O que é 'guerra híbrida'. E por que o conflito atual é uma

Juliana Sayuri 28 de fevereiro de 2022 (atualizado 28/12/2023 às 22h22)

Enquanto tropas russas invadem o território ucraniano, internet fica instável no país devido a uma série de ataques cibernéticos

Desde o início da invasão russa à Ucrânia , a conectividade com a internet foi afetada principalmente no sul e no leste do território ucraniano, onde vêm sendo registrados confrontos mais intensos. A Embaixada da Ucrânia no Brasil informou neste domingo (27) que os canais oficiais da unidade também foram bloqueados por "ataques cibernéticos massivos" realizados pela Rússia.

O bilionário Elon Musk , fundador das empresas SpaceX e Tesla, anunciou a ativação de satélites de internet Starlink, da SpaceX . "O serviço Starlink agora está ativo na Ucrânia. Mais terminais a caminho", escreveu Musk, no Twitter , respondendo a um post do vice-premiê ucraniano Mykhailo Fedorov, no sábado (26). "Enquanto você tenta colonizar Marte , a Rússia tenta ocupar a Ucrânia", foi o tuíte de Fedorov a Musk. "Nós estamos criando um Exército de TI [tecnologia da informação]", Fedorov postou depois.

Também no sábado, o grupo hacker Anonymous declarou "guerra cibernética" contra a Rússia e exigiu a retirada das tropas de Vladimir Putin do território ucraniano; caso contrário, iniciaria ataques a sites do governo russo.

Neste texto, o Nexo explica qual o peso da internet e quais os impactos possíveis das ofensivas digitais no conflito entre Rússia e Ucrânia , que vem sendo caracterizado como uma "guerra híbrida" .

O que é guerra híbrida

Antes da invasão iniciada no dia 24 de fevereiro, a Ucrânia já vinha acusando o governo russo de deflagrar uma "guerra híbrida" mediante ataques cibernéticos contra sites oficiais do governo ucraniano.

Guerra híbrida se refere a um conflito que engloba estratégias e táticas para além de ações militares, como propaganda, difusão de fake news e ciberataques contra adversários políticos. O conceito foi cunhado no início da década de 2000 e foi empregado por autores para analisar contextos conturbados, por exemplo, no Brasil e na Ucrânia.

Ações dos Estados Unidos e a expansão da Otan (Organização do Tratado do Atlântico Norte) no Leste Europeu catalisaram o conflito entre Rússia e Ucrânia, avaliou o analista político norte-americano Andrew Korybko, autor de "Guerras híbridas: das revoluções coloridas aos golpes" (2018), em entrevista ao portal UOL publicada no dia 25 de fevereiro.

> "A guerra híbrida [...] é o paradoxal 'caos estruturado' [...] que está se tornando uma arma para satisfazer objetivos de política externa específicos. Isso faz dela tanto uma estratégia como uma arma"
>
> **Andrew Korybko**
> analista político, no livro "Guerras híbridas: das revoluções coloridas aos golpes" (2018)

Além de um confronto militar, o conflito atual seria híbrido por envolver uma ciberguerra, isto é, englobando ofensivas digitais e outras estratégias não convencionais. Não é a primeira vez que a Rússia é acusada de investir neste campo. As acusações sempre foram refutadas.

> "Um ataque tipificado como guerra híbrida, portanto, não é algo daquele cenário que envolve tanques e soldados em fronts de batalha. Na vertente que estamos assistindo, trata-se de algo que se produz no campo de uma guerra 'informacional' [...]"
>
> **Piero Leirner**
> professor de antropologia no livro "O Brasil no espectro de uma guerra híbrida" (2020)

Histórico

2022

Antes da invasão, a Rússia já era acusada de investir em uma campanha massiva de sabotagens e ataques cibernéticos para minar o governo do presidente ucraniano, Volodymyr Zelensky. Em janeiro de 2022, a Ucrânia e a Otan assinaram um acordo de cooperação cibernética , após um ataque deixar vários sites do governo fora de serviço. Na época, os Estados Unidos declararam que a Rússia estaria preparando uma operação de sabotagem que poderia servir de "pretexto" para uma invasão. A embaixadora dos Estados Unidos na Otan, Julianne Smith, disse à imprensa que, entre os possíveis desdobramentos das tensões entre Rússia e Ucrânia, considerava-se um ataque militar "e outros níveis" .

2021

Os Estados Unidos declararam estado de emergência temporário após um ataque com vírus do grupo hacker DarkSide paralisar o fluxo de combustível ao desconectar a rede e roubar mais de 100 gigabytes de informações do oleoduto da empresa Colonial Pipeline, em maio de 2021. O presidente Joe Biden acusou um grupo de hackers ativo na Rússia da autoria do ataque, mas não atribuiu a responsabilidade ao governo de Vladimir Putin. "Até agora não há evidências, por parte de nossa equipe de inteligência, de que a Rússia esteja envolvida, embora haja evidências de que os atores, o 'ransomware', estão na Rússia", declarou Biden.

Histórico

2017

Diversas empresas e instituições pelo mundo foram atacadas por um novo tipo de vírus, identificado como Petya ou NotPetya , que destrói informações de computadores. As primeiras notícias vieram da Ucrânia, onde foram afetados aeroportos, centrais de tráfego, usinas e até o Banco Central do país, alvo de 60% das infecções do vírus. Também foram afetadas empresas na Europa, nos Estados Unidos e até no Brasil. Não foi possível identificar com certeza quem estava por trás do ciberataque, mas, segundo uma reportagem da revista "Wired", eram fortes os indícios de intenção de atingir especialmente a Ucrânia. "Foi direcionado para nós. Não foi um ato criminoso comum. É provavelmente bancado por algum Estado. É difícil imaginar qualquer outro [que não a Rússia] que faria isso", disse então o diretor do Centro de Ciberdefesa da Ucrânia, Roman Boyachurk.

2015

A Ucrânia foi alvo do primeiro hackeamento bem-sucedido contra uma rede elétrica no mundo. Num ataque supostamente coordenado por hackers russos, um vírus, identificado como BlackEnergy, desligou a energia elétrica de milhares de casas em dezembro de 2015. Outros ocorreram em 2016 e 2017 – entre eles, um na usina nuclear Wolf Creek, no estado norte-americano do Kansas, segundo o FBI, também coordenado por ciberativistas a partir de território russo.

2014

A Ucrânia acusou a Rússia de ter bloqueado comunicações da companhia telefônica Ukrtelecom , na Crimeia, onde avançavam tropas russas. Em maio de 2014, os grupos hackers pró-Ucrânia Cyber Hundred e Null Sector atacaram sites e o Banco Central da Rússia. Ao mesmo tempo, o grupo hacker pró-Rússia Cyber Berkut violou o sistema central da comissão eleitoral para tentar apagar dados da disputa presidencial na Ucrânia.

A autoria de ataques, entretanto, é difícil de precisar, assim como o vínculo de hackers com os Estados. "Se você lança um míssil, sabe-se de onde saiu e quem o construiu. No mundo da internet não é assim: é complicadíssimo saber de onde vêm os ataques e quem está por trás", definiu Luis Corrons, analista de segurança do antivírus Avast, em entrevista ao jornal espanhol El País.

Além de invasões digitais, a Rússia também foi acusada de "orquestrar" junto a Belarus uma crise na Lituânia e na Polônia (integrantes da União Europeia) mediante fluxos migratórios : estrangeiros vindos principalmente do Oriente Médio estavam passando pelo território bielorrusso para entrar livremente na Europa através da fronteira da Polônia.

Belarus e Ucrânia são os únicos países na fronteira oeste da Rússia que não foram incorporados à Otan. Na época, o governo lituano disse que os imigrantes estavam sendo usados como uma "arma política". A presidente da Comissão Europeia, Ursula von der Leyen, disse que a UE estava enfrentando um "ataque híbrido cínico e perigoso".

O impacto de ofensivas digitais

Os russos foram acusados de lançar campanhas de desinformação na internet ucraniana e de usar a tática para tentar influenciar eleições estadunidenses, que levaram Donald Trump ao poder , em 2016.

Já os Estados Unidos foram acusados de realizar uma campanha digital para sabotar o Irã , onde a rede de computadores de uma usina nuclear foi danificada por um vírus, em 2010; e de tentar hackear a rede elétrica da Rússia , em 2019, entre outras iniciativas.

Diante do conflito na Ucrânia, Joe Biden também considera responder a ciberataques se a Rússia atingir digitalmente os Estados Unidos, segundo a rede de TV americana NBC News. "Se a Rússia realizar ciberataques contra nossas companhias, nossa infraestrutura crítica, nós estamos preparados para responder" , declarou.

Ciberataques, também conhecidos como APT (ameaça persistente avançada), podem afetar acesso a internet, abastecimento energético, infraestruturas físicas e instituições financeiras, entre outras. Podem comprometer ainda mais o acesso à informação dos indivíduos.

"É importante lembrar o componente psicológico da guerra, que pode ser impactado enormemente pelas operações cibernéticas. Imagine o quão perdido você se sentiria se a guerra estivesse em andamento e, de repente, você não pudesse ligar para sua família ou acessar a internet para receber atualizações sobre a invasão", assinalou Luca Belli, coordenador do Centro de Tecnologia e Sociedade da FGV Direito Rio, ao jornal Folha de S.Paulo.

"É possível, e até provável, que sistemas de energia, telecomunicações e redes de internet sejam severamente interrompidos para criar caos durante a invasão", disse Belli.

Em paralelo, plataformas de mídia e tecnologia também estão sendo pressionadas, tanto por ucranianos e norte-americanos quanto por russos . Alphabet (empresa responsável por Google e YouTube), Meta (que reúne Facebook, Instagram e WhatsApp) e Twitter suspenderam ferramentas de impulsionamento pago, publicidade e monetização de veículos como Russia Today e Sputnik , acusadas de propagar desinformação para justificar a guerra. Em resposta, a Rússia restringiu o acesso a Facebook e Twitter no domingo (27).

Link para matéria:
https://www.nexojornal.com.br/expresso/2022/02/28/O-que-%C3%A9-%E2%80%98guerra-h%C3%ADbrida%E2%80%99.-E-por-que-o-conflito-atual-%C3%A9-uma?posicao-home-direita=3

BBC NEWS BRASIL

O que é guerra híbrida? Por dentro do centro de estudos que investiga ameaça

Frank Gardner
Role,Repórter de Segurança da BBC News
18 fevereiro 2023

Fortes explosões subaquáticas no Mar Báltico abriram enormes buracos nos gasodutos Nord Stream entre a Dinamarca e a Suécia

Explosões subaquáticas misteriosas, ataques cibernéticos anônimos e campanhas online para minar democracias ocidentais: tudo isso é considerado um tipo de "ameaça híbrida".

A BBC visitou um centro dedicado a combater essa forma relativamente nova de guerra que preocupa cada vez mais a Organização do Tratado do Atlântico Norte (Otan) e a União Europeia.

"Trata-se da manipulação do espaço da informação. Trata-se de ataques à infraestrutura crítica", explica Teija Tiilikainen , diretora do Centro Europeu de Excelência para Combate a Ameaças Híbridas (Hybrid CoE, na sigla em inglês), criado há seis anos em Helsinque, capital da Finlândia.

Ela explica que esse formato de ameaça é ambíguo, e por isso é muito difícil para os países se protegerem.

Ameaças reais

Mas essas ameaças não são ficção.

Em setembro do ano passado, fortes explosões subaquáticas no Mar Báltico abriram buracos enormes nos gasodutos Nord Stream, entre as costas dinamarquesa e sueca. Os gasodutos foram construídos para transportar gás russo para o norte da Alemanha.

Moscou negou imediatamente qualquer envolvimento nas explosões, mas autoridades de países ocidentais suspeitam que se tratava de um plano para sabotar o suprimento de energia do Ocidente. O motivo seria o apoio ocidental à Ucrânia após a invasão russa em fevereiro do ano passado.

Também houve episódios de interferência eleitoral. Pouca gente se deu conta na época, mas após a eleição de 2016 nos Estados Unidos, investigadores concluíram que houve interferência russa – novamente negada por Moscou – com o objetivo de reduzir as chances de Hillary Clinton contra Donald Trump.

A Rússia teria usado "bots" (robôs) online — contas artificiais de rede social controladas por ativistas apoiados pelo governo russo, a partir de "fábricas de trolls" em São Petersburgo.

Outra amaça híbrida é a desinformação: a propagação intencional de uma narrativa falsa, muitas vezes atraente para certos setores mais receptivos da população.

Este fenômeno se acelerou desde a invasão russa da Ucrânia, com milhões de cidadãos — não apenas na Rússia, mas também em países ocidentais — aceitando a narrativa do Kremlin de que a invasão foi um ato necessário de autodefesa.

As ameaças híbridas incluem sabotagem subaquática, uma preocupação crescente no Mar Báltico

Território neutro

Para ajudar os governos ocidentais a identificar e se proteger contra essas ameaças, a Otan e a União Europeia criaram o Hybrid CoE na Finlândia.
O país é uma escolha interessante e talvez natural para um centro deste tipo. A Finlândia permaneceu neutra desde a Segunda Guerra Mundial, quando cedeu território à antiga União Soviética.

Os dois países compartilham uma fronteira de 1,3 mil quilômetros. Agora, apreensiva, a Finlândia tem se aproximado cada vez mais do Ocidente, o que culminou com seu pedido de adesão à Otan no passado.

Em uma manhã fria e com neve, visitei o centro, localizado em um edifício comercial perto do Ministério da Defesa, a uma curta distância da embaixada russa, um prédio cinzento da era soviética.
Lá, Teija Tiilikainen lidera uma equipe de cerca de 40 analistas e especialistas de vários países da Otan e da União Europeia, incluindo um cidadão britânico "emprestado" do Ministério da Defesa em Londres.
Tiilikainen diz que uma área de preocupação é o Ártico, onde foi detectado um grande potencial de ameaças híbridas.

BBC NEWS BRASIL

""Novas fontes de energia estão surgindo", explica. "Há novas possibilidades para as grandes potências protegerem seus interesses. Há também muita manipulação de informação."

"A narrativa russa é que o Ártico é uma região especial à margem conflitos, onde nada de ruim acontece. E, mesmo assim, Rússia está construindo um exército ali."

Ataques sutis, mas perigosos

Talvez a principal característica das ameaças híbridas seja que elas quase nunca envolvem um ataque real, ou seja, alguém abrindo fogo com uma arma. Elas são mais sutis, mas não menos perigosas.
Muitas vezes é difícil determinar quem está por trás desses atos, como o grande ciberataque de 2007 contra a Estônia ou as explosões de gasodutos no ano passado no Báltico.

Os responsáveis têm o cuidado de deixar o mínimo possível de rastros.

Há inúmeras maneiras de um Estado prejudicar outro sem recorrer à ação militar direta.

Isso é ilustrado por um manual redigido pelo centro, no qual são descritas as ameaças híbridas marítimas. O documento contém 10 cenários imaginários, mas todos muito plausíveis.

Eles vão desde o uso clandestino de armas subaquáticas até a declaração de uma zona de controle ao redor de uma ilha, passando por bloqueio de estreitos.

Um cenário real analisado em detalhes foi a ação da Rússia no Mar de Azov antes da invasão da Ucrânia.

Desde outubro de 2018, os navios ucranianos que saíam dos portos de Mariupol e Berdyansk precisavam fazer fila para serem inspecionados pelas autoridades russas se quisessem navegar pelo Estreito de Kerch e chegar no Mar Negro.

Esse trâmite — segundo Jukka Savolainen, diretor de vulnerabilidades e resiliência do Hybrid CoE— poderia durar dias ou até duas semanas, o que causava prejuízos econômicos à Ucrânia.

A Rússia conseguiu vencer a guerra de informação entre setores significativos da população no que se refere à invasão da Ucrânia

Guerra de informação

Mas é no campo da desinformação que os especialistas do centro encontraram os resultados mais surpreendentes.
Depois de reunir e avaliar inúmeras pesquisas de opinião em toda a Europa, eles concluíram que em vários países da Otan, a Rússia está ganhando a guerra de informação entre setores significativos da população.

Na Alemanha, por exemplo, a versão do Kremlin de que o ataque à Ucrânia foi uma reação necessária à provocação da Otan vem ganhando popularidade à medida que a guerra avança.

Na Eslováquia, mais de 30% dos entrevistados acreditam que a guerra na Ucrânia foi provocada deliberadamente pelo Ocidente. Na Hungria, 18% atribuíram a guerra à "opressão da população de língua russa na Ucrânia".

"Eu não avaliaria a desinformação russa como especialmente sofisticada", explica Jakub Kalensky, analista da República Tcheca.

"Não é a mensagem que tem apelo, mas a quantidade."

Tiilikainen explica que o papel do centro não é tomar medidas para combater as ameaças híbridas — mas, sim, avaliar, informar e treinar outros para fazer o que for necessário para proteger a Europa desse fenômeno crescente.