As ameaças híbridas no contexto do conflito russo-ucraniano

Natália Grass

O conflito entre Rússia e Ucrânia teve início em fevereiro de 2022 e se perpetua até o momento. Dentre as diversas problemáticas que o permeiam, o grave desrespeito aos direitos humanos, a destruição de patrimônios e as acusações de crimes de guerra são os mais repercutidos. A partir disso, abre-se um espaço para a ampliação de outras formas de ataque militar e civil de ambos os lados. Dentre essas, os ataques cibernéticos, ataques aéreos e intrusão terrestre no território ucaraniano.

Em grande medida, se faz necessária a distinção entre o que é ou não uma guerra civil, ou se esses ataques que vêm de lados diferentes podem ser ampliados e resultar em outros tipos de conflito. Com isso em vista, a presente análise busca compreender como os diversos tipos de ataque se configuram em um contexto de ameaças híbridas, bem como assimilar quais são os resultados desses tipos de ataques para os dois países envolvidos na guerra.

Guerra cibernética

De acordo com Bernardo Wahl (2022), não existe uma definição largamente aceita do que é a "Guerra Cibernética". Todavia, são apresentadas propostas de possíveis definições, ainda que não extensivas, sobre o assunto. Dentre elas, o conceito de Thomas Rid (2012), que explicita a inexistência da Guerra Cibernética, pois, de acordo com Thomas Rid, a guerra deveria ser violenta, possuir um teor instrumentalizado e ser atribuída politicamente (Rid, 2012). Nesse sentido, o autor dispõe que as ofensivas cibernéticas são constituídas por sabotagem e espionagem (WAHL, 2022), que visam adentrar no sistema adversário, enfraquecer um sistema militar ou econômico e estremecer a autoridade ou ordem previamente estabelecidas. A união dessas ameaças poderia, inclusive, derrubar um governo ou abalar as bases de sua constituição.

Um exemplo concreto e presente na relação entre os países é o ataque sofrido pelo site da marinha ucraniana no dia 6 de julho de 2021. Os hackers postaram relatórios falsos sobre os exercícios militares do International Sea Breeze-2021 no site. Ainda que não tenha sido comprovada a autoria do crime, o governo ucraniano já havia acusado a Rússia de orquestrar ataques deste tipo para "ganhar" uma guerra híbrida com o país. Ataques como esse enfraquecem a instituição e demonstram falhas que podem ser utilizados em momentos oportunos, enfraquecendo as instituições de um determinado país.

Dentre as diversas definições do que é a guerra, uma das mais famosas é a do autor clássico Clausewitz, em seu livro Da Guerra, em que a guerra é definida como sendo "a continuação da política por outros meios", tendo como principal objetivo o combate (Clausewitz, 1996, p. 27). Ao utilizar esse conceito, os ataques só seriam enquadrados como guerra no contexto de ameaças híbridas. De acordo com Clark e Knake (2010), a ameaça híbrida consiste no uso de técnicas regulares (já conhecidas e comuns) e irregulares (novas e utilizadas com baixa frequência), incluindo abordagem indiretas, como agentes terceirizados e não militares. A partir dessa definição, as ofensivas digitais podem ser definidas como "Guerra Cibernética" (Clarck; Knake, 2010).

Quando se pensa sobre as ameaças híbridas no contexto do conflito entre Rússia e Ucrânia, imagina-se que há a união de táticas e estratégias que combinam a ação de forças irregulares, operações cibernéticas e manipulação política para alcançar metas estratégicas russas. A utilização de ataques cibernéticos também ocorreu no contexto da anexação da Criméia, em 2014, e não pode ser atribuída única e exclusivamente aos russos. A presença de grupos pró-Rússia no território, além da ineficácia de países como Estados Unidos e membros da União Européia, foram centrais na ocupação da região.

Paralelamente, há trinta anos de história de especulação sobre como as ferramentas e técnicas do cibercrime underground – ataques distribuídos de negação de serviço ("DDoS"), interrupção e comprometimento de serviços, desfigurações de páginas web e técnicas semelhantes – podem permitir que os civis desempenhem papel central em uma guerra "quente" entre nações desenvolvidas. Muito disso é especulação baseada em modelos criminológicos de baixo nível, grupos clandestinos de cibercrime e nas ligações entre estes movimentos "hacktivistas" clandestinos e bem organizados, tornando o futuro da

 Recebido em 26 jun. 2023 | Publicado em 26 mar. 2024

guerra híbrido, caótico e imprevisível.

Invasões russas

A partir do contexto de digressões no campo dos ataques cibernéticos, o governo russo é o que ataca de forma mais intensa e contínua (Alperovich, 2022). Dentre as principais ações russas, ocorreu o monitoramento de operações militares, uso de operações para interromper as operações militares e realizar a condução de operações psicológicas na população ucraniana.

Segundo Alperovitch (2022), a principal forma de se pensar sobre a intrusão no território é o monitoramento de operações militares, iniciadas a partir do grampeamento de comunicação das unidades militares, agências de inteligência e conceber ainda o posicionamento das tropas, bem como suas táticas defensivas. Em consequência, haveria uma facilitação das futuras e possíveis operações do governo russo.

A Rússia também poderia utilizar operações no ciberespaço para enganar militares e possivelmente interromper as operações das forças ucranianas, desviando as tropas ou mesmo enviando direções contrárias para gerar um atraso na defesa ucraniana. Essa interrupção de comunicação interferiu diretamente na coordenação e envio de tropas pela Ucrânia para locais mais afetados como Kharkiv e Mariupol. Outro mecanismo seria o de atingir bancos de dados digitais de logística das forças armadas, resultando na ilusão temporária do contingente, bem como atacar as redes de controle de tráfego aéreo, impedindo os voos civis e até mesmo o apoio internacional para ajuda humanitária (Naibo, 2022).

Um terceiro ponto importante seria a condução de "operações psicológicas". Esse mecanismo consiste na prática de ataques aos principais meios de comunicação, seja criando relatórios falsos ou mesmo espalhando rumores em redes sociais como o Whatsapp. Há ainda a possibilidade de ataque às redes elétricas, que poderiam deixar milhões de pessoas sem acesso ao calor durante o inverno rigoroso, e dificultar o acesso a recursos financeiros, como saques e transações em crédito.

O governo russo não tem a intenção de destruir locais e serviços que podem ser utilizados a seu favor, como a Siderúrgica Azovstal (Zappone, 2022). Ainda que os ataques cibernéticos sejam secundários no conflito em questão,

 Recebido em 26 jun. 2023 | Publicado em 26 mar. 2024

estes não podem ter seus efeitos ignorados, pois assim como os ataques militares, afetam também os civis não envolvidos no conflito. Essas operações servem, sobretudo, para enviar uma mensagem bastante clara aos líderes ucranianos: a resistência será inútil, uma vez que a Rússia está por toda parte (Alperovitch, 2022).

A partir do momento em que a Rússia não conseguiu alcançar o seu objetivo de derrubar o governo de Kiev, os militares russos passaram a ter dificuldades na conquista do território. Os desafios enfrentados pelos militares russos foram principalmente a demissão de oficiais e a morte de um número significativo de militares em combate (Wolf, 2022). O conflito russo-ucraniano reúne múltiplas arestas que envolvem atores relevantes nas relações internacionais. Durante oito anos, a Rússia culpou a Ucrânia pelo desfecho desta situação, através de uma mistura de fake news, acompanhada do revisionismo histórico da extinta União Soviética. A narrativa russa justifica suas ações devido ao conflito na Ucrânia: guerra híbrida e intervenção militar convencional (Clarke, Knake; 2010).

A guerra de desinformação está se tornando um dos principais objetivos do conflito. O jogo de guerra híbrido e a implementação de uma linguística poderosa denotam um caráter que por vezes não é subjetivo, mas apela ao poder de conquista que a Rússia almejava. Segundo o presidente russo, o objetivo oficial do ataque é a desnazificação da Ucrânia (Zappone, 2022). Nesse sentido, os ataques cibernéticos evidenciam o efeito de causa e consequências constantes, ora sendo meios para facilitar os ataques, ora consequência, como a desinformação nas redes sociais que afetam diretamente os civis ucranianos.

Se o dano econômico na Rússia se tornar grave o suficiente, Putin pode decidir que vale a pena ressaltar por meios não militares, como ataques cibernéticos. A opinião pública nos Estados Unidos vê os ataques cibernéticos como um meio muito diferente daquele usado na guerra convencional, uma vez que os ataques híbridos de tornam ferramentas intensificadoras no processo de conquista e ocupação territorial. Pode-se inferir que os Estados Unidos e os países europeus envolvidos no conflito ucraniano suportariam um certo nível de dano causado por um ciberataque russo (Zappone 2022).

 Recebido em 26 jun. 2023 | Publicado em 26 mar. 2024

Conclusão

O conflito na Ucrânia tornou-se uma guerra global (ao envolver outros países com posicionamentos e doação de armamentos) implementada pela Rússia no momento da invasão. A desinformação é a principal ferramenta do Kremlin para justificar sua expansão em termos militares convencionais. As sanções ocidentais contra a Rússia tornam-se uma ferramenta de contrapeso – por meio do poder não militar – para impedir a conquista dos objetivos estratégicos russos. E a extrapolação territorial de suas consequências envolve tanto a ajuda financeira e militar dos países como a recepção de ucranianos em outros países como refugiados.

A partir do exposto ao longo do texto, pode-se compreender que as ameaças e ataques híbridos configuram um embate danoso e com pouca mediação. Além disso, o enfraquecimento institucional ucraniano serve de apoio para a expansão russa no território. Portanto, pode-se compreender que por meio das intrusões russas no território ucraniano também de forma híbrida, a guerra apresenta outro aspecto. Sendo esse aspectos fundamentais para a compreensão mais profunda da escalada do conflito, com ênfase nas táticas de espionagem russa como um intensificador no conflito. A resposta ucraniana, ainda que insuficiente, é crucial para a redução de danos no conflito. Por fim, há o destaque de influência e força russas, sobrepondo-se aos domínios ucranianos de forma consistente e contínua.

Recebido em 26 jun. 2023 | Publicado em 26 mar. 2024

Referências

ALPEROVITCH, Dmitri. How Russia Has Turned Ukraine Into a Cyber-Battlefield. Foreign Affairs, 28 jan. 2022. Disponível em: https://www.foreignaffairs.com/articles/russia-fsu/2022-01-28/how-russia-has-turned-ukraine-cyber-battlefield. Acesso em: 13 mai. 2023.

CLARKE, Richard A; KNAKE, Robert K. (2010). Cyber War: The Next Threat to National Security and What To Do About It. Nova Iorque: HarperCollins, 290 p.

CLAUSEWITZ, Carl von. Da Guerra. São Paulo: Martins Fontes, 1996.

NAIBO, Gloria. The reality of cyber warfare: The Ukraine-Russia conflict as a catalyst for new dynamics in cyberspace. Praha, 2022. Diplomová práce. Univerzita Karlova, Fakulta sociálních věd, Katedra bezpečnostních studií.

PEARSON, James; BING, Christopher. The cyber war between Ukraine and Russia: An overview. Reuters, 10 mai. 2022. Disponível em: <https://www.reuters.com/world/europe/factbox-the-cyber-war-between-ukraine-russia-2022-05-10/>. Acesso em: 11 mai. 2022.

RM STAFF. Why Hasn't Russia Unleashed 'Cybergeddon' in Its War on Ukraine?. Russia Matters, Harvard Kennedy School Belfer Center for Science and International Affairs, 04 mai. 2022. Disponível em: https://www.russiamatters.org/analysis/why-hasnt-russia-unleashed-cybergeddon-its-war-ukraine. Acesso em: 10 mai. 2022.

UKRAINE says Russian hackers hit its Navy website. Reuters. Disponível em: Ukraine says Russian hackers hit its Navy website | Reuters. Acesso em: 04 mai 2023.

WAHL, Jorge. A DIMENSÃO CIBERNÉTICA DA GUERRA ENTRE A RÚSSIA E A UCR NIA EM 2022: : UMA AVALIAÇÃO INICIAL PASSADOS 100 DIAS DO CONFLITO. Revista Hoplos, 6(10), 102-124. Recuperado de https://periodicos.uff.br/hoplos/article/view/54787 .

WOLFF, Josephine. Why Russia Hasn't Launched Major Cyber Attacks Since the Invasion of Ukraine. Time, 02 mar. 2022. Disponível em: <https://time.com/6153902/russia-major-cyber-attacks-invasion-ukraine/>. Acesso em: 15 mai. 2022.

ZAPPONE, Chris. Seven reasons Putin hasn't launched a cyberwar in Ukraine – yet. The Sydney Morning Herald, 25 abr. 2022. Disponível em: <https://www.smh.com.au/world/europe/seven-reasons-putin-hasn-t-launched-a-cyberwar-in-ukraine-yet-20220421-p5af3o.html>. Acesso em 15 mai. 2023.