/2011 até 5/4/2011 (%).

País	**Crescimento no Número de Usuários (Facebook) entre 5/1/2011 e 5/4/2011 (%)**

[19] Uma *Fanpage* é uma página específica no Facebook que cria contato entre uma empresa, organização, ou movimento e seus clientes/fãs.

Argélia	40.43
Barein	9.18
Djibuti	14.48
Egito	42.12
Iraque	82.24
Líbia	-71.73
Síria	40.63
Tunísia	29.42
Iêmen	89.95

Fonte: Dados da Arab Social Media Report, Compilação Própria.

Os dados mostram um aumento do número de usuários do Facebook, o que pode estar ligado a onda de protestos que ocorreu, com exceção da Líbia, onde o acesso à internet foi interrompido pelo governo. Esse aumento pode evidenciar o papel importante, mas possivelmente não exclusivo, que o Facebook teve na mobilização desses movimentos, principalmente naqueles que tiveram as manifestações mais significativas.

Foi conduzido um *Survey* (ARAB, 2011), também, que classifica a finalidade da utilização do Facebook pelos seus usuários, no Egito e na Tunísia. No Egito, cerca de 85% dos entrevistados responderam que utilizam a rede nessas classificações: Organizar ações ativistas (30%); Espalhar informações para o mundo sobre o movimento e eventos relacionados (24%); Conscientização dentro do país das causas dos movimentos (31%). Já cerca de 15% disseram que utilizam apenas para entretenimento, comunicação pessoal e outros motivos. Na Tunísia a proporção dos entrevistados foi de aproximadamente 86% (22%, 33%, e 31% respectivamente), para 14%.

Tabela 02: Mensuração de Eficiência de Páginas em 10 casos selecionados

Caso	**TPF**[20]	**Eficiência da página**
Tunísia, 14 Jan.	18.8%	Sim

[20] TPF: Taxa de Penetração do Facebook (%)

Egito, 25 Jan.	5.5%	Sim
Iêmen, 3 e 10 Fev.	0.93%	Sim
Síria, 4 Fev.	1.2%	Não
Barein, 14 Fev.	32%	Sim
Líbia, 17 Fev.	4.3%	Sim
Omã, 3 Mar.	7.8%	Sim
Arábia Saudita, 11 e 20 Mar.	13%	Sim
Síria, 15 Mar.	1.67%	Sim
Palestina, 15 Maio	12.8%	Sim

Fonte: Dados da Arab Social Media Report, Compilação Própria.

A tabela 02 demonstra a eficiência das páginas utilizadas para informar e mobilizar protestantes, que seria alcançada se a população atendeu, e foi para as ruas, quando a página do Facebook organizou os protestos para determinada data. Ou seja, o "Sim" significa que houve resposta real da população, em cada caso, que representa o chamado da página para o protesto (País/Data). Pode-se perceber que independente da "Taxa de Penetração do Facebook" no país, em quase todos os casos (exceto pela Síria em 4 de fevereiro) há uma resposta real da população ao chamado.

O Facebook, portanto, foi uma ferramenta utilizada pelos ativistas para organizar e distribuir informações entre si, da realização de protestos, voltando-se para incentivar a população de fato, e não a sociedade internacional.

Assim como o Facebook, o Twitter foi uma ferramenta que foi utilizada e serviu como instrumento das reivindicações. Porém, ao contrário do Facebook, o Twitter está voltado ao mundo estrangeiro, como plataforma para debate e um compartilhamento de notícias sobre os acontecimentos nos países Árabes. Enquanto Facebook e Youtube serviam mais como forma de "jornalismo ativista", e de debates e processos organizatórios entre os manifestantes, o Twitter serviu como uma base para que os ativistas pudessem contatar suas mensagens para o meio internacional, em inglês (HOUNSHELL, 2011).

3.2 O Conflito Sírio

A recente guerra civil Síria tem suas origens na própria violência do Exército nacional contra sua população em protestos alegadamente pacíficos. A maior oposição ao governo de Bashar Al-Assad, o Exército Livre Sírio – ELS - composto por civis e por soldados desertores indignados, pretendaim derrubar o regime e instaurar um governo democrático que respeitasse

os direitos humanos. O grupo teve apoio de países como os EUA, França, Reino Unido, Turquia, Barein, Jordânia e Marrocos. O conflito se complicou quando foi descoberto células islâmicas radicais entre a oposição, que supostamente respondiam ao EIIL (Estado Islâmico do Iraque e do Levante), chamadas de Frente al-Nusra. Elas tinham como objetivo derrubar o governo e estabelecer um califado na região, assim como o Estado Islâmico havia feito no Iraque. Nessas circunstâncias, a oposição moderada síria declarou que é era contraria a esses grupos. Esse contexto tripolar dificulta uma clareza entre os atos cometidos, os grupos que cometeram, e a definição dos lados.

É importante destacar que o papel das mídias sociais, tal como nos outros casos da Primavera Árabe, como forma de organização e de distribuição de informação, teve uma importância maior na medida em que os ativistas se organizavam em uma unidade. Nesse sentido, o conflito Sírio está sendo o conflito civil mais "Socially mediated"– impactado pelas redes sociais – da história (LYNCH; FREELON; ADAY, 2014).

Como uma enorme parte do que a população internacional sabe, ou pensa que sabe, sobre o conflito vem de vídeos e comentários que circulam pelas redes sociais, as mídias sociais podem criar a ilusão de ondas de informação "não mediadas", ou seja, aqueles internautas que seguem as redes têm a impressão de que tais informações são precisas e confiáveis. Porém, as informações aparentemente não mediadas podem ser enviesadas por essas redes de ativistas para fabricar narrativas que apelem à intervenção internacional contra o governo (LYNCH, FREELON, ADAY, 2014).

Essa utilização específica das mídias sociais como alteradora da percepção internacional se encaixa nas "Operações psicológicas" na definição de guerra híbrida (HUNTER, 2014). Isso fica mais claro quando se observa que há narrativas competitivas vindas das redes sociais, onde não apenas a oposição ao governo quis espalhar a narrativa para a mídia internacional de que havia uma insurreição pacífica e pró-ocidental, mas o próprio regime Sírio se utilizou da estratégia midiática para retratar seus opositores como radicais Islâmicos financiados e apoiados por estrangeiros.

Lynch afirma (2014, p. 16-21) que há uma diferença, ou viés, quando se compara a língua utilizada nas redes sociais, se referindo especificamente ao Twitter. As informações em inglês pareciam ter uma visão mais geral, de solidariedade à população Síria, e de apoio a oposição e aos protestos, enquanto as informações em Árabe continham comentários, vídeos e imagens dos radicais Islâmicos e a favor deles. Assim, a mídia internacional, no início, muitas vezes ignorava as informações de língua Árabe o que causava uma distorção na interpretação dos acontecimentos.

As principais facções políticas de oposição na Síria, como o Conselho Nacional Sírio, o Comitê Nacional de Coordenação para a Mudança Democrática, e os Comitês de Coordenação Local da Síria, operam e mantêm redes profissionais de *websites* e plataformas de mídias sociais que transmitem informações. O Observatório Sírio de Direitos Humanos, que tem laços com o Conselho Nacional Sírio, também são muito ativos na mídia social, publicando informações sobre possíveis abusos dos direitos humanos no regime de Assad. A "Omawi News Live" e a "Ugarit News" são duas das mais importantes redes, atuando em canais do Youtube e no Twitter, que servem como plataformas informacionais que transmitem uma grande quantidade de material midiático a favor da oposição síria. O próprio Exército Livre Sírio tem uma alta atuação nas mídias sociais por meio de redes e canais que incentivam e promovem a luta armada contra o governo. Relativo a isso, o regime Sírio não ficou na inércia, dando forte atenção às mídias sociais oficiais do país, como o "Syrian Arab News Agency" (SANA), e formando o Exército Eletrônico Sírio, que não apenas exerce suas atividades de defesa e segurança cibernética, mas também exerce atividades midiáticas que tentam demonstrar a ilegitimidade e a radicalização dos opositores (ZAMBELIS, 2012).

As mídias sociais tiveram extrema importância, também, para o terceiro ator no conflito Sírio: os grupos islâmicos radicais como o EIIL. Utilizando-se das mídias sociais, o Estado Islâmico pôde aterrorizar o mundo ocidental de maneira simples e eficiente: "Uma vítima, uma faca, e uma câmera" (YEUNG, 2015, p. 2-3). Nesse tipo de conflito não são necessários grandes acontecimentos, com armas físicas massivas. Faz-se necessário somente a percepção dos usuários sobre algo que é cada vez mais compartilhado e visto nas redes e a multiplicação das pessoas que se mobilizam para postar e compartilhar as imagens e os vídeos.

A utilização desses canais torna-se um dos caminhos irregulares para confrontar, indiretamente, um estado, contornando as deficiências financeiras, políticas, e militares que uma organização não tradicional pode enfrentar.

Conclusões

Evidencia-se, portanto, a importância da guerra cibernética em um teatro de operações moderno, servindo a "Primavera Árabe" como evidência da capacidade que o ciberespaço tem de mobilizar grandes números de pessoas, por todo um território, em relativo curto espaço de tempo, com baixo custo e propiciando a elas acesso direto e instantâneo a informação. O conflito Rússia-Ucrânia por sua vez, mostra como táticas de guerra cibernética podem ser usadas como um multiplicador de forças ou até mesmo como forma principal de ataque quando usada de forma coordenada por um Exército, ao mesmo tempo em que podem prover certo grau de negabilidade a governos.

Por fim, *malwares* como o "KillDisk" e o "STUXNET" servem para chamar atenção para o potencial destrutivo real que um ataque cibernético pode causar e a necessidade de se ter um centro e sistema de defesa dedicado a combater e explorar tais ameaças, principalmente quando se leva em consideração a tendência mundial de digitalização dos meios e a grande velocidade com a qual novas tecnologias surgem em um tempo em que guerra tradicional mescla-se com táticas não-convencionais, criando um novo campo de batalha em que os guerreiros podem ou não estar até mesmo em continentes distintos.

Referências

APPLEGATE, S: The Dawn of Kinetic Cyber. In: Podins, K., Stinissen, J., Maybaum, M (eds.): **5th International Conference on Cyber Conflicts**. p.3-6, NATO CCDCOE Publications. Tallinn 2013.

ARAB Social Media Report. **Dubai School of Government**. Vol. 1, No, 2, maio de 2011.

ARQUILA, jonh; RONFELDT, david; Cyberwar is coming! Comparative Strategy, Vol. 12, No. 2, Spring **1993**, pp. 141–165

BAUMGARTNER, Kurt; RAIU, Costin TheCozyDuke APT.**Kaspersky Lab**. Abril 21, 2015. <https://securelist.com/blog/69731/the-cozyduke-apt/> in 'Duke APT group's latest tools: cloud services and Linux support.' July 22, 2015. *F-Secure*. https://www.f-

secure.com/weblog/archives/00002822.html apudWEEDON, J: Beyond Cyber War: Russia´s use of Strategic Cyber Espionage and Information Operations in Ukraine. In: Geers, K (ed.). **Cyber War in Perspective: Russian Aggression Against Ukraine**. p.67-77NATO CCDCOE Publications. Tallinn. 2015

CASTELLS, Manuel. **A Galáxia da Internet – reflexões sobre a internet, os negócios e a Sociedade**. Rio de Janeiro: Jorge Zahar Editor, 2003

CHOUCRI, Nazli;CLARK, David; **Cyberspace and International Relations: Toward an Integrated System,** 2011

CLAUSEWITZ, C: **On War**. Howard, M., Paret, M. (eds.), Princeton, NJ 1984.

CLULEY, Graham. MiniDionis: Where a Voicemail Can Lead to a Malware Attack. Julho 16, 2015 apudWEEDON, J: Beyond Cyber War: Russia´s use of Strategic Cyber Espionage and Information Operations in Ukraine. In: Geers, K (ed.). **Cyber War in Perspective: Russian Aggression Against Ukraine**. p.67-77NATO CCDCOE Publications. Tallinn. 2015

DIMAGGIO, Paul; HARGITTAI, Eszter; NEUMAN, W Russell; ROBINSON, John P. Social implications of the Internet. **Annual Review of Sociology**, 2001, 27, p. 307-336

FIRE-EYE, A Window Into Russia's Cyber Espionage Operations? **Fire-eye Threat Intelligence** Outubro, 27, 2014<https://www.fireeye.com/blog/threat-research/2014/10/apt28-a-window-into-russias-cyber-espionage-operations.html>Acessoem 20.05.2016. apudWEEDON, J: Beyond Cyber War: Russia´s use of Strategic Cyber Espionage and Information Operations in Ukraine. In: Geers, K (ed.). **Cyber War in Perspective: Russian Aggression Against Ukraine**. p.67-77NATO CCDCOE Publications. Tallinn. 2015

GEERS, Kenneth. Cyber War in Perspective Russian Agression against Ukraine, **NATO Cooperative Cyber Defence Centre of Excellence**, Tallin, Estônia, 2015.

GILES, Keir. Russian Cyber Security: concepts and current activity. **Conflict Studies Research Centre**, 6 september 2012a.

_____. Russia's Public Stance on Cyberspace Issues. **Conflict Studies Research Centre**, 4 International Conference on Cyber Conflict, 2012b

GLENNY, Misha. McMafia: A Journey Through the Global Criminal Underworld. New York, Vintage Books: 2009 apudMAURER, T: Cyber Proxies and the Crisis in Ukraine. In: Geers, K (ed**.). Cyber War in Perspective: Russian Aggression Against Ukraine**. p.79-86NATO CCDCOEPublications. Tallinn 2015

HEICKERÖ, Roland. Emergin Cyber Threats and Russian Views on Information Warfare and Information Operations. **FOI, Swedish Defence Research Agency**. March 2010. http://www.foi.se/ReportFiles/foir_2970.pdf apudWEEDON, J: Beyond Cyber War: Russia´s use of Strategic Cyber Espionage and Information Operations in Ukraine. In: Geers, K (ed.). **Cyber War in Perspective: Russian Aggression Against Ukraine**. p.67-77NATO CCDCOE Publications. Tallinn. 2015

HOUNSHELL, Blake. The Revolution Will Be Tweeted: life in the vanguard of the new Twitter proletariat. **Foreign Policy**, 2011.

HUNTER, E., PERNIK, P: The Challenges of Hybrid Warfare. **ICDS Analysis**. 2014.

KELLO, Lucas .The Meaning of the Cyber Revolution: Perils to Theory and Statecraft, **International Security**, 2013.

LAWRENCE, Dune; RILEY, Michael. Hackers Target Hong Kong Protesters via iPhones. Bloomberg Business. Outubro 1, 2014 apudWEEDON, J: Beyond Cyber War: Russia´s use of Strategic Cyber Espionage and Information Operations in Ukraine. In: Geers, K (ed.). **Cyber War in Perspective: Russian Aggression Against Ukraine**. p.67-77NATO CCDCOE Publications. Tallinn. 2015

LIMNEL, Jarno. The Exploitation of Cyber Domain as Part of Warfare: Russo-krainian War. **International Journal of Cyber-Security and Digital Forensics**, vol 4, 2015 p.521-532

LYNCH, Marc. **The Arab Uprisings Explained**, Columbia Studies in Middle East Politics, p. 96, 2014.

LYNCH, Marc: The big think behind the Arab spring. **Foreign Policy**. V.190, p. 46, 2011.

LYNCH, M; FREELON, D; ADAY, S. Syria´s Socially Mediated Civil War. **United States Institute of Peace**, No. 91, 2014.

MAURER, T: Cyber Proxies and the Crisis in Ukraine. In: Geers, K (ed**.). Cyber War in Perspective: Russian Aggression Against Ukraine**. p.79-86NATO CCDCOEPublications. Tallinn 2015.

MILES, Donna. U.S European Command, NATO Boost Cyber Defenses, **American Force Press Service**, U.S. Department of Defense, Maio 18, 2012 apudLUCAS, Kello. The

Meaning of the Cyber Revolution: Perils to Theory and Statecraft, **International Security**, 2013

PHSYORG **A new defense for Navy ships: Protection from cyber attacks.**2015. Disponível em: <http://phys.org/news/2015-09-defense-navy-ships-cyber.html> acesso em: 10 de fevereiro 2016

RÁCZ, A: Russia´s Hybrid War in Ukraine: Breaking the Enemy´s Ability to Resist. **FIIA Report 43**. The Finnish Institute of International Affairs 2015.

REIS, L., BARROS, S. Internet e revolução no Egito: o uso de sites de redes sociais durante a convulsão social que derrubou o governo ditatorial egípcio em 2011. **XI Congresso Luso Afro Brasileiro de Ciências Sociais**, 7 a 10 de agosto, 2011.

SAKKOV, S. Foreword. In: Geers, K (ed.). **Cyber War in Perspective: Russian Aggression Against Ukraine.** NATO CCDCOE Publications. Tallinn 2015.

TUPTUK, N., HAILES, S. The cyberattack on Ukraine's power grid is a warning of what's to come. **PHYSORG**, 2016. Disponível em: <http://phys.org/news/2016-01-cyberattack-ukraine-power-grid.html>. Acesso em: 22 de abril de 2016.

VIEIRA, V. P. P: O papel da comunicação digital na arena internacional: Mobilização política online e a Primavera Árabe. **Boletim Meridiano 47**, vol. 14, n. 139, set.-out. 2013 [p. 24 a 30].

WEEDON, J: Beyond Cyber War: Russia´s use of Strategic Cyber Espionage and Information Operations in Ukraine. In: Geers, K (ed.). **Cyber War in Perspective: Russian Aggression Against Ukraine**. p.67-77NATO CCDCOE Publications. Tallinn. 2015.

YEUNG, C. Y: **A Critical Analysis on ISIS Media Strategies**.20 de março, 2015.

ZAMBELIS, Chris. Information Wars: Assessing the Social Media Battlefield in Syria. **The Combating Terrorism Center Sentinel**, Vol. 5, p.19, 2012.

Sites consultados:

Site da Fanpage “We Are All Khaled Said”: *https://www.facebook.com/elshaheeed.co.uk*

Site oficial do CNS: *http://ar.syriancouncil.org*

Site oficial do CNCMD: *http://www.ncsyria.com*

Site oficial do CCLS:*http://www.lccsyria.org*

Site oficial do OSDH: *http://www.syriahr.com*

Rede da Omawi News Live: *https://twitter.com/OmawiLive*

Disponível em: <http://cert.gov.ua/> Acesso em
Disponível em: <https://www.isightpartners.com/>
Disponível em: <https://www.symantec.com/>
Disponível: em: <http://www.bloomberg.com/news/articles/2014-10-01/hackers-target-hong-kong-protesters-via-iphones>
Disponível em: <https://www.ovh.pt/anti-ddos/principio-anti-ddos.xml> Acesso em 15.04.2016

Disponível em: <https://www2.fireeye.com/apt28.html> Acesso em 20.04.216