Guerra Cibernética e Terrorismo Cibernético: uma Análise da invasão Russa na Ucrânia.

Eduardo de Souza CUNHA[1]

Recibido: 13 de mayo de 2024; Aceptado: 02 de julio de 2024.
Eduardo de Souza CUNHA. "Guerra Cibernética e Terrorismo Cibernético: uma Análise da invasão Russa na Ucrânia." *Hemisferio Revista del Colegio Interamericano de Defensa* 10 (2024): 7-25. https://doi.org/10.59848/24.1207.HV10n1

Resumo:

Este artigo examina a complexa interseção entre guerra cibernética e terrorismo cibernético, utilizando como estudo de caso a invasão da Ucrânia pela Rússia e os ataques cibernéticos subsequentes. Buscar-se-á explorar brevemente o contexto histórico, assim como as motivações por trás dos ataques e os efeitos sobre a população civil e as infraestruturas críticas. Serão abordados os efeitos cibernéticos cinéticos e não cinéticos sofridos pela Ucrânia, destacando a necessidade de uma compreensão mais profunda desses fenômenos e de estratégias mais eficazes para mitigação dos seus impactos. Ao final, buscar-se-á entender a correlação e peculiaridades da Guerra Cibernética e do Terrorismo Cibernético.

Palavras Chave: Guerra Cibernética - Terrorismo Cibernético - Invasão da Ucrânia - População Civil - Infraestruturas Críticas

Abstract:

This article examines the complex intersection between cyber warfare and cyber terrorism, using the Russian invasion of Ukraine and the subsequent cyber attacks as a case study. It will briefly explore the historical context, the motivations behind the attacks, and the effects on the civilian population and critical infrastructure. The article will address both kinetic and non-kinetic cyber effects experienced by Ukraine, highlighting the need for a deeper understanding of these phenomena and more effective strategies for mitigating their impacts. In conclusion, it will seek to understand the correlation and peculiarities of Cyber Warfare and Cyber Terrorism.

[1] O autor é Oficial do Exército Brasileiro com mais de 33 anos de serviço, tendo atuado como Subchefe do Estado-Maior do Comando de Defesa Cibernética do Brasil. Com Mestrado em Ciências Militares, atualmente é professor de Segurança Cibernética no Colégio Interamericano de Defesa. Ao longo de sua carreira, tem se dedicado à proteção das infraestruturas críticas nacionais e à formação de novos profissionais na área de segurança cibernética. Contato: eduardo.cunha@iadc.edu. https://orcid.org/0009-0008-7060-7840

***Keywords**: Cyber Warfare - Cyber Terrorism - Ukraine Invasion - Civilian Population - Critical Infrastructure*

Introdução:

Há algum tempo tem-se tornado cada vez mais complexa a profundidade das ameaças cibernéticas como os crimes, a espionagem e o hacktivismo. Porém, duas delas, até fruto da minha natureza militar, me chamam mais a atenção: a Guerra e o Terrorismo cibernéticos. A linha que separa esses dois ramos da cibernética é muito tênue. Entre elas está a população civil que se serve dos serviços oferecidos pelas infraestruturas críticas e mais sofrem quando essas são impactadas.

A era digital trouxe consigo para sociedade uma série de benefícios, mas por outro lado, junto a elas novos desafios e ameaças, as quais se incluem a guerra cibernética e o terrorismo cibernético. A invasão da Ucrânia pela Rússia, em conjunto com os ataques cibernéticos direcionados, oferece um bom exemplo vívido das interações complexas entre esses fenômenos e seus efeitos sobre a segurança internacional.

Durante a invasão, especificamente no período compreendido entre os anos de 2022 e 2024, e mesmo antes desse, uma série de ataques cibernéticos foi perpetrada contra infraestruturas críticas e sistemas de comunicação ucranianos. Esses ataques tinham por objetivo a desorganização da comunicação e coordenação militar, desestabilização do governo ucraniano e minar a confiança da população nas instituições governamentais, além de espionagem, inteligência, propaganda e guerra psicológica.

Os ataques cibernéticos perpetrados pela Rússia durante a invasão da Ucrânia foram diversificados e altamente coordenados, o que sinaliza um planejamento prévio e reforça o emprego da arma cibernética como novo e importante elemento no combate. Eles incluíram não só ataques de Negação de Serviço (Distributed Denial of Service, DDoS) contra infraestruturas de comunicação e sites governamentais, bem como ataques direcionados a redes elétricas e sistemas de controle industrial. Esses ataques tinham por objetivos minar a capacidade da Ucrânia de se comunicar, coordenar uma resposta militar eficaz e manter a estabilidade interna.

Esses ataques cibernéticos tiveram consequências significativas para a população civil e as infraestruturas críticas ucranianas. As interrupções nos serviços de comunicação dificultaram a coordenação das operações militares e a disseminação de informações

precisas para o público. Além disso, os ataques contra redes elétricas e sistemas de controle industrial causaram cortes de energia em áreas críticas, afetando negativamente hospitais, instalações de água e outros serviços essenciais.

Como conclusão parcial, fica latente que os objetivos dos ataques cibernéticos russos durante a invasão da Ucrânia eram multifacetados, buscando alcançar vantagens militares, políticas e psicológicas para facilitar os esforços de guerra da Rússia e minar a resistência ucraniana. A proposta desse Artigo é tentar compreender o uso da arma cibernética em alvos militares e seus impactos na população civil se pode ser considerado como um ato terrorista ou não, concluindo sobre a importância na atribuição e classificação de ataques cibernéticos e como podemos agir para mitigar ou dissuadir essas ações.

Breve Histórico:

As relações entre Rússia e Ucrânia têm sido historicamente complexas, marcadas por tensões políticas, étnicas e territoriais. Fato relevante e recente para isso foi a anexação da Crimeia pela Rússia em 2014, que exacerbou essas tensões, levando a um conflito armado no leste da Ucrânia entre forças pró-russas e ucranianas.

A escalada da guerra cibernética entre Rússia e Ucrânia teve início em 2014, como desdobramento do conflito mais amplo entre esses dois países. A crise política na Ucrânia teve início após o então presidente Viktor Yanukovych recusar-se a assinar um acordo comercial com a União Europeia em novembro de 2013, resultando em uma deterioração da situação política no país. Em fevereiro de 2014, tropas russas ocuparam a Crimeia, enquanto uma série de ciberataques coordenados interromperam os serviços de telecomunicações e sites governamentais ucranianos.

Os ataques cibernéticos prosseguiram com diferentes graus de intensidade, envolvendo invasões de sistemas, interrupções de serviços online e vazamentos de informações confidenciais. Grupos de hackers pró-Ucrânia e pró-Rússia, como "Cyber Hundred", "Null Sector" e "CyberBerkut", estiveram ativos em diferentes momentos, conduzindo ataques DDoS e comprometendo sistemas de informação.[2]

[2] Ronaldo Oliveira de Souza et al., “Guerra híbrida e ciberconflitos: uma análise das ferramentas cibernéticas nos casos da síria e conflito rússia-ucrânia” (Revista eletrônica Estácio Recife, 2019), 6-17.

Antes mesmo da escalada para a guerra entre Rússia e Ucrânia, as atividades cibernéticas desempenharam um papel fundamental na competição e nos conflitos entre esses dois países. A Rússia empregou operações cibernéticas ofensivas (OCO) como parte de sua estratégia de guerra irregular, buscando desestabilizar a Ucrânia e influenciar a opinião pública a seu favor. Isso incluiu ataques distribuídos de DDoS e a alteração de sites para controlar a narrativa pró-Rússia e prejudicar a capacidade do governo ucraniano de operar eficazmente.

Por sua vez, a Ucrânia também se engajou em operações de informação, utilizando plataformas de mídia social, televisão e redes sociais para promover uma narrativa alternativa e resistir às ações russas. Essas atividades cibernéticas faziam parte de um ambiente informacional mais amplo, onde a rivalidade entre os dois países se transformou em conflito armado em 2022. A interseção entre o domínio cibernético e o físico tornou-se evidente, com a ciberguerra sendo uma extensão das operações no campo de batalha convencional.[3]

Dessa forma, podemos dizer então que as complexas relações entre Rússia e Ucrânia, exacerbadas pela anexação da Crimeia em 2014, desencadearam um conflito armado no leste da Ucrânia e uma escalada da guerra cibernética entre os dois países. Desde então, os ataques cibernéticos têm sido uma parte crucial das estratégias de ambos os lados, refletindo não apenas uma rivalidade política, mas também se tornando uma extensão das hostilidades no campo de batalha convencional.

Formas de ataques:

Os ataques cibernéticos levados a efeito pela Rússia podem ser entendidos dentro do contexto mais amplo das estratégias militares e políticas do Kremlin. Além de objetivos militares convencionais, como minar a capacidade de defesa da Ucrânia, os ataques cibernéticos também visavam desestabilizar a sociedade ucraniana e minar a confiança nas instituições governamentais.

[3] Defibaugh, "Past and Present Russian Information Operations in Ukraine: Competition into Conflict", Anais da 19ª Conferência Internacional sobre Guerra Cibernética e Segurança, ICCWS 2024, 64-65.

Atualmente, a "zona cinzenta" e ou "guerra híbrida", que são ações ou estratégias que ficam entre a paz e a guerra aberta. Essas atividades são deliberadamente ambíguas e difíceis de atribuir, projetadas para obter vantagens sem desencadear uma resposta militar convencional. Elas representam uma evolução nas formas de conflito contemporâneas, caracterizadas pela ambiguidade, complexidade e integração de uma variedade de métodos e técnicas de guerra. Esses conceitos desafiam as noções tradicionais de segurança e exigem respostas adaptativas e multidimensionais por parte das instituições estatais e internacionais.

Na zona cinzenta dos conflitos pós-Guerra Fria, uma variedade de ferramentas e táticas tem sido empregadas para conduzir atividades que se encontram entre a paz e uma guerra declarada. Essas ferramentas e táticas são empregadas de forma gradual por atores estatais e não estatais, combinando elementos militares e não militares. O objetivo tem sido em geral de minar, desestabilizar, enfraquecer ou atacar um adversário, muitas vezes explorando as vulnerabilidades do estado-alvo.[4]

Nesse mister, os ataques cibernéticos conduzidos pela Rússia em apoio às operações militares, mesmo antes da invasão, mas sobretudo com grande intensidade no dia “D”, foram conduzidos de forma organizada e planejada, a fim de atingir principalmente objetivos estratégicos. Dentre elas, podemos destacar as principais formas de ataque cibernético perpetrados pela Rússia e seus objetivos militares:

- Ataques de DDoS: visavam sobrecarregar e inutilizar sistemas de comunicação e infraestrutura de defesa ucraniana, dificultando a coordenação e a resposta militar.

- Infiltração e Espionagem Cibernética: tinham por objetivo principal obter informações confidenciais e estratégicas sobre as capacidades militares e planos de defesa da Ucrânia.

- Ataques de Ransomware: visavam paralisar instituições e setores estratégicos da Ucrânia, como governamentais e de infraestrutura crítica, de formas a desestabilizar o país e minar sua capacidade de resposta militar.

[4] Henrique et al., “OSINT e relações internacionais: o caso dos militares russos em Donbas entre 2014 e 2021” Revista Brasileira de Estudos Estratégicos REST V15 Nº29 (Jan-Jun 2023), 70-92.

- Desinformação e Manipulação de Mídia: um dos mais empregados, visavam influenciar a opinião pública nacional e internacional, distorcendo a narrativa do conflito e minando o apoio à Ucrânia, enquanto promoviam a agenda russa.

- Ataques a Infraestrutura Crítica: interrupção de serviços essenciais, como eletricidade, água e transporte, visando desestabilizar a população e prejudicar as capacidades de defesa e resposta da Ucrânia.

- Ataques de Engenharia Social: enganar e manipular funcionários e oficiais ucranianos para obter acesso não autorizado a sistemas e informações sensíveis, comprometendo a segurança nacional.

- Ataques de wiper: os ataques "wiper" podem ter sido usados para interromper a infraestrutura crítica da Ucrânia, como sistemas de energia, transporte e comunicação. Ao destruir dados e comprometer sistemas, esses ataques podem ter causado danos significativos com consequências não só para o governo ucraniano, mas sobretudo para população civil.

Nesse sentido, um exemplo interessante ocorrido em 2022 foi que um ataque cibernético mirado contra uma estação elétrica na Ucrânia desencadeou um apagão não planejado. Este evento acarretou consequências significativas não apenas para a infraestrutura elétrica ucraniana, mas também para a segurança nacional e a percepção global sobre a vulnerabilidade das infraestruturas críticas.[5]

O ataque destacou a habilidade de grupos de hackers, possivelmente respaldados por estados ou atores não estatais com agendas geopolíticas, de infligir danos consideráveis através de ataques cibernéticos direcionados. Essa situação ressaltou a importância de salvaguardar as infraestruturas críticas contra ameaças cibernéticas e a necessidade de adotar medidas de segurança mais sólidas e vigilantes.

A resposta a esse incidente não se limitou apenas à restauração da energia afetada, mas também incluiu uma investigação meticulosa para identificar os responsáveis e avaliar a extensão dos danos causados. Adicionalmente, estimulou um debate

[5] Mueller et al., “Cyber Operations during the Russo-Ukrainian War From Strange Patterns to Alternative” Center for Strategic and International Studies (CSIS), julho 2023, 15-26.

internacional sobre a segurança cibernética das infraestruturas críticas em escala global, resultando em uma maior conscientização e implementação de medidas preventivas.

Em última análise, esse episódio serviu como um alerta para a comunidade internacional sobre os riscos crescentes associados à guerra cibernética e a necessidade premente de uma cooperação mais estreita entre os países para enfrentar esses desafios em matéria de segurança cibernética.

Podemos concluir parcialmente que os ataques cibernéticos durante a invasão da Ucrânia pela Rússia são parte de estratégias militares e políticas mais amplas, visando desestabilizar a sociedade ucraniana e minar a confiança nas instituições governamentais. Esses ataques demonstram a complexidade da "zona cinzenta" e da "guerra híbrida", desafiando conceitos tradicionais de segurança. Os objetivos dos ataques incluem negação de serviço, manipulação de mídia e interrupção de infraestrutura crítica.

Efeitos sobre a População Civil nos ataques às Infraestruturas Críticas:

Os impactos dos ataques cibernéticos às infraestruturas críticas ucranianas trouxeram consequências graves para população civil, pois causaram perturbações em serviços primordiais, tais como energia e comunicações. Essas ações também acarretaram prejuízos econômicos e emocionais, uma vez que a falta de informações, seja pela mídia tradicional ou mesmo pelas novas redes sociais, comprometeram a estabilidade nacional e agravaram a situação humanitária. Tente se colocar na situação em que seu país é atacado por uma Força militar estrangeira e as poucas informações que chegam são muitas vezes incorretas. Poderia isso ser considerado um ato terrorista?

Vimos anteriormente que os ataques cibernéticos às infraestruturas críticas ucranianas tinham objetivos militares e estratégicos. Uma pergunta que se deve fazer então é no sentido de procurar entender se houve por parte da Rússia uma judiciosa análise de riscos. A análise de riscos em operações cibernéticas é fundamental para compreender as potenciais consequências e impactos das ações realizadas. No contexto das operações contra infraestruturas críticas, essa avaliação envolve considerar a possibilidade de retaliação, escalada do conflito, repercussões diplomáticas e o impacto na população civil, entre outros fatores relevantes.

No caso específico dos momentos em que se sucederam as invasões por tropas russas os ataques perpetrados às infraestruturas críticas da Ucrânia causaram um impacto devastador na população civil, manifestando-se em diversas áreas, tais como:

- Perda de serviços essenciais: hospitais, escolas, residências e empresas foram privadas de eletricidade, água, aquecimento e comunicação. Esse cenário acarretou considerável sofrimento e privação das necessidades básicas das pessoas.

- Interrupções na economia: os ataques tiveram um efeito severo na economia ucraniana, interrompendo cadeias de suprimentos, operações comerciais e transporte. Isso resultou em um aumento do desemprego, da pobreza e da insegurança econômica.

- Crise humanitária: milhões de indivíduos foram obrigados a deixar suas residências devido aos conflitos e à destruição da infraestrutura. Como resultado, uma grande crise humanitária emergiu, com muitos ucranianos lutando para acessar alimentos, abrigo e assistência médica.

- Impacto ambiental: os ataques também provocaram danos ambientais significativos, incluindo vazamentos de substâncias químicas perigosas e incêndios em refinarias de petróleo. Tais incidentes terão implicações de longo prazo para a saúde pública e o meio ambiente da Ucrânia.

O Relatório de 2022 da Microsoft traz as primeiras lições da guerra cibernética no estudo de caso da Ucrânia. Durante a guerra, houve relatos de ataques cibernéticos coordenados com ataques de mísseis contra ferrovias e sistemas de transporte que transportavam armas e suprimentos militares. Esses ataques visavam interromper as operações logísticas e prejudicar a capacidade de movimentação de recursos essenciais, afetando indiretamente a população civil que dependia desses sistemas para transporte e abastecimento.

Outro relato do referido relatório diz que os militares russos direcionaram ataques cibernéticos destrutivos do tipo wipers às redes informáticas locais do governo ucraniano. Esses ataques visavam comprometer a infraestrutura digital do governo, potencialmente causando interrupções nos serviços públicos e nas operações governamentais, o que impactou a população civil que dependia desses serviços.

Porém, os ataques com maiores efeitos negativos para população foram no setor de energia e finanças. A Ucrânia foi alvo de ataques cibernéticos que resultaram em cortes de energia em várias regiões do país. Esses ataques comprometeram a infraestrutura da

rede elétrica, causando interrupções no fornecimento de eletricidade para residências, empresas e serviços essenciais. A falta de eletricidade teve impactos graves na vida cotidiana da população, afetando a iluminação, o aquecimento, a refrigeração de alimentos e a operação de equipamentos essenciais.

Durante a guerra, também houve relatos de ataques cibernéticos direcionados a ativos financeiros na Ucrânia. Esses ataques podem ter visado instituições financeiras, sistemas de pagamento e outras infraestruturas relacionadas ao setor financeiro. A interrupção ou comprometimento desses ativos financeiros causaram instabilidade econômica, perda de fundos e impactaram negativamente a população civil que dependia desses serviços para transações financeiras e acesso a recursos financeiros.[6]

Apesar de não ser um ataque específico a infraestrutura crítica, existe um campo em que a Rússia já trabalha a muito tempo em todo mundo que é o da desinformação. No caso específico foram identificadas campanhas de desinformação russa durante a guerra cibernética na Ucrânia. Essas campanhas visavam disseminar narrativas falsas e enganosas para manipular a opinião pública e influenciar a percepção dos eventos em curso. As campanhas de desinformação russa envolveram a amplificação de narrativas falsas por meio de sites patrocinados pela Rússia, que publicavam histórias promovendo uma determinada narrativa.

Conclui-se então que os ataques cibernéticos às infraestruturas críticas na Ucrânia causaram danos graves à população civil, incluindo interrupções nos serviços essenciais, prejuízos econômicos e uma crise humanitária emergente. A coordenação entre ataques cibernéticos e cinéticos levanta questões sobre a análise de riscos por parte da Rússia. Danos ambientais, cortes de energia e ataques financeiros ilustram o impacto generalizado sobre a vida cotidiana. As campanhas de desinformação russa agravaram a situação. Esses eventos destacam a necessidade urgente de proteger infraestruturas críticas e a população civil contra ameaças cibernéticas e suas consequências humanitárias.

[6] Brad Smith, “Defending Ukraine: Early Lessons from the Cyber War”, Microsoft, (Junho 2022), 10-27.

Guerra Cibernética e Terrorismo Cibernético:

A distinção entre guerra cibernética e terrorismo cibernético nesse contexto é complexa. Enquanto alguns ataques tinham como objetivo principalmente alvos militares e infraestrutura crítica, os efeitos sobre a população civil e a motivação para instilar o medo e o caos também refletem em elementos de terrorismo cibernético. Faz-se necessário então definir o que é Terrorismo, Guerra Cibernética e Terrorismo Cibernético.

O terrorismo é uma forma de violência política que busca gerar medo, intimidação e coerção através do uso deliberado de violência contra civis ou não combatentes. Geralmente, os atos terroristas são realizados por grupos ou indivíduos com motivações políticas, ideológicas, religiosas ou sociais, com o objetivo de promover uma agenda específica, desestabilizar governos ou sociedades, ou causar impacto emocional e psicológico.[7]

O ciberterrorismo é uma forma específica de terrorismo que envolve o uso de ataques cibernéticos, como hacking, malware, DDoS e outras técnicas de ciberataque, com o objetivo de causar danos, instilar medo e atingir objetivos políticos, sociais ou ideológicos. O ciberterrorismo combina elementos do terrorismo tradicional com o uso de tecnologia da informação e comunicação para realizar ataques.

O ciberterrorismo é ainda definido como a utilização de ativos computacionais e outras tecnologias de informação e comunicação para conduzir ataques terroristas ou promover causas terroristas. Esses ataques podem incluir a disseminação de propaganda, roubo ou manipulação de dados e a perturbação de infraestruturas críticas. Em outra análise o ciberterrorismo envolve ameaçar ou causar danos corporais para obter poder político ou ideológico através de ameaça ou intimidação. Perceba-se que nessa definição não há o componente militar.

O impacto do ciberterrorismo na sociedade pode ser devastador. Pode resultar em perdas financeiras, perdas de vidas, danos à reputação e perda de estabilidade. Além disso, o ciberterrorismo pode afetar a economia de uma nação, causar instabilidade política e gerar medo e ansiedade na população. A interrupção de infraestruturas vitais, como redes

[7] Usman et al., "Cyber-warfare Versus Cyber-terrorism: An Emerging 21st Century Trend", Journal of Politics and International Studies, (10 de dezembro de 2023), 149-155.

de transporte, redes elétricas e redes bancárias, é um dos maiores efeitos desse tipo de ataques cibernéticos.[8]

A guerra cibernética é uma forma de conflito que ocorre no ciberespaço, envolvendo ataques e operações realizadas por meio de sistemas de computadores e redes digitais. Nesse contexto, a guerra cibernética se concentra em explorar e comprometer sistemas de informação e comunicação para obter vantagens estratégicas, causar danos, interromper operações inimigas e promover objetivos militares, políticos ou econômicos.

Do que foi pesquisado até aqui, a grande pergunta se as ações de Guerra Cibernética promovidas pela Rússia durante a invasão da Ucrânia podem ser consideradas também como Terrorismo Cibernético não possui um consenso, pois está sujeita às diversas interpretações. Vejamos.

Não é incomum que governos e entidades estatais sejam acusados de envolvimento em atividades cibernéticas que possam ser consideradas como ciberterrorismo. No caso da Rússia e sua relação com a Ucrânia, houve alegações e evidências de ataques cibernéticos e operações de desinformação que visavam desestabilizar o país vizinho.

Durante a invasão da Crimeia pela Rússia em 2014 e o conflito contínuo no leste da Ucrânia, houve relatos de ciberataques contra infraestruturas críticas, sistemas de comunicação e redes governamentais ucranianas. Além disso, a disseminação de desinformação e propaganda online também foi uma estratégia utilizada para influenciar a opinião pública e minar a estabilidade do país.

Embora não haja um consenso universal sobre a definição de terrorismo cibernético e suas ramificações legais, as ações cibernéticas da Rússia durante o conflito com a Ucrânia podem ser interpretadas como parte de uma estratégia mais ampla de guerra híbrida, que inclui elementos cibernéticos, de informação e militares.

É importante ressaltar que a atribuição de responsabilidade por ataques cibernéticos, que é uma etapa fundamental, é um processo complexo que envolve investigações detalhadas, análise forense digital e cooperação internacional. As relações

[8] Iftikhar, “Cyberterrorism as a global threat: a review on repercussions and countermeasures”, Faculty of Computer Studies, Arab Open University, Riyadh, Saudi Arabia (15 de janeiro de 2024), 3-32.

entre Rússia e Ucrânia no contexto cibernético são sensíveis e sujeitas a interpretações diversas, dependendo do ponto de vista principalmente político.

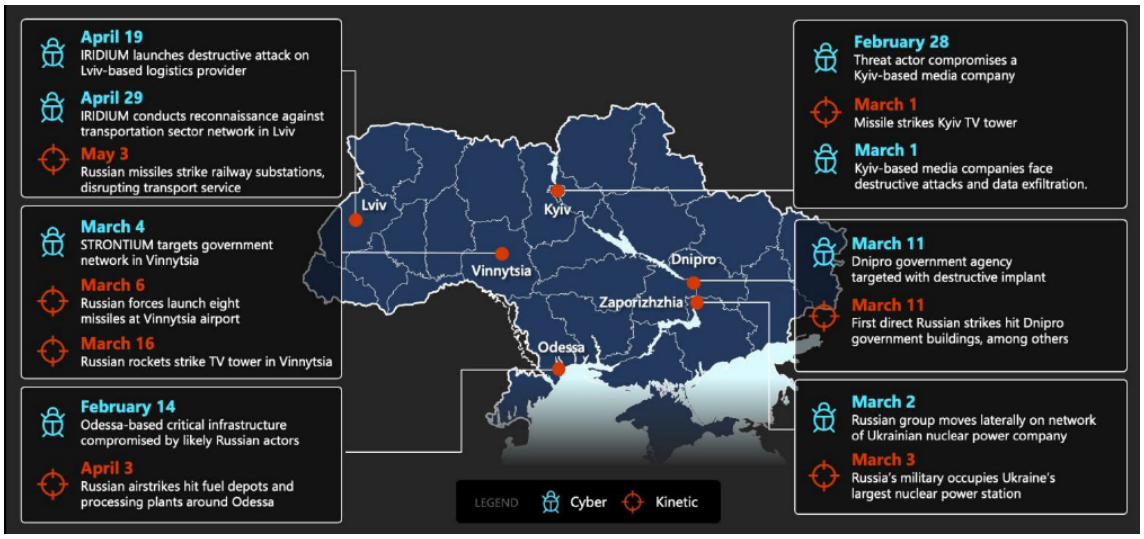
Alguns argumentos a favor da caracterização como ciberterrorismo argumentam que esses ataques cibernéticos constituem ciberterrorismo porque visaram civis e tiveram o objetivo de causar medo e dano.

Eles apontam para a Convenção do Conselho da Europa sobre o Cibercrime, que define ciberterrorismo como o uso de tecnologia da informação para causar medo ou dano com o objetivo de coagir um governo ou população civil. Também argumentam que a Rússia tem um histórico de uso de ataques cibernéticos como arma de guerra e que a invasão da Ucrânia faz parte de um amplo esforço para minar a Ucrânia e sua democracia.

Outros argumentos contra a caracterização como ciberterrorismo dizem que esses ataques cibernéticos não constituem ciberterrorismo porque não visaram diretamente civis e não tiveram como objetivo causar morte ou ferimentos graves. Os ataques foram direcionados principalmente a infraestrutura militar e governamental e que eram táticas militares legítimas no contexto de um conflito armado.

A definição de ciberterrorismo é vaga e subjetiva e não há consenso internacional. Não há, dentro dessa visão, até mesmo consenso se a Rússia cometeu ciberterrorismo durante a invasão da Ucrânia. A caracterização dependerá da definição específica de ciberterrorismo que está sendo usada e das circunstâncias específicas de cada ataque individual. Trata-se então, muito mais uma definição por parte da expressão do poder Político.

Abaixo podemos verificar uma coordenação de ataques cibernéticos com ataques cinéticos:



Fonte: Microsoft Defending Ukraine Early Lessons from the Cyber War, 2022.

É fato que a guerra cibernética entre Rússia e Ucrânia afetou diretamente as vidas das pessoas comuns, gerando medo, incerteza e insegurança. Os ataques cibernéticos não apenas visavam infraestruturas críticas e instituições governamentais, mas também tiveram impacto sobre a população civil, que enfrentou interrupções nos serviços essenciais, como eletricidade, água e comunicações.

Imagine-se em uma situação em que você não consegue acessar a internet para se comunicar com seus entes queridos ou o sistema de transporte público para chegar ao trabalho está fora de operação. Esses são apenas alguns exemplos das dificuldades enfrentadas pelas pessoas durante esses ataques, como vimos anteriormente.

Além disso, os ataques cibernéticos tiveram efeitos devastadores sobre a economia, levando ao desemprego, à perda de renda e à dificuldade em garantir o sustento básico. As empresas sofreram com interrupções em suas operações, o que afetaram não apenas os proprietários, mas também os funcionários e suas famílias.

É importante lembrar que por trás de cada ataque cibernético há pessoas reais, cujas vidas são afetadas de maneiras profundas e muitas vezes duradouras. Portanto, é crucial abordar essas questões não apenas como questões técnicas ou geopolíticas, mas também como problemas que impactam diretamente o bem-estar e a segurança das pessoas comuns.

Porém, conforme demonstrado no estudo da Microsoft, onde houve uma coordenação entre ataques cibernéticos e ataques cinéticos, todos levando a danos físicos

com efeitos trágicos para população civil, poderíamos considerar então que esses foram realizados dentro de um planejamento com objetivos militares de guerra. Então, num sentido mais amplo, dentro de um contexto de "guerra", onde sobressaem os ataques cinéticos, o conceito de terrorismo também deve ser bem avaliado. Fato é que durante esta pesquisa, não foi encontrado consenso até mesmo entre a relação guerra e terrorismo. Portanto, ressalta-se, mais uma vez que essa atribuição se deva muito mais a expressão Política do poder, que varia de país para país.

Do exposto, podemos inferir que a distinção entre guerra cibernética e terrorismo cibernético é um assunto complexo, especialmente quando estamos tratando de um assunto ainda andamento como é o conflito entre Rússia e Ucrânia, onde os ataques cibernéticos afetaram tanto infraestruturas quanto civis. A coordenação entre ataques cibernéticos e cinéticos torna a classificação desses eventos ainda mais desafiadora. Apesar da falta de consenso sobre a definição precisa de terrorismo cibernético, é crucial reconhecer o impacto direto desses ataques na vida das pessoas e adotar medidas para proteger sua segurança e bem-estar.

Estratégias de Mitigação e Resposta:

Para enfrentar esses desafios, é necessário um enfoque abrangente que inclua medidas defensivas e ofensivas, cooperação internacional e aprimoramento da capacidade de resiliência cibernética. Além disso, é crucial um diálogo contínuo sobre normas e princípios no ciberespaço para evitar escaladas descontroladas e garantir a estabilidade internacional.

Se nós extrapolarmos para o campo da guerra híbrida dentro da chamada "zona cinza", onde diariamente ocorre uma guerra muitas vezes "não declarada", podemos citar o Manual de Tallinn 2.0, que fornece informações sobre a aplicação do direito internacional às operações cibernéticas, incluindo o terrorismo cibernético. Embora o manual não se concentre especificamente no ciberterrorismo como uma categoria separada, aborda vários aspectos relacionados com operações cibernéticas que podem ser consideradas como ciberterrorismo.

Por exemplo, o manual discute os princípios da soberania, da responsabilidade do Estado e do direito dos conflitos armados no contexto das operações cibernéticas. Abrange também temas como contramedidas, proporcionalidade e proibição de ações que

afetem os direitos humanos fundamentais. Globalmente, o Manual de Tallinn 2.0 oferece um quadro abrangente para a compreensão das implicações jurídicas das atividades cibernéticas, que pode ser aplicado a vários cenários, incluindo aqueles que envolvem o terrorismo cibernético.[9]

A verdade é que falta de uma maior adesão mundial em convenções e leis internacionais não só como o Manual de Tallin, mas também de outras legislações, como a Convenção de Budapeste, que falam sobre o crime cibernético, contribuem significativamente para o aumento dos ataques cibernéticos por vários motivos, entre eles podemos citar a impunidade, a dificuldade na cooperação internacional, a crescente sofisticação dos ataques e o aumento da frequência de ataques.[10]

O Departamento de Defesa dos Estados Unidos (DoD), por meio da Estratégia Cibernética de 2023, apresenta várias estratégias de mitigação de incidentes cibernéticos, visando fortalecer a segurança cibernética e proteger as infraestruturas críticas dos EUA. Algumas das estratégias mencionadas no documento incluem:

Parcerias Público-Privadas: o DoD pretende expandir as parcerias público-privadas para garantir que os recursos, conhecimentos e informações do DoD sejam disponibilizados para apoiar as principais iniciativas do setor privado. Isso inclui aproveitar os conhecimentos técnicos e as capacidades analíticas do setor privado para identificar atividades cibernéticas maliciosas baseadas no exterior e mitigar vulnerabilidades em larga escala.

Operações no Ciberespaço: o DoD utilizará operações no ciberespaço para limitar, frustrar ou interromper as atividades dos adversários abaixo do nível de conflito armado, visando alcançar condições de segurança favoráveis. O Comando Cibernético dos EUA (USCYBERCOM) apoiará campanhas em todo o Departamento para reforçar a dissuasão e obter vantagens.

Exercícios de Treinamento: o Departamento realizará exercícios de treinamento holísticos, baseados em cenários realistas, para preparar e fortalecer suas capacidades de

[9] Jensen, "The Tallinn Manual 2.0: highlights and insights", Brigham Young University Law School, 2017, 15-44.

[10] Dang, "The Prevention of Cyberterrorism and Cyberwar", GA First Committee: Disarmament and International Security (DISEC), 2011, 4-6.

defesa cibernética. Esses exercícios ajudarão a criar uma abordagem integrada de ameaças, operações e processos no ciberespaço.[11]

Um bom exemplo de treinamento é o Exercício Guardião Cibernético, maior exercício de segurança cibernética do hemisfério sul. Trata-se de uma simulação conduzida pelo Ministério da Defesa do Brasil e coordenado pelo seu Comando de Defesa Cibernético (ComDCiber). Em sua 5ª edição, no ano de 2023 a atividade reuniu as três Forças Armadas e cerca de 150 instituições, entres entes governamentais e diversas empresas brasileiras. O objetivo final é fortalecer a segurança cibernética das principais infraestruturas estratégicas do Brasil.

A importância desses exercícios é acima de tudo é a de fortalecer as relações de confiança entre os entes, permitindo um melhor compartilhamento de informações de incidentes, integração, somar esforços e dar pronta respostas. Em resumo, gerenciar a crise de forma integrada e com a rapidez necessária. Duas palavras se sobressaem em qualquer exercício ou treinamento nessa direção: confiança e integração.

Para mitigar os riscos associados aos ataques cibernéticos podemos adicionar, ainda, algumas estratégias a serem adotadas, como é o caso da Cooperação Internacional, essa largamente empregada até os dias de hoje em apoio à Ucrânia. Inclua-se a essa cooperação o compartilhamento de informações, fundamental para uma maior velocidade na resposta a incidentes e principalmente a prevenção. Outras medidas incluem a capacitação de profissionais, o monitoramento contínuo e a participação em iniciativas internacionais.

Na verdade, a resposta aos desafios da guerra cibernética e do ciberterrorismo requerem uma abordagem abrangente, que inclua medidas defensivas e ofensivas, cooperação internacional e o fortalecimento da resiliência cibernética. A adesão global a convenções internacionais, como o Manual de Tallinn e a Convenção de Budapeste, é essencial para enfrentar o aumento dos ataques cibernéticos. Além disso, estratégias como parcerias público-privadas, operações no ciberespaço e exercícios de treinamento são fundamentais para fortalecer a segurança cibernética. A cooperação internacional, o compartilhamento de informações e a capacitação de profissionais são medidas adicionais

[11] U.S. Department of Defense “DOD Cyber Strategy Summary”, 2023, 18-24.

cruciais para mitigar os riscos associados aos ataques cibernéticos e garantir uma resposta eficaz e preventiva.

Conclusão:

A invasão da Ucrânia pela Rússia e os ataques cibernéticos subsequentes destacam a complexidade e os desafios associados à guerra cibernética e ao terrorismo cibernético. É essencial uma compreensão mais profunda desses fenômenos e a implementação de estratégias eficazes para mitigar seus impactos sobre a segurança internacional e a estabilidade global.

A expansão contínua do mundo digital é praticamente ilimitada e nenhum órgão ou governo jamais conseguirá restringir completamente sua capacidade de abranger quase todos os aspectos da vida no futuro. Como resultado dessa vastidão, as ameaças e os ataques cibernéticos assumem formas cada vez mais diversas e evolutivas, mirando uma variedade maior de alvos. Os perpetradores desses ataques empregam tecnologia avançada e inteligência, resultando em um novo cenário com lacunas significativas em relação ao passado.

Essa evolução transforma não apenas os conflitos e guerras no mundo real, mas também os ataques cibernéticos e as guerras virtuais. Paralelamente, o terrorismo também avança constantemente, adotando tecnologia de ponta e ferramentas inteligentes, o que resulta no correspondente ciberterrorismo. Tudo isso gera desafios significativos para a segurança dos sistemas de informação e para a prevenção de ataques contra infraestruturas nacionais, bem como para a segurança e a paz das pessoas.[12]

A análise mais abrangente das ameaças cibernéticas, como guerra e terrorismo cibernético, revelam a interconexão complexa entre esses fenômenos, especialmente no contexto das relações entre Rússia e Ucrânia. A invasão russa na Ucrânia entre 2022 e 2024 exemplifica essa complexidade, destacando a diversidade e coordenação dos ataques cibernéticos e seu impacto adverso sobre a estabilidade interna e as infraestruturas críticas. Esses eventos ressaltam a importância de compreender os efeitos da guerra cibernética sobre a população civil e sublinham a necessidade urgente de proteger tanto as infraestruturas quanto os civis contra tais ameaças. A distinção entre guerra e

[12] Ferrag et al. “Hybrid Threats, Cyberterrorism and Cyberwarfare”, CRC Press, 2024, 9-17.

terrorismo cibernéticos continua sendo um desafio, especialmente em contextos como o conflito Rússia-Ucrânia, onde os ataques afetam ambos.

A guerra cibernética na Ucrânia é um lembrete de que o ciberespaço se tornou um campo de batalha crucial no mundo moderno. A proteção da população civil e das infraestruturas críticas contra ataques cibernéticos exige uma resposta global coordenada e multifacetada. A comunidade internacional deve trabalhar em conjunto para desenvolver mecanismos eficazes de prevenção, detecção e resposta a essas ameaças crescentes.

A verdade é que o tema "terrorismo cibernético" deve ser aprofundado. Essa "guerra" vem sendo travada diariamente em todo mundo dentro da zona cinzenta, mesmo fora do contexto Ucrânia e Rússia, seja perpetrado por criminosos em busca de dinheiro, seja até mesmo por atores Estatais com objetivos não diplomáticos. Nesse mister, a questão da atribuição é fundamental e deve ser tratado pelo nível político por meio da gestão de uma política de segurança cibernética. A elevação desses crimes cibernéticos ao status de "terrorismo", podem dar o arcabouço legal para criação de leis mais rígidas que visem acima de tudo a dissuasão.

Bibliografia:

Defibaugh. "Past and Present Russian Information Operations in Ukraine: Competition into Conflict." In *Proceedings of the 19th International Conference on Cyber Warfare and Security, ICCWS 2024*, 64-65.

Dang. "The Prevention of Cyberterrorism and Cyberwar." GA First Committee: Disarmament and International Security (DISEC), 2011, 4-6. Acessado em 2 de abril de 2024. https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=5422c0fb4c95e3c8d47bf7263a06d0c51b2e01cd.

Ferrag, M.A., Kantzavelou, I., Maglaras, L., and Janicke, H. "Hybrid Threats, Cyberterrorism and Cyberwarfare." CRC Press, 2024, 9-17.

Henrique, Silva, and Daniel Belmonte. "OSINT e relações internacionais: o caso dos militares russos em Donbas entre 2014 e 2021." *Revista Brasileira de Estudos Estratégicos REST* V15 Nº29 (Jan-Jun 2023), 70-92. Acessado em 8 de abril de 2024. http://rest.uff.br/index.php/rest/article/view/291.

Iftikhar. "Cyberterrorism as a Global Threat: A Review on Repercussions and Countermeasures." Faculty of Computer Studies, Arab Open University, Riyadh, Saudi Arabia (15 de janeiro de 2024), 3-32. Acessado em 20 de abril de 2024. https://peerj.com/articles/cs-1772/.

Jensen. "The Tallinn Manual 2.0: Highlights and Insights." Brigham Young University Law School, 2017, 15-44. Acessado em 17 de abril de 2024. https://heinonline.org/HOL/LandingPage?handle=hein.journals/geojintl48&div=30&id=&page=.

Mueller, Jensen, Valeriano, Maness, and Macias. “Cyber Operations during the Russo-Ukrainian War: From Strange Patterns to Alternative.” *Center for Strategic and International Studies (CSIS)*, julho 2023, 15-26.

Oliveira de Souza, Ronaldo. “Guerra híbrida e ciberconflitos: uma análise das ferramentas cibernéticas nos casos da Síria e conflito Rússia-Ucrânia.” *Revista eletrônica Estácio Recife*, 2019, 6-17. Acessado em 15 de abril de 2024. https://www.gov.br/defesa/pt-br/arquivos/ensino_e_pesquisa/defesa_academia/cadn/artigos/XIII_cadn/guerra_hibrida_e_ciberconflitos_uma_analise_das_ferramentas_ciberneticas_nos_casos_da_siria_e_conflito_russiaucrania.pdf.

Smith, Brad. “Defending Ukraine: Early Lessons from the Cyber War.” *Microsoft*, (Junho 2022), 10-27.

U.S. Department of Defense. “DOD Cyber Strategy Summary”, 2023, 18-24.

Usman, Tabbasum, Ahmad, Shahzad, See fewer. “Cyber-warfare Versus Cyber-terrorism: An Emerging 21st Century Trend.” *Journal of Politics and International Studies*, (10 de dezembro de 2023), 149-155. Acessado em 10 de abril de 2024. https://plantsghar.com/index.php/45/article/view/1321/1310.