O ciberespaço e a guerra na Ucrânia

Harry Williams | *André Barrinha*

INTRODUÇÃO

Antes da invasão russa da Ucrânia em fevereiro de 2022, existia uma expectativa elevada entre analistas e comentadores de que, caso acontecesse uma incursão militar, esta seria acompanhada por uma série de ciberataques em larga escala por parte de Moscovo[1]. Nas últimas décadas, a Rússia tinha vindo a conquistar a reputação de uma ciberpotência global[2]. A perceção de poder da Rússia neste domínio aumentou os receios sobre a ameaça que poderia representar para a Ucrânia, especialmente após a invasão da Crimeia em 2014. Nos anos seguintes a esta, o grupo de *hackers* russo Sandworm lançou ataques à rede elétrica ucraniana, deixando centenas de milhares de ucranianos sem energia durante várias horas[3], enquanto o lançamento do NotPetya em 2017 causou enormes prejuízos financeiros à Ucrânia e teve um custo global de cerca de dez mil milhões de dólares[4]. Há quem argumente que a Ucrânia tem sido usada como um campo de testes para as cibercapacidades russa[5]. Já anteriormente, *hackers* russos tinham levado a cabo ataques contra a Estónia, em 2007, e contra a Geórgia, em 2008[6], e, como é conhecido, utilizado táticas de guerra de informação nas eleições dos Estados Unidos da América (EUA) em 2016. O histórico de ações russas nesta área, juntamente com a sua posição de ciberpotência (ao que podemos ainda acrescentar a crescente interpretação do ciberespaço como cenário de confronto[7]), levou à noção generalizada de que qualquer conflito entre a Rússia e a Ucrânia incluiria uma ciber-

RESUMO

Era esperado que a invasão da Ucrânia pela Rússia fosse acompanhada por ataques cibernéticos em larga escala. Contudo, embora as cibercapacidades tenham efetivamente desempenhado um papel de apoio no conflito, o grau de sofisticação e intensidade da sua utilização tem sido, de uma maneira geral, limitado, em parte devido ao fortalecimento das defesas ucranianas e ao papel sem precedentes de atores terceiros no conflito, incluindo Estados, corporações privadas e grupos de *hackers* civis. Este artigo analisa a ciberdimensão do conflito e explora algumas lições que podem ser retiradas deste estudo de caso sobre o uso de cibercapacidades em guerras, e como é que futuros (ciber)conflitos poderão ser estudados por investigadores da área das Relações Internacionais.

Palavras-chave: ciberguerra, operações de informação, Rússia, Ucrânia.

ABSTRACT

Cyberspace and the war in Ukraine

The invasion of Ukraine by Russia was expected to be accompanied by the deployment of large-scale →

 https://doi.org/10.23906/ri2025.85a06

cyberattacks. While cyber capabilities have undeniably played a supporting role in the conflict, the sophistication and intensity have been limited overall, partly by the strengthened Ukrainian defences and the unprecedented role of third parties, including states, private corporations, and civilian hacking groups. This paper examines the cyber-dimension of the conflict. It explores the lessons that can be learnt from this case study about cyber capabilities in warfare and how IR scholars study future (cyber) conflicts.

Keywords: cyber-warfare, information operations, Russia, Ukraine.

componente significativa. Chegou-se inclusive a especular que as ciberarmas poderiam tornar o uso da força física desnecessário[8], embora a visão predominante fosse a de que estas seriam conjugadas de forma eficaz com a guerra convencional[9]. Independentemente da forma que o conflito tomasse, esperava-se que o ciberespaço desempenhasse um papel central.

A realidade tem-se revelado algo diferente do esperado. As cibercapacidades têm sido utilizadas pelos dois lados do conflito, mas este não atingiu a dimensão de uma ciberguerra total como alguns especularam[10]. Ao invés, estas capacidades têm desempenhado um papel secundário. As ações russas têm sido limitadas em termos de sofisticação, e a maioria dos ataques de maior intensidade tem sido evitada pelas defesas ucranianas, com o auxílio de terceiros[11]. Igualmente, as ações ucranianas neste domínio têm levado a alguns sucessos pontuais, mas nenhum deles com um efeito de nível estratégico.

A disparidade entre as expectativas e os resultados em relação ao uso do ciberespaço no conflito Rússia-Ucrânia oferece um estudo de caso fascinante sobre como cibercapacidades são utilizadas em contextos de guerra. Em termos de estrutura, este artigo examinará, primeiro, os usos das cibercapacidades no conflito Rússia-Ucrânia, em comparação com as expectativas iniciais. Em seguida, explorará as principais lições a retirar deste estudo de caso e as implicações mais vastas para o campo das Relações Internacionais, na investigação sobre o papel do ciberespaço em contextos de guerra. A análise focar-se-á em eventos decorridos entre fevereiro de 2022 e meados de 2024, apoiando-se em dados de fontes de acesso aberto, como relatórios técnicos, publicações e artigos de imprensa, reconhecendo que poderão não representar o panorama completo do conflito devido à omissão de dados classificados ou não publicados.

O USO DE CIBERATAQUES NO CONFLITO

Desde o começo do conflito, a 24 de fevereiro de 2022, que Moscovo tem tentado interferir com os sistemas e redes informáticas ucranianas como complemento às suas operações cinéticas no terreno. Por exemplo, o início da invasão russa da Ucrânia foi precedido, poucas horas antes, de um ataque à Viasat, um importante fornecedor de telecomunicações, que envolveu simultaneamente um ataque distribuído de negação de serviço (DDoS) e intrusão nas redes terrestres, interrompendo os serviços de internet de milhares de utilizadores na Ucrânia e na Europa. Coordenado com a incursão das tropas russas em território ucraniano, o ataque foi provavelmente pensado para dificultar a resposta de Kiev, embora existam relatos contraditórios sobre o impacto do ataque. Victor Zhora, um dos principais responsáveis pelas operações ucranianas no

ciberespaço durante o primeiro ano do conflito, afirmou na altura do ataque que este tinha causado «uma enorme quebra a nível das comunicações». No entanto, esta avaliação seria contradita pelo mesmo pouco tempo depois, dizendo não haver provas de que o ataque tivesse piorado a conectividade militar, e salientando que os satélites da Viasat desempenhavam um papel secundário (de *backup*) no acesso das tropas ucranianas às suas redes de informação[12]. O lançamento deste ataque no início da campanha parecia apoiar a ideia de que a Rússia utilizaria ciberataques como um pilar essencial na invasão da Ucrânia. Contudo, a realidade acabaria por se revelar um pouco diferente das expectativas.

As táticas disruptivas continuaram nas fases iniciais da guerra, com um aumento de ataques de baixa intensidade, como *wipers*[13], direcionados a empresas, bancos e indústrias governamentais; desfiguração de *websites* governamentais; ataques de *phishing* contra altos oficiais militares e governamentais; e ataques de DDoS para interromper o funcionamento de serviços vitais[14]. No entanto, as ações russas refletiram uma prioridade na quantidade em detrimento da qualidade, numa abordagem muitas vezes descrita como de «força bruta»[15], privilegiando o engajamento persistente a um nível de sofisticação baixo. Apesar do aumento no volume de ataques, os analistas observaram uma eficiência reduzida destes em comparação com anteriores ações da Rússia contra a Ucrânia[16], o que pode, em parte, ser explicado pela melhoria significativa da qualidade das capacidades de defesa ucranianas[17], mas também por uma desadequada preparação russa. Moscovo tinha-se preparado para uma campanha de curta duração alicerçada numa invasão terrestre rápida e esmagadora e em campanhas de desinformação e desestabilização. A gorada expectativa de uma vitória e ocupação rápidas obrigou Moscovo a alterar os seus planos, focando-se na utilização de *wipers* e de ataques DDoS[18].

Não quer isso dizer que a Rússia não tenha tentado ciberataques mais significativos. Em abril de 2022, um ataque à infraestrutura energética da Ucrânia foi identificado pela CSIRT[19] ucraniana e rapidamente neutralizado, sem impacto nas redes elétricas visadas[20]. O *malware* usado era uma versão mais sofisticada do ataque de 2016 e, se bem-sucedido, teria degradado o sistema a um ponto difícil de restaurar. Uma campanha semelhante foi levada a cabo em outubro do mesmo ano, causando um apagão que coincidiu com uma série de ataques de mísseis na zona de Kiev[21]. Em dezembro de 2023, um ataque bem-sucedido à Kyivstar – a maior operadora de redes móveis da Ucrânia – danificou significativamente a rede virtual da empresa, interrompendo temporariamente os serviços de comunicação em todo o país[22]. Este ataque tinha sido precedido, em maio, de uma intrusão que permitiu o acesso de *hackers* russos a mensagens SMS, dados de localização e possivelmente contas de Telegram dos utilizadores. A interrupção também afetou o funcionamento de sirenes de alerta aéreo nalgumas áreas, bem como os sistemas bancários e caixas automáticas que dependiam da rede Kyivstar, mas supostamente teve pouco impacto na funcionalidade militar da Ucrânia.

Os exemplos acima demonstram que as operações cibernéticas desempenharam, até agora, um papel limitado no conflito. Parte desta ausência deve-se às defesas ucranianas. A *threat intelligence* obtida em ataques anteriores permitiu uma maior resiliência dos sistemas ucranianos, e o apoio de organizações terceiras e de Estados aliados provou ser valioso para as defesas locais[23].

AS OPERAÇÕES CIBERNÉTICAS DESEMPENHARAM, ATÉ AGORA, UM PAPEL LIMITADO NO CONFLITO. PARTE DESTA AUSÊNCIA DEVE-SE ÀS DEFESAS UCRANIANAS.

DO CIBERCONFLITO À GUERRA DE INFORMAÇÃO

Embora a ciberdimensão do conflito tenha ficado aquém de algumas expectativas, o mesmo não se pode dizer das operações de espionagem e informação russas. É possível argumentar que a utilização estratégica mais bem-sucedida das cibercapacidades por parte da Rússia tem-se revelado no domínio da informação. Uma parte significativa das suas operações neste domínio envolveu espionagem e roubo de dados, como a recolha de inteligência para o planeamento estratégico e a identificação de alvos prioritários. A Microsoft identificou pelo menos dois casos em que uma intrusão de rede foi seguida por um ataque de mísseis a um alvo relacionado: um ataque a infraestruturas ferroviárias em Lviv e um ataque a um aeroporto em Vinnytsia, dois dias após ter sido identificada uma intrusão numa rede governamental[24]. Os Serviços de Segurança da Ucrânia (SBU) afirmaram em 2023 que a Diretoria Principal de Inteligência russa (GRU) estava a visar satélites Starlink para recolher dados sobre a atividade militar ucraniana[25]. Militares e figuras políticas ucranianas foram, igualmente, alvo de campanhas de *phishing* e de ataques aos seus dispositivos pessoais[26]. Em janeiro de 2024, agentes russos invadiram *webcams* civis em Kiev para recolher dados de imagem sobre as defesas da cidade antes de lançar um ataque com mísseis[27]. Para além de usar estas informações para planeamento militar, a recolha de dados também pode ser utilizada para controlar uma população através do medo, usando dados pessoais para identificar e alvejar indivíduos que possam representar uma ameaça à força ocupante[28]. Assim, o foco na recolha de dados e na obtenção de inteligência alinha-se com a expectativa russa de uma vitória rápida e de uma ocupação prolongada da Ucrânia, ao invés do estado de guerra prolongado que se veio a verificar.

Um segundo foco das operações de informação russas tem sido a disseminação de desinformação. As campanhas de desinformação têm origem na doutrina soviética de controlo reflexivo, que consiste na disponibilização de informações para consumo do inimigo com o objetivo de controlar subliminarmente crenças e comportamentos, e tem-se revelado um elemento central nas táticas russas de guerra de informação[29]. A Rússia criou um «ambiente de informação caótico»[30], conduzindo campanhas que variam desde ações para manter o apoio interno ao esforço de guerra na Rússia, até à fragilização da unidade nas nações ocidentais e à distorção das críticas aos crimes de

guerra russos, e ao ataque à moral e confiança da população ucraniana na sua capacidade de se organizar e resistir aos ataques russos[31]. Circularam *deepfakes* do Presidente Zelensky, incluindo um, no início do conflito, em que ele apelava aos soldados ucranianos para se renderem às forças russas[32]. Estações de rádio ucranianas foram alvo de transmissões falsas a informar que Zelensky estava em estado crítico[33]. Políticos e celebridades ocidentais que publicamente apoiaram a Ucrânia foram alvo de ataques de engenharia social para obter declarações que pudessem ser manipuladas de forma a manifestar posições pró-Rússia[34]. Todas estas táticas refletem uma campanha de subversão destinada a minar a confiança na força e na liderança ucranianas e promover uma agenda pró-Rússia.

Moscovo demonstrou particular sucesso no controlo do fluxo de informação nos territórios ocupados militarmente. Os ocupantes russos na região de Kherson redirecionaram o tráfego local de internet e das redes móveis através de infraestruturas russas, bloqueando o acesso a fontes noticiosas ucranianas e independentes, ao Facebook, Instagram e X (anteriormente Twitter), e implementando normas, vigilância e censura rígidas na internet[35]. Essas medidas cortaram eficazmente a ligação de Kherson a informações externas, limitando a população ao acesso a notícias e meios de comunicação russos. Os civis foram alvo de informações falsas sobre as ações do Governo ucraniano e bombardeados com propaganda russa[36].

No geral, o ciberespaço tem sido predominantemente usado por Moscovo em operações de informação e espionagem, bem como em ataques constantes de baixa intensidade. As cibercapacidades surgem neste conflito como «a cereja no topo do bolo» para as operações russas, em vez de constituírem um ramo principal das suas táticas militares[37].

KIEV CONTRA-ATACA

À medida que a Ucrânia enfrentava um aumento no volume de ciberataques, a sua principal preocupação consistia na manutenção da funcionalidade dos sistemas militares e governamentais visados pela Rússia. No entanto, paralelamente a este foco na defesa, surgiu um movimento crescente disposto a retaliar contra os esforços russos, particularmente entre *hacktivistas*. Grupos como o IT Army e o Cyber Regiment desempenharam um papel importante nas capacidades ofensivas da Ucrânia. Embora não sejam oficialmente patrocinados por Kiev, foram feitos esforços para legitimar e coordenar as suas atividades[38]. O grupo *hacktivista* descentralizado Anonymous também tem estado ativo, tendo atacado órgãos de comunicação social e canais de televisão estatais russos[39]. Embora seja difícil quantificar a eficácia desses grupos no contexto do conflito mais amplo, esses atores desempenharam pelo menos um papel indireto na interrupção das operações russas[40].

Ao longo do conflito, as agências de inteligência e cibersegurança da Ucrânia também aumentaram a sua atividade. Em particular, 2024 assistiu a um aumento marcante na atividade contra a Rússia pela Diretoria Principal de Inteligência da Ucrânia (HUR),

a qual, em fevereiro, conseguiu acesso a servidores russos contendo documentos classificados e informações detalhadas sobre oficiais de alto escalão e unidades estruturais do Ministério da Defesa da Rússia[41]. Outros ataques visaram *websites* governamentais russos, aeroportos e infraestruturas de telecomunicações, resultando em significativas interrupções de internet em toda a Rússia[42].

Tal como os ataques russos, os ataques ucranianos não dominaram os holofotes num conflito marcado pela violência cinética, mas demonstraram ainda assim uma presença persistente no tabuleiro de xadrez contínuo em que se tornou o conflito entre os dois países.

LIÇÕES APRENDIDAS

O conflito Rússia-Ucrânia oferece, pois, várias lições importantes sobre o uso do ciberespaço num conflito armado. Em primeiro lugar, no contexto de guerra, a destruição física e as operações militares cinéticas são mais fáceis e simples de planear e executar do que ciberataques de larga escala, além de gerarem um impacto mais direto e eficaz. Apesar dos avanços tecnológicos na guerra, o conflito permanece essencialmente cinético. Existe uma disparidade assimétrica entre as capacidades cibermilitares e cinéticas, sendo o potencial destrutivo de um míssil ou de um ataque de *drones* significativamente maior do que o resultado direto de um ciberataque[43]. Por exemplo, enquanto a maioria dos ciberataques russos contra infraestruturas falhou ou foi eliminado, as redes elétricas têm sido um alvo principal de ataques com mísseis e *drones*, reduzindo significativamente a funcionalidade e operatividade das infraestruturas elétricas e hídricas ucranianas[44]. Em suma: «é muito mais simples para a Rússia lançar um bombardeamento de artilharia contra uma subestação elétrica do que *hackeá-la* de Moscovo»[45].

NO CONTEXTO DE GUERRA, A DESTRUIÇÃO FÍSICA E AS OPERAÇÕES MILITARES CINÉTICAS SÃO MAIS FÁCEIS E SIMPLES DE PLANEAR E EXECUTAR DO QUE CIBERATAQUES DE LARGA ESCALA, ALÉM DE GERAREM UM IMPACTO MAIS DIRETO E EFICAZ.

Em segundo lugar, os ciberataques de larga escala exigem tempo e planeamento. O uso eficaz de *malware* a um nível estratégico requer um longo tempo de preparação e desenvolvimento, sendo frequentemente de uso único, já que os alvos rapidamente desenvolvem defesas contra as vulnerabilidades na origem desses ataques. Antecipando uma vitória rápida, a Rússia utilizou cibercapacidades sofisticadas no início do conflito. No entanto, quando a Ucrânia se mostrou defensivamente mais bem preparada do que o esperado, a Rússia foi forçada a recorrer a ataques de baixa intensidade, como DDoS e *wiper malware*, que são mais fáceis de implementar e exigem menos planeamento prévio[46]. Nestas condições, o uso de operações de informação, espionagem e subversão revelou-se mais eficaz do que a utilização de ciberataques de natureza destrutiva para conseguir uma vantagem militar.

Em terceiro lugar, a articulação entre operações cinéticas e ciberoperações permanece difícil, mesmo para atores poderosos como a Rússia. Existem poucos exemplos claros de uso de ciberataques diretamente associados a ações militares cinéticas[47], e menos ainda em que haja evidência de articulação planeada e não apenas coincidência. As dificuldades logísticas e a necessidade de coordenação entre departamentos e agências governamentais dificultam essas mesmas atividades. Além disso, o espaço temporal necessário para o planeamento e a execução de operações cibernéticas nem sempre se coaduna com os rápidos desenvolvimentos militares no campo de batalha. Em qualquer destes contextos, a coordenação parece fazer mais sentido em missões de recolha de inteligência que visam fornecer informações sobre os alvos aos militares[48], beneficiando das cibercapacidades sem estar limitada às mesmas.

Em quarto lugar, o uso de táticas de informação pela Rússia dentro da Ucrânia foi menos eficaz do que o pretendido. Embora se possa argumentar que o controlo russo sobre as notícias e sobre a comunicação social dentro das suas próprias fronteiras e em territórios ocupados pode ser eficaz para manter uma imagem forte e uma opinião pró-Rússia[49], as operações de informação russas não conseguiram derrubar a resistência da população ucraniana[50]. Os agentes russos estavam preparados para uma vitória rápida seguida de uma ocupação, e as suas táticas não se adequavam a uma guerra prolongada. Um exemplo disso, logo em 2022, foi a já mencionada circulação de um *deepfake* do Presidente Zelensky a pedir a rendição das forças ucranianas. No entanto, levantaram-se vários problemas: a tecnologia usada para criar o *deepfake* estava desatualizada, o que resultou num vídeo de baixa qualidade; o lançamento foi mal agendado, várias semanas após o início do conflito, quando Zelensky já havia feito discursos inspiradores ao público e seria improvável que fizesse tal declaração; e a divulgação não foi feita por canais oficiais, colocando a sua legitimidade em causa[51]. Além do mais, o Governo ucraniano já havia instituído proibições à circulação de meios de comunicação e jornalistas russos, limitando ainda mais o alcance e o impacto da propaganda russa entre os civis.

Em quinto lugar, a defesa, a preparação e a resiliência são vitais no ciberespaço. O fracasso da Rússia em levar a cabo ciberataques estrategicamente significativos deve-se, em parte, às suas próprias limitações operacionais, mas também à defesa e oposição ucranianas. O uso da Ucrânia como campo de teste para as cibercapacidades da Rússia forneceu ao país uma década de aprendizagem, permitindo-lhe identificar vulnerabilidades e reforçar as suas defesas. Isso também foi resultado do árduo trabalho de bastidores dos aliados ocidentais para aumentar as cibercapacidades e as ciberdefesas da Ucrânia. Os EUA têm trabalhado de perto com o Governo ucraniano para fortalecer a resiliência e segurança do ciberespaço ucraniano, com organizações como a USAID[52], o FBI (Federal Bureau of Investigation) e a CISA (Cybersecurity and Infrastructure Security Agency) a desempenharem papéis importantes na proteção das redes de informação no país. Estas duas últimas organizações, em particular, ajudaram tam-

bém a desmontar campanhas de desinformação direcionadas ao Governo e às forças armadas ucranianas[53]. Também a União Europeia (UE) enviou especialistas para ajudar a Ucrânia a defender-se contra ciberataques[54]. Alguma desta ajuda aconteceu após a invasão russa, mas houve igualmente vários programas em curso ao longo da última década, o que serviu para garantir que a Ucrânia estivesse bem preparada para defender o seu ciberespaço. Esses esforços ajudaram, por sua vez, a reforçar as defesas ucranianas e a limitar o impacto dos ataques realizados pela Rússia[55].

Por último, os atores não estatais têm desempenhado um papel sem precedentes no conflito, tanto em termos defensivos como ofensivos. Além da ajuda de países aliados, empresas multinacionais de tecnologia ofereceram assistência valiosa à Ucrânia durante o conflito. A Microsoft e a Mandiant (da Google) estabeleceram uma parceria com o Governo ucraniano para fornecer informações relativamente a potenciais e efetivos ataques ao ciberespaço ucraniano[56], analisando também táticas russas para prever áreas críticas de defesa à medida que o conflito avançava[57]. Uma área de particular vulnerabilidade identificada foi a dependência do Governo ucraniano relativamente a servidores de dados. A Amazon Web Services ajudou a hospedar e a proteger dados do Governo e do sector privado ucranianos na sua nuvem[58], transferidos com a ajuda da Microsoft[59]. Satélites Starlink da SpaceX forneceram internet e comunicações para substituir as redes degradadas e destruídas no início da guerra, e têm sido utilizados para fins militares e humanitários[60]. A Google expandiu o seu Project Shield para proteger os *websites* dos órgãos de comunicação social e da sociedade civil ucraniana contra ataques DDoS[61]. Muitas das organizações do sector privado que ofereceram ajuda fizeram-no por conta própria ou financiadas por aliados ocidentais da Ucrânia[62].

ALÉM DA AJUDA DE PAÍSES ALIADOS, EMPRESAS MULTINACIONAIS DE TECNOLOGIA OFERECERAM ASSISTÊNCIA VALIOSA À UCRÂNIA DURANTE O CONFLITO. A MICROSOFT E A MANDIANT (DA GOOGLE) ESTABELECERAM UMA PARCERIA COM O GOVERNO UCRANIANO.

No que diz respeito às capacidades ofensivas da Ucrânia, os *hacktivistas* revelaram-se importantes no conflito[63]. Os seus ataques contra instituições e empresas russas têm afetado o normal funcionamento da economia e da sociedade russas[64]. Apenas dois dias após a invasão, o vice-primeiro-ministro ucraniano, Mykhailo Fedorov, apelou publicamente a que *hackers* se voluntariassem para ajudar a Ucrânia, direcionando ataques a sistemas russos[65], o que levou à criação do famoso IT Army. Mais tarde, surgiram outros grupos semelhantes, como o Cyber Regiment, a Ukrainian Cyber Alliance e o IT Stand for Ukraine[66]. Além disso, grupos como o Anonymous também se envolveram no conflito, declarando abertamente uma ciberguerra contra a Rússia[67].

Hackers e *hacktivistas* civis também desempenharam um papel do outro lado do conflito. Grupos como Solntsepek, InfoCentr, Killnet e o Cyber Army of Russia Reborn surgiram para combater as atividades cibernéticas ucranianas[68]. Para ambos os países, a relação

entre os grupos *hacktivistas* e o Estado é pouco clara, particularmente no que diz respeito à distinção entre ataques sancionados pelo Estado e ataques *ad hoc* organizados por estes grupos. Como já foi dito, o IT Army da Ucrânia e muitos outros grupos mais pequenos de *hackers* voluntários formaram-se na sequência direta de apelos das autoridades ucranianas, e parece que os alvos têm sido fornecidos através de canais governamentais[69]. O líder do grupo IT Stand for Ukraine confirmou que a sua equipa trabalhava diretamente com as autoridades ucranianas, mas era independente do Estado[70]. Especulou-se que comandantes russos terão dado assistência e articulado os grupos *hacktivistas* de forma a concertar os seus esforços, mas o líder do Killnet declarou, numa entrevista à BBC, que o grupo era «completamente independente dos serviços especiais russos»[71]. De qualquer forma, a sua participação no conflito ampliou e complexificou a lista de atores beligerantes envolvidos no mesmo.

LIÇÕES PARA AS RELAÇÕES INTERNACIONAIS

Até agora, defendemos que a cibercomponente do conflito tem sido relevante, mas não determinante no esforço de guerra na Ucrânia. Contrariamente às expectativas, a iniciativa de integrar operações militares cibernéticas e cinéticas não tem sido extraordinariamente destrutiva; o ciberespaço não funcionou como um multiplicador de força decisivo. A aparente relutância ou incapacidade da Rússia em levar a cabo operações em grande escala contra a bem defendida Ucrânia pôs em evidência o elevado grau de complexidade que aquelas geralmente envolvem, bem como a dificuldade de as conjugar com as operações cinéticas. No entanto, a verdade é que se retirássemos os elementos cinéticos do campo de batalha, estaríamos a assistir ao mais intenso ciberconflito da história, com ambos os lados a executarem múltiplas operações neste domínio. O ciberespaço faz agora parte integrante da guerra, tal como a utilização de *drones* e de outros sistemas de armas tecnologicamente sofisticados. Contudo, estes não tomaram conta do campo de batalha por completo, coexistindo com instrumentos rudimentares e armas antiquadas, tais como telefones com fios e metralhadoras *vintage*[72]. Essencialmente, o conflito na Ucrânia revela um tipo de guerra em que o passado, o presente e o futuro da tecnologia coexistem. Por conseguinte, a utilização de cibercapacidades tem de ser entendida no âmbito de um ecossistema tecnológico mais vasto, que pode ser simultaneamente sofisticado e anacrónico.

Outro aspecto digno de realce é o facto de não ter havido uma escalada significativa para além das fronteiras do conflito. Nos primeiros meses de guerra, talvez em resposta à coligação de países que se juntaram para ajudar a Ucrânia, a Microsoft detetou intrusões russas em redes de organizações, fora da Ucrânia, de pelo menos 42 países diferentes, com especial incidência nos EUA e na Polónia, o centro logístico da ajuda militar e humanitária à Ucrânia[73]. A atividade contra a Polónia, em particular, pode ter representado uma tentativa de interromper o fornecimento de ajuda e de armas à Ucrânia. As operações de informação têm como alvo a unidade e a cooperação ocidentais contra

a Rússia. O grupo Star Blizzard, ligado ao Estado russo, visou funcionários dos serviços secretos, peritos em assuntos russos, organizações não governamentais e *think tanks* em toda a Europa, predominantemente através de ataques *phishing* personalizados e sofisticados[74]. Apesar da atividade continuada dos intervenientes russos no Ocidente, não houve qualquer ciberataque de larga escala ligado ao conflito fora das suas fronteiras. Até nova indicação, poder-se-á afirmar que a dissuasão dos EUA e dos aliados contra a Rússia tem sido moderadamente eficaz.

Por último, o conflito tem posto em evidência o papel ambíguo dos atores não estatais no conflito. A Ucrânia tem recebido ajuda de empresas e países terceiros, bem como de *hackers* e grupos de *hacktivistas* voluntários. Como demonstrado acima, os atores envolvidos não se limitam ao confronto entre Estados. Várias empresas multinacionais ofereceram assistência à Ucrânia em matéria de capacidades defensivas e ofensivas, nomeadamente a Microsoft, a Google e a AWS. Este apoio foi elogiado por muitos. Sem estas ajudas, a Ucrânia poderia já ter perdido a guerra[75]. No entanto, é de notar que as motivações destas empresas podem não ser inteiramente altruístas; é do interesse de empresas como a Microsoft defenderem-se contra ciberataques, uma vez que o potencial *spillover* de *malware* de rápida disseminação poderia causar danos aos seus próprios sistemas, e o assumir de uma postura moral coloca-as numa posição potencialmente favorável a nível global[76]. De qualquer modo, o envolvimento ativo destas empresas no conflito introduziu a chamada *big tech* como um importante ator nesta guerra[77].

O CONFLITO TEM POSTO EM EVIDÊNCIA O PAPEL AMBÍGUO DOS ATORES NÃO ESTATAIS NO CONFLITO. A UCRÂNIA TEM RECEBIDO AJUDA DE EMPRESAS E PAÍSES TERCEIROS, BEM COMO DE *HACKERS* E GRUPOS DE *HACKTIVISTAS* VOLUNTÁRIOS.

O outro debate em torno dos intervenientes não estatais diz respeito ao envolvimento de grupos de *hackers* voluntários no conflito. Existem dúvidas quanto à legalidade das suas ações, em particular, se são suficientemente organizados para constituírem um grupo armado aos olhos do Manual de Tallinn 2.0 sobre o direito internacional aplicável às ciberoperações e, por conseguinte, passíveis de serem puníveis[78]. Em resposta, o Governo ucraniano tem envidado esforços para legitimar o seu papel a título oficial[79]. O ataque a infraestruturas civis por grupos *hacktivistas* russos e ucranianos também causou controvérsia. Em outubro de 2023, o Comité Internacional da Cruz Vermelha publicou um «Código de Genebra para a Ciberguerra», que repudia ataques *hacktivistas* que afetem civis[80] e que foi aceite pela Killnet e pelo IT Army of Ukraine. Mais uma vez, o envolvimento ativo destes atores levanta questões sobre a importância estratégica destes, mas também sobre o seu estatuto jurídico no conflito; nomeadamente, se podem ser considerados alvos legítimos, e qual o estatuto jurídico dos países onde estes piratas informáticos estão alojados.

Tal como em muitas outras dimensões da guerra e da política externa, o conflito na Ucrânia trouxe novas e importantes noções sobre o papel do ciberespaço na guerra.

CONCLUSÃO

O conflito entre a Ucrânia e a Rússia é um exemplo sem precedentes sobre o modo como as cibercapacidades são utilizadas em contexto de guerra. Antes da invasão, havia um receio generalizado de que a Rússia pudesse lançar ciberataques de elevada sofisticação contra as infraestruturas críticas e os sistemas vitais da Ucrânia, de forma a obter uma vantagem militar e garantir uma vitória rápida. No entanto, as cibercapacidades têm assumido um papel mais secundário no conflito; apesar de uma presença contínua, têm-se centrado predominantemente na perturbação e informação, e não tanto na destruição.

Tomando este conflito como um estudo de caso, podemos tirar várias conclusões sobre a utilização do ciberespaço na guerra. Em primeiro lugar, tem sido demonstrada a relação assimétrica entre as capacidades cinéticas e cibernéticas, nomeadamente, que a destruição física é mais fiável e eficaz, e mais fácil de coordenar do que ciberataques de alta intensidade. Quer devido às defesas ucranianas, quer devido a falhas russas, a maioria dos ciberataques destrutivos contra os sistemas ucranianos não foi bem-sucedida. Um ataque militar contra o mesmo alvo pode ser mais rápido e mais preciso no seu impacto. Os ciberataques de larga escala também levam tempo a preparar e a desenvolver, e a capacidade dos alvos para adaptarem as suas defesas com base na inteligência de ataques limita-os frequentemente a uma única utilização. No que respeita às operações russas de desinformação na Ucrânia, estas têm tido uma eficácia muito limitada. Por último, o conflito pôs em evidência a importância da defesa, da preparação e da resiliência dos sistemas informáticos. Sem as fortes defesas desenvolvidas pela Ucrânia em parceria com os Estados aliados e sem o papel sem precedentes das empresas multinacionais, os ciberataques russos teriam sido mais eficazes e oferecido uma vantagem mais clara para a Rússia.

Este conflito tem igualmente dado várias lições importantes que podem influenciar a forma como os futuros investigadores da área das Relações Internacionais estudam a utilização das cibercapacidades ofensivas na guerra. Sendo este o primeiro grande conflito do século XXI entre forças armadas tecnologicamente sofisticadas, a Rússia e a Ucrânia demonstraram as vantagens potenciais da utilização de ciberataques a par da atividade militar e, sobretudo, as suas limitações. Os receios de uma rápida escalada dos ciberataques revelaram-se infundados, e verificou-se, em geral, uma falta de coordenação entre as operações cinéticas e as cibernéticas. Por outro lado, a Rússia demonstrou o potencial disruptivo dos ataques de baixa intensidade como forma de engajamento persistente, bem como os modos de utilização e manipulação da informação com vista à obtenção de vantagens no teatro de operações. Além disso, a utilização de ciberataques espalhou o conflito para além das fronteiras, com a Rússia a levar a cabo intrusões em redes, operações de espionagem e atividades disruptivas contra aliados ucranianos e países da Organização do Tratado do Atlântico Norte (NATO, na sigla inglesa). Apesar de não haver registo de ataques cibernéticos de larga escala contra

alvos nestes países, a guerra já não está confinada aos Estados em conflito. Por último, abriu o debate sobre o papel ambíguo e sem precedentes dos intervenientes não estatais, nomeadamente no que diz respeito à legalidade e à moralidade das ações de civis e de empresas nesta guerra. RI

Data de receção: 30 de novembro de 2024 | Data de aprovação: 22 de janeiro de 2025

Harry Williams Doutorando no Departamento de Política, Línguas e Estudos Internacionais da Universidade de Bath, como parte do EPSRC Centre for Doctoral Training in Cyber Security. A sua pesquisa centra-se em cibersegurança e em cultura popular e política mundial.

> Department of Politics, Languages and International Studies, Universitay of Bath. North Rd, Claverton Down, Bath BA2 7AY, Reino Unido | hw2384@bath.ac.uk

André Barrinha Professor associado de Relações Internacionais na Universidade de Bath. O seu trabalho foi publicado em revistas como *Contemporary Security Policy*, *International Affairs* e *Journal of European Integration*. Atualmente, dirige a secção Science, Technology and Art in International Relations da International Studies Association.

> Department of Politics, Languages and International Studies, Universitay of Bath. North Rd, Claverton Down, Bath BA2 7AY, Reino Unido | a.barrinha@bath.ac.uk | ORCID: https://orcid.org/0000-0002-6650-3730

NOTAS

1 COURTNEY, William; WILSON, Peter A. – «If Russia invaded Ukraine». RAND. 2021. Consultado em: 23 de agosto de 2024. Disponível em: https://www.rand.org/pubs/commentary/2021/12/expect-shock-and-awe-if-russia-invades-ukraine.html; MILLER, Maggie – «Russian invasion of Ukraine could redefine cyber warfare». POLITICO. 28 de janeiro de 2022. Consultado em: 10 de outubro de 2024. Disponível em: https://www.politico.com/news/2022/01/28/russia-cyber-army-ukraine-00003051.

2 A Rússia ficou em quarto lugar no Índice Nacional de Ciberpoder (*cyber power*) de 2020, destacando-se em áreas como o controlo de informação e capacidades ofensivas. VOO, Julia, *et al.* – *National Cyber Power Index 2020*. Belfer Center, 2020. De forma semelhante, em 2022, ocupou o terceiro lugar no *ranking* geral; este relatório foi publicado seis meses após a invasão, de modo que as ações da Rússia no início do conflito já contribuíram para esta classificação. VOO, Julia, *et al.* – *National Cyber Power Index 2022*. Belfer Center, 2022.

3 BRONK, Chris; COLLINS, Gabriel; WALLACH, Dan – «The Ukrainian information and cyber war». In *Cyber Defense Review*. Vol. 8, N.º 3, 2023, pp. 33-49; MUELLER, Grace B., *et al.* – «Cyber operations during the Russo-Ukrainian War». CSIS. 2023. Consultado em: 13 de julho de 2024. Disponível em: https://www.csis.org/analysis/cyber-operations-during-russo-ukrainian-war; PRZETACZNIK, Jakub; TARPOVA, Simona – *Russia's War on Ukraine*. European Parliament, 2022.

4 BAEZNER, Marie – «Cyber and information warfare in the Ukrainian conflict». Centre for Security Studies. ETH Zurich. 2018. Consultado em: 10 de outubro de 2024. Disponível em: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/20181003_MB_HS_RUS-UKR%20V2_rev.pdf; GREENBERG, Andy – «The untold story of NotPetya, the most devastating cyberattack in history». WIRED. 2018. Consultado em: 3 de outubro de 2024. Disponível em: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

5 DAVIS, Elizabeth Van Wie – *Shadow Warfare: Cyberwar Policy in the United States, Russia and China*. Maryland: Rowman & Littlefield, 2021; GARSON, Melanie – «From script kiddies to cyber warriors». In *Evolving Cyber Operations and Capabilities*. Center for Strategic and International Studies, 2023, pp. 23-32; MASCHMEYER, Lennart – «Assessing hybrid war: separating fact from fiction». In *CSS*. N.º 332, novembro de 2023. Consultado em: 8 de outubro de 2024. Disponível em: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CSSAnalyse332-EN.pdf.

6 A Rússia levou a cabo operações maciças de negação de serviço contra a Estónia em 2007, em retaliação contra a deslocação do Monumento ao Soldado de Bronze, e operações de informação disruptivas contra a Geórgia em 2008, durante a Guerra Russo-Georgiana. MUELLER, Grace B., *et al.* – «Cyber operations during the Russo-Ukrainian War».

7 HAKALA, Janne; MELNYCHUK, Jazlyn – *Russia's Strategy in Cyberspace*. NATO Strategic Communications Centre of Excellence. 2021. Consultado em: 10 de outubro de 2024. Disponível em: https://stratcomcoe.org/cuploads/pfiles/Nato-Cyber-Report_11-06-2021-4f4ce.pdf.

8 GILES, Kier – «Putin does not need to invade Ukraine to get his way». Chatham House. 10 de janeiro de 2022. Consultado em: 10 de outubro de 2024. Disponível em: https://www.chathamhouse.org/2021/12/putin-does-not-need-invade-ukraine-get-his-way.

9 MILLER, Maggie – «Russian invasion of Ukraine could redefine cyber warfare».

10 BRONK, Chris; COLLINS, Gabriel; WALLACH, Dan – «The Ukrainian information and cyber war»; GRZEGORZEWSKI, Mark – «Russia's 2022 cyber-enabled warfare against Ukraine: why Russia failed to perform to expectations». In *The Great Power Competition Volume 5: The Russian Invasion of Ukraine and Implications for the Central Region*. Cham: Springer Nature Switzerland, 2023, pp. 47-73; WILDE, Gavin – «Cyber operations in Ukraine: Russia's unmet expectations». Carnegie Endowment for International Peace. 2022. Consultado em: 5 de setembro de 2024. Disponível em: https://carnegieendowment.org/2022/12/12/cyber-operations-in-ukraine-russia-s-unmet-expectations-pub-88607; WILLETT, Marcus – «The cyber dimension of the Russia-Ukraine War». IISS. Outubro de 2022. Consultado em: 7 de setembro de 2024. Disponível em: https://www.iiss.org/blogs/survival-blog/2022/10/the-cyber-dimension-of-the-russia-ukraine-war

11 CLARKE, Aaron – «Hacking the invasion: the cyber implications of Russia's invasion of Ukraine». Third Way. 25 de abril de 2022. Consultado em: 2 de outubro de 2024. Disponível em: https://www.thirdway.org/memo/hacking-the-invasion-the-cyber-implications-of-russias-invasion-of-ukraine; GREENBERG, Andy – «Ukraine suffered more data-wiping malware in 2022 than anywhere ever». WIRED. 2023. Consultado em: 3 de outubro de 2024. Disponível em: https://www.wired.com/story/ukraine-russia-wiper-malware/; «RUSSIA'S CYBERATTACK activity in the Ukraine». Microsoft Threat Intelligence. 27 de abril de 2022. Consultado em: 4 de outubro de 2024. Disponível em: https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/special-report-ukraine; WATTS, Clint – «Preparing for a Russian cyber offensive against Ukraine this winter». Microsoft. 2022. Consultado em: 7 de outubro de 2024. Disponível em: https://blogs.microsoft.com/on-the-issues/2022/12/03/preparing-russian-cyber-offensive-ukraine/.

12 BATEMAN, Jon – *Russia's Wartime Cyber Operations in Ukraine*. Carnegie Endowment for International Peace. 16 de dezembro de 2022. Consultado em: 3 de setembro de 2024. Disponível em: https://carnegieendowment.org/research/2022/12/russias-wartime-cyber-operations-in-ukraine-military-impacts-influences-and-implications?lang=en.

13 O *malware wiper* foi concebido para destruir ou corromper permanentemente os dados de um sistema visado. EDWARDS, Steven – «What are wipers?». Crowdstrike. 2023. Consultado em: 25 de outubro de 2024. Disponível em: https://www.crowdstrike.com/en-us/cybersecurity-101/malware/wiper-attack/.

14 CLARKE, Aaron – «Hacking the invasion...»; GROSSMAN, Taylor, *et al.* – *The Cyber Dimensions of the Russia-Ukraine War*. European Cyber Conflict Research Initiative, 2023; «RUSSIA'S CYBERATTACK activity in the Ukraine»; STATE SERVICE OF SPECIAL COMMUNICATIONS AND INFORMATION PROTECTION OF UKRAINE – «Russia's cyber tactics H1'2023». 2023. Consultado em: 2 de outubro de 2024. Disponível em: https://cip.gov.ua/services/cm/api/attachment/download?id=60068.

15 GREENBERG, Andy – «Ukraine suffered more data-wiping malware in 2022 than anywhere ever».

16 *Ibidem*.

17 WATLING, Jack; DANYLYUK, Oleksandr; REYNOLDS, Nick – «Preliminary lessons from Russia's unconventional operations during the Russo-Ukrainian War, February 2022-February 2023». RUSI. Fevereiro de 2023. Consultado em: 9 de setembro de 2024. Disponível em: https://www.rusi.org/explore-our-research/publications/special-resources/preliminary-lessons-russias-unconventional-operations-during-russo-ukrainian-war-february-2022.

18 GILES, Kier – «Russian cyber and information warfare in practice». Chatham House. Dezembro de 2023. Consultado em: 9 de outubro de 2024. Disponível em: https://www.chathamhouse.org/2023/12/russian-cyber-and-information-warfare-practice/01-introduction; MCLAUGHLIN, Jenna – «An inside look at Ukraine's cyber war with Russia». NPR. 2023. Consultado em: 11 de outubro de 2024. Disponível em: https://www.npr.org/2023/09/04/1197548380/an-inside-look-at-ukraines-cyber-war-with-russia.

19 Cyber Incident Response Team.

20 BATEMAN, Jon – *Russia's Wartime Cyber Operations in Ukraine*; TIDY, Joe – «Ukrainian power grid "lucky" to with-

stand Russian cyber-attack». BBC News. 12 de abril de 2022. Consultado em: 12 de outubro de 2024. Disponível em: https://www.bbc.com/news/technology-61085480.

21 GREENBERG, Andy – «Sandworm hackers caused another blackout in Ukraine – during a missile strike». WIRED. 2023. Consultado em: 3 de outubro de 2024. Disponível em: https://www.wired.com/story/sandworm-ukraine-third-blackout-cyberattack/; «SANDWORM DISRUPTS power in Ukraine using a novel attack against operational technology». Mandiant. 2023. Consultado em: 10 de outubro de 2024. Disponível em: https://cloud.google.com/blog/topics/threat-intelligence/sandworm-disrupts-power-ukraine-operational-technology; «BLACKOUTS AFTER Russian strikes deepen Ukraine's concerns before winter». Reuters. 10 de outubro de 2022. Consultado em: 10 de outubro de 2024. Disponível em: https://www.reuters.com/world/europe/blackouts-after-russian-strikes-deepen-ukraines-concerns-before-winter-2022-10-10/.

22 BALMFORTH, Tom – «Russian hackers were inside Ukraine telecoms giant for months». Reuters. 4 de janeiro de 2024. Consultado em: 10 de outubro de 2024. Disponível em: https://www.reuters.com/world/europe/russian-hackers-were-inside-ukraine-telecoms-giant-months-cyber-spy-chief-2024-01-04/; HUNDER, Max; LANDAY, Jonathan; BERN, Stefaniia – «Ukraine's top mobile operator hit by biggest cyberattack of war». Reuters. 12 de dezembro de 2023. Consultado em: 10 de outubro de 2024. Disponível em: https://www.reuters.com/technology/cybersecurity/ukraines-biggest-mobile-operator-suffers-massive-hacker-attack-statement-2023-12-12/.

23 «RUSSIA'S CYBERATTACK activity in the Ukraine».

24 BATEMAN, Jon – *Russia's Wartime Cyber Operations in Ukraine*.

25 «SIGNIFICANT CYBER incidents». CSIS. 2024. Consultado em: 4 de setembro de 2024. Disponível em: https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents.

26 LYNGAAS, Sean – «Russian military hackers take aim at Ukrainian soldiers' battle plans, US and allies say». CNN Politics. 31 de agosto de 2023. Consultado em: 11 de outubro de 2024. Disponível em: https://edition.cnn.com/2023/08/31/politics/military-hackers-russia-ukraine/index.html; WILDE, Gavin – «Cyber operations in Ukraine…».

27 «SIGNIFICANT CYBER incidents».

28 WATLING, Jack; DANYLYUK, Oleksandr; REYNOLDS, Nick – «Preliminary lessons from Russia's unconventional operations during the Russo-Ukrainian War…».

29 LEVITE, Ariel – «Integrating cyber into warfighting: some early takeaways from the Ukraine conflict». Carnegie Endowment for International Peace. 18 de abril de 2023. Consultado em: 28 de setembro de 2024. Disponível em: https://carnegieendowment.org/2023/04/18/integrating-cyber-into-warfighting-some-early-takeaways-from-ukraine-conflict-pub-89544; WILDE, Gavin – «Cyber operations in Ukraine…».

30 «RUSSIA'S CYBERATTACK activity in the Ukraine».

31 SMITH, Brad – «Defending Ukraine: early lessons from the cyber war». Microsoft. 2022. Consultado em: 7 de outubro de 2024. Disponível em: https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/.

32 ALLYN, Bobby – «Deepfake video of Zelenskyy could be "tip of the iceberg" in info war, experts warn». NPR. 16 de março de 2022. Consultado em: 11 de outubro de 2024. Disponível em: https://www.npr.org/2022/03/16/1087062648/deepfake-video-zelenskyy-experts-war-manipulation-ukraine-russia.

33 «SIGNIFICANT CYBER incidents».

34 *Ibidem*; WATTS, Clint – «Russian influence and cyber operations adapt for long haul and exploit war fatigue». Microsoft. 2023. Consultado em: 7 de outubro de 2024. Disponível em: https://blogs.microsoft.com/on-the-issues/2023/12/07/russia-ukraine-digital-threat-celebrity-cameo-mtac/.

35 CABINET OF MINISTERS OF UKRAINE – «The invaders have disabled communication and the Internet in Kherson region and part of Zaporizhzhia region». Government Portal. 2022. Consultado em: 5 de julho de 2024. Disponível em: https://www.kmu.gov.ua/en/news/derzhspeczvyazku-okupanti-vidklyuchili-zvyazok-ta-internet-v-hersonskij-ta-chastini-zaporizkoyi-oblastej; «RUSSIA REROUTES internet traffic in occupied Ukraine to its infrastructure». Reuters. 2 de maio de 2022. Consultado em: 13 de outubro de 2024. Disponível em: https://www.reuters.com/world/europe/russia-reroutes-internet-traffic-occupied-ukraine-its-infrastructure-2022-05-02/.

36 «KHERSON: HOW is Russia imposing its rule in occupied Ukraine?». BBC News. 11 de maio de 2022. Consultado em: 1 de outubro de 2024. Disponível em: https://www.bbc.co.uk/news/world-61338617; STATE SERVICE OF SPECIAL COMMUNICATIONS AND INFORMATION PROTECTION OF UKRAINE – «The invaders have disabled communication and the internet in Kherson region and part of Zaporizhzhia region». Government Portal. 2022. Consultado em: 2 de outubro de 2024. Disponível em: https://www.kmu.gov.ua/en/news/derzhspeczvyazku-okupanti-vidklyuchili-zvyazok-ta-internet-v-hersonskij-ta-chastini-zaporizkoyi-oblastej.

37 BRONK, Chris; COLLINS, Gabriel; WALLACH, Dan – «The Ukrainian information and cyber war»; MUELLER, Grace B., *et al.* – «Cyber operations during the Russo-Ukrainian War».

38 MCLAUGHLIN, Jenna – «Ukrainian hacktivists fight back against Russia as cyber conflict deepens». NPR. 2023. Consultado em: 11 de outubro de 2024. Disponível em: https://www.npr.org/2023/11/21/1214170140/ukraine-hacktivists-cyber-russia-war.

39 FENDORF, Kyle; MILLER, Jessie – «Tracking cyber operations and actors in the Russia-Ukraine War». Council on Foreign Relations. 2022. Consultado em: 11 de outubro de 2024. Disponível em: https://www.cfr.org/blog/tracking-cyber-operations-and-actors-russia-ukraine-war.

40 BURGESS, Matt – «Russia is being hacked at an unprecedented scale». WIRED. 2022. Consultado em: 11 de outubro de 2024. Disponível em: https://www.wired.com/story/russia-hacked-attacks/; MCLAUGHLIN, Jenna – «Ukrainian hacktivists fight back against Russia as cyber conflict deepens».

41 «HUR HACKS Russian Defense ministry, gets access to classified documents». Kyiv Post. 4 de março de 2024. Consultado em: 11 de outubro de 2024. Disponível em: https://www.kyivpost.com/post/28979.

42 «UKRAINIAN HACKERS launch cyberattacks on subsidiary of major Russian Telecom». Kyiv Post. 28 de abril de 2024. Consultado em: 11 de outubro de 2024. Disponível em: https://www.kyivpost.com/post/31798; ZAKHARCHENKO, Kateryna – «HUR cyberattack hits Russian internet providers in occupied Crimea». Kyiv Post. 26 de junho de 2024. Consultado em: 11 de outubro de 2024. Disponível em: https://www.kyivpost.com/post/34917.

43 GILES, Kier – «Russian cyber and information warfare in practice»; LONERGAN, Erica D., *et al.* – «Putin's invasion of Ukraine didn't rely on cyber-warfare. Here's why». In *The Washington Post*. 7 de março de 2022. Consultado em: 9 de outubro de 2024. Disponível em: https://www.washingtonpost.com/politics/2022/03/07/putins-invasion-ukraine-didnt-rely-cyber-warfare-heres-why/.

44 BATEMAN, Jon – *Russia's Wartime Cyber Operations in Ukraine*; «RUSSIA RAINS missiles down on Ukraine's capital and other cities in retaliation for Crimea bridge blast». CBS News. 10 de outubro de 2022. Consultado em: 1 de outubro de 2024. Disponível em: https://www.cbsnews.com/news/ukraine-news-russia-war-kyiv-missile-attack-putin-crimea-bridge/; HOWARD, Jacqueline – «Russia launches "massive" overnight attack on Ukraine power grid». BBC News. 22 de junho de 2024. Consultado em: 11 de outubro de 2024. Disponível em: https://www.bbc.com/news/articles/czvvj4j-4p8ro; «UKRAINE'S ENERGY security and the coming winter». IEA. 2024. Consultado em: 10 de outubro de 2024. Disponível em: https://www.iea.org/reports/ukraines-energy-security-and-the-coming-winter.

45 LONERGAN, Erica D., *et al.* – «Putin's invasion of Ukraine didn't rely on cyber-warfare…».

46 GILES, Kier – «Russian cyber and information warfare in practice».

47 A Operação Pomar, levada a cabo por Israel contra alvos nucleares na Síria, em 2007, é um bom exemplo desta exceção.

48 RID, Thomas – «Cyber war will not take place». In *Journal of Strategic Studies*. Vol. 35, N.º 1, 2012, pp. 5-32.

49 GILES, Kier – «Russian cyber and information warfare in practice».

50 «THE HEAD of GCHQ says Vladimir Putin is losing the information war in Ukraine». The Economist. 18 de abril de 2022. Consultado em: 7 de outubro de 2024. Disponível em: https://www.economist.com/by-invitation/2022/08/18/the-head-of-gchq-says-vladimir-putin-is-losing-the-information-war-in-ukraine.

51 GILES, Kier – «Russian cyber and information warfare in practice».

52 «CYBERSECURITY». USAID. 2022. Consultado em: 1 de outubro de 2024. Disponível em: https://www.usaid.gov/ukraine/fact-sheets/aug-05-2022-cybersecurity.

53 «U.S. SUPPORT for connectivity and cybersecurity in Ukraine». U.S. Department of State. Office of the Spokesperson. 2022. Consultado em: 27 de setembro de 2024. Disponível em: https://www.state.gov/u-s-support-for-connectivity-and-cybersecurity-in-ukraine/.

54 MADIEGA, Tambiama – *Russia's War on Ukraine: Digital Issues*. European Parliament, 2022; «U.S. SUPPORT for connectivity and cybersecurity in Ukraine».

55 «RUSSIA'S CYBERATTACK activity in the Ukraine».

56 SMITH, Brad – «Defending Ukraine…».

57 WATTS, Clint – «Preparing for a Russian cyber offensive against Ukraine this winter».

58 «SAFEGUARDING UKRAINE'S data to preserve its present and build its future». Amazon. 2022. Consultado em: 10 de outubro de 2024. Disponível em: https://www.aboutamazon.com/news/aws/safeguarding-ukraines-data-to-preserve-its-present-and-build-its-future.

59 «HOW TECHNOLOGY helped Ukraine resist during wartime». Microsoft. 2023. Consultado em: 14 de outubro de 2024. Disponível em: https://news.microsoft.com/en-cee/2023/01/20/how-technology-helped-ukraine-resist-during-wartime/.

60 MARQUARDT, Alex – «Musk's SpaceX says it can no longer pay for critical satellite services in Ukraine, asks Pentagon to pick up the tab». CNN Politics. 13 de outubro de 2022. Consultado em: 14 de outubro de 2024. Disponível em: https://edition.cnn.com/2022/10/13/politics/elon-musk-spacex-starlink-ukraine/index.html.

61 GILES, Kier – «Russian cyber and information warfare in practice».

62 *Ibidem*; MARQUARDT, Alex – «Musk's SpaceX says it can no longer pay for critical satellite services in Ukraine…».

63 RENDER-KATOLIK, Aiden – «The IT Army of Ukraine». CSIS. 2023. Consultado em: 14 de outubro de 2024. Disponível em: https://www.csis.org/blogs/strategic-technologies-blog/it-army-ukraine.

64 VU, Anh V., *et al.* – «Getting bored of cyberwar: exploring the role of low-level cybercrime actors in the Russia-Ukraine conflict». In *WWW '24: Proceedings of the ACM Web Conference 2024*, pp. 1596-1607.

65 SHORE, Jennifer – «Don't underestimate Ukraine's volunteer hackers». Foreign Policy. 11 de abril de 2022. Consultado em: 14 de outubro de 2024. Disponível em: https://foreignpolicy.com/2022/04/11/russia-cyberwarfare-us-ukraine-volunteer-hackers-it-army/.

66 INSKEEP, Steve; MCLAUGHLIN, Jenna – «Russia-Ukraine escalation: Ukrainian "hacktivists" battle Russia online». NPR. 2023. Consultado em: 14 de outubro de 2024. Disponível em: https://www.npr.org/2023/11/20/1214109074/russia-ukraine-cyber-escalation-ukrainian-hacktivists-battle-russia-online; MCLAUGHLIN, Jenna – «Ukrainian hacktivists fight back against Russia as cyber conflict deepens»; TIDY, Joe – «Meet the hacker armies on Ukraine's cyber front line». BBC News. 15 de abril de 2023. Consultado em: 9 de outubro de 2024. Disponível em: https://www.bbc.com/news/technology-65250356.

67 FENDORF, Kyle; MILLER, Jessie – «Tracking cyber operations and actors in the Russia-Ukraine War».

68 «RUSSIAN THREAT actors dig in, prepare to seize on war fatigue». Microsoft Threat Intelligence. 2023. Consultado em: 9 de outubro de 2024. Disponível em: https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/russian-threat-actors-dig-in-prepare-to-seize-on-war-fatigue; TIDY, Joe – «Meet the hacker armies on Ukraine's cyber front line».

69 BURGESS, Matt – «Ukraine's volunteer "IT Army" is hacking in uncharted territory». WIRED. 2022. Consultado em: 4 de outubro de 2024. Disponível em: https://www.wired.com/story/ukraine-it-army-russia-war-cyberattacks-ddos/.

70 TIDY, Joe – «Meet the hacker armies on Ukraine's cyber front line».

71 *Ibidem*.

72 BEALE, Jonathan – «Ukraine war: how old tech is helping Ukraine avoid detection». BBC News. 3 de maio de 2023. Consultado em: 25 de outubro de 2024. Disponível em: https://www.bbc.co.uk/news/world-europe-65458263; BROWN, Steve – «Ukraine makes best operational use of vintage machine guns». Kyiv Post. 29 de julho de 2024. Consultado em: 28 de outubro de 2024. Disponível em: https://www.kyivpost.com/post/36536.

73 «SIGNIFICANT CYBER incidents»; SMITH, Brad – «Defending Ukraine…».

74 MASADA, Steven – «Protecting democratic institutions from cyber threats». Microsoft. 2024. Consultado em: 7 de outubro de 2024. Disponível em: https://blogs.microsoft.com/on-the-issues/2024/10/03/protecting-democratic-institutions-from-cyber-threats/.

75 «RUSSIA'S CYBERATTACK activity in the Ukraine».

76 VOO, Julia – «Lessons from Ukraine's cyber defense and implications for future conflict». In *Evolving Cyber Operations and Capabilities*. Center for Strategic and International Studies, 2023, pp. 15-22.

77 KRAMER, Franklin D. – «The sixth domain: the role of the private sector in warfare». Atlantic Council. 2023. Consultado em: 14 de outubro de 2024. Disponível em: https://www.atlanticcouncil.org/in-depth-research-reports/report/the-sixth-domain-the-role-of-the-private-sector-in-warfare/.

78 BIGGERSTAFF, William Casey – «The status of Ukraine's "IT Army" under the law of armed conflict». Lieber Institute West Point. 2023. Consultado em: 14 de outubro de 2024. Disponível em: https://lieber.westpoint.edu/status-ukraines-it-army-law-armed-conflict/; SCHMITT, Michael N., ed. – *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, 2017.

79 MCLAUGHLIN, Jenna – «Ukrainian hacktivists fight back against Russia as cyber conflict deepens».

80 TIDY, Joe – «Ukrainian cyber conflict: hacking gangs vow to de-escalate». BBC News. 6 de outubro de 2023. Consultado em: 14 de outubro de 2024. Disponível em: https://www.bbc.com/news/technology-67029296.

BIBLIOGRAFIA

ALLYN, Bobby – «Deepfake video of Zelenskyy could be "tip of the iceberg" in info war, experts warn». NPR. 16 de março de 2022. Consultado em: 11 de outubro de 2024. Disponível em: https://www.npr.org/2022/03/16/1087062648/deepfake-video-zelenskyy-experts-war-manipulation-ukraine-russia.

BAEZNER, Marie – «Cyber and information warfare in the Ukrainian conflict». Centre for Security Studies. ETH Zurich. 2018. Consultado em: 10 de outubro de 2024. Disponível em: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/20181003_MB_HS_RUS-UKR%20V2_rev.pdf.

BALMFORTH, Tom – «Russian hackers were inside Ukraine telecoms giant for months». Reuters. 4 de janeiro de 2024. Consultado em: 10 de outubro de 2024. Disponível em: https://www.reuters.com/world/europe/russian-hackers-were-inside-ukraine-telecoms-giant-months-cyber-spy-chief-2024-01-04/.

BATEMAN, Jon – *Russia's Wartime Cyber Operations in Ukraine*. Carnegie Endowment for International Peace. 16 de dezembro de 2022. Consultado em: 3 de setembro de 2024. Disponível em: https://carnegieendowment.org/research/2022/12/russias-wartime-cyber-operations-in-ukraine-military-impacts-influences-and-implications?lang=en.

BEALE, Jonathan – «Ukraine war: how old tech is helping Ukraine avoid detection». BBC News. 2023. Consultado em: 25 de outubro de 2024. Disponível em: https://www.bbc.co.uk/news/world-europe-65458263.

BIGGERSTAFF, William Casey – «The status of Ukraine's "IT Army" under the law of armed conflict». Lieber Institute West Point. 2023. Consultado em: 14 de outubro de 2024. Disponível em: https://lieber.westpoint.edu/status-ukraines-it-army-law-armed-conflict/.

«BLACKOUTS AFTER Russian strikes deepen Ukraine's concerns before winter». Reuters. 10 de outubro de 2022. Consultado em: 10 de outubro de 2024. Disponível em: https://www.reuters.com/world/europe/blackouts-after-russian-strikes-deepen-ukraines-concerns-before-winter-2022-10-10/.

BRONK, Chris; COLLINS, Gabriel; WALLACH, Dan – «The Ukrainian information and cyber war». In *Cyber Defense Review*. Vol. 8, N.º 3, 2023, pp. 33-49.

BROWN, Steve – «Ukraine makes best operational use of vintage machine guns». Kyiv Post. 2024. Consultado em: 28 de outubro de 2024. Disponível em: https://www.kyivpost.com/post/36536.

BURGESS, Matt – «Russia is being hacked at an unprecedented scale». WIRED. 2022. Consultado em: 11 de outubro de 2024. Disponível em: https://www.wired.com/story/russia-hacked-attacks/.

BURGESS, Matt – «Ukraine's volunteer "IT Army" is hacking in uncharted territory». WIRED. 2022. Consultado em: 4 de outubro de 2024. Disponível em: https://www.wired.com/story/ukraine-it-army-russia-war-cyberattacks-ddos/.

CABINET OF MINISTERS OF UKRAINE – «The invaders have disabled communication and the Internet in Kherson region and part of Zaporizhzhia region». Government Portal. 2022. Consultado em: 5 de julho de 2024. Disponível em: https://www.kmu.gov.ua/en/news/derzhspeczvyazku-okupanti-vidklyuchili-zvyazok-ta-internet-v-hersonskij-ta-chastini-zaporizkoyi-oblastej.

CLARKE, Aaron – «Hacking the invasion: the cyber implications of Russia's invasion of Ukraine». Third Way. 25 de abril de 2022. Consultado em: 2 de outubro de 2024. Disponível em: https://www.thirdway.org/memo/hacking-the-invasion-the-cyber-implications-of-russias-invasion-of-ukraine.

COURTNEY, William; WILSON, Peter A. – «If Russia invaded Ukraine». RAND. 8 de dezembro de 2021. Consultado em: 23 de agosto de 2024. Disponível em: https://www.rand.org/pubs/commentary/2021/12/expect-shock-and-awe-if-russia-invades-ukraine.html.

«CYBERSECURITY». USAID. 2022. Consultado em: 1 de outubro de 2024. Disponível em: https://www.usaid.gov/ukraine/fact-sheets/aug-05-2022-cybersecurity.

DAVIS, Elizabeth Van Wie – *Shadow Warfare: Cyberwar Policy in the United States, Russia and China*. Maryland: Rowman & Littlefield, 2021.

EDWARDS, Steven – «What are wipers?». Crowdstrike. 20 de dezembro de 2023. Consultado em: 25 de outubro de 2024. Disponível em: https://www.crowdstrike.com/en-us/cybersecurity-101/malware/wiper-attack/.

FENDORF, Kyle; MILLER, Jessie – «Tracking cyber operations and actors in the Russia-Ukraine War». Council on Foreign Relations. 24 de março de 2022. Consultado em: 11 de outubro de 2024. Disponível em: https://www.cfr.org/blog/tracking-cyber-operations-and-actors-russia-ukraine-war.

GARSON, Melanie – «From script kiddies to cyber warriors». In *Evolving Cyber Operations and Capabilities*. Center for Strategic and International Studies, maio de 2023, pp. 23-32.

GILES, Kier – «Putin does not need to invade Ukraine to get his way». Chatham House. 10 de janeiro de 2022. Consultado em: 10 de outubro de 2024. Disponível em: https://www.chathamhouse.org/2021/12/putin-does-not-need-invade-ukraine-get-his-way.

GILES, Kier – «Russian cyber and information warfare in practice». Chatham House. 14 de dezembro de 2023. Consultado em: 9 de outubro de 2024. Disponível em: https://www.chathamhouse.org/2023/12/russian-cyber-and-information-warfare-practice/01-introduction.

GREENBERG, Andy – «The untold story of NotPetya, the most devastating cyberattack in history». WIRED. 2018. Consultado em: 3 de outubro de 2024. Disponível em: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

GREENBERG, Andy – «Sandworm hackers caused another blackout in Ukraine – during a missile strike». WIRED. 22 de agosto de 2023. Consultado em: 3 de outubro de 2024. Disponível em: https://www.wired.com/story/sandworm-ukraine-third-blackout-cyberattack/.

GREENBERG, Andy – «Ukraine suffered more data-wiping malware in 2022 than anywhere ever». WIRED. 22 de fevereiro de 2023. Consultado em: 3 de outubro de 2024. Disponível em: https://www.wired.com/story/ukraine-russia-wiper-malware/.

GROSSMAN, Taylor; KAMINSKA, Monica; SHIRES, James; SMEETS, Max – *The Cyber Dimensions of the Russia-Ukraine War*. European Cyber Conflict Research Initiative, 2023.

GRZEGORZEWSKI, Mark – «Russia's 2022 cyber-enabled warfare against Ukraine: why Russia failed to perform to expectations». In *The Great Power Competition Volume 5: The Russian Invasion of Ukraine and Implications for the Central Region*. Cham: Springer Nature Switzerland, 2023, pp. 47-73.

HAKALA, Janne; MELNYCHUK, Jazlyn – *Russia's Strategy in Cyberspace*. NATO Strategic Communications Centre of Excellence. 2021. Consultado em: 10 de outubro de 2024. Disponível em: https://stratcomcoe.org/cuploads/pfiles/Nato-Cyber-Report_11-06-2021-4f4ce.pdf.

«HOW TECHNOLOGY helped Ukraine resist during wartime». Microsoft. 20 de janeiro de 2023. Consultado em: 14 de outubro de 2024. Disponível em: https://news.microsoft.com/en-cee/2023/01/20/how-technology-helped-ukraine-resist-during-wartime/.

HOWARD, Jacqueline – «Russia launches "massive" overnight attack on Ukraine power grid». BBC News. 22 de junho de 2024. Consultado em: 11 de outubro de 2024. Disponível em: https://www.bbc.com/news/articles/czvvj4j4p8ro.

HUNDER, Max; LANDAY, Jonathan; BERN,

Stefaniia – «Ukraine's top mobile operator hit by biggest cyberattack of war». Reuters. 12 de dezembro de 2023. Consultado em: 10 de outubro de 2024. Disponível em: https://www.reuters.com/technology/cybersecurity/ukraines-biggest-mobile-operator-suffers-massive-hacker-attack-statement-2023-12-12/.

«HUR HACKS Russian Defense ministry, gets access to classified documents». Kyiv Post. 4 de março de 2024. Consultado em: 11 de outubro de 2024. Disponível em: https://www.kyivpost.com/post/28979.

INSKEEP, Steve; MCLAUGHLIN, Jenna – «Russia-Ukraine escalation: Ukrainian "hacktivists" battle Russia online». NPR. 20 de novembro de 2023. Consultado em: 14 de outubro de 2024. Disponível em: https://www.npr.org/2023/11/20/1214109074/russia-ukraine-cyber-escalation-ukrainian-hacktivists-battle-russia-online.

«KHERSON: HOW is Russia imposing its rule in occupied Ukraine?». BBC News. 11 de maio de 2022. Consultado em: 1 de outubro de 2024. Disponível em: https://www.bbc.co.uk/news/world-61338617.

KRAMER, Franklin D. – «The sixth domain: the role of the private sector in warfare». Atlantic Council. 4 de outubro de 2023. Consultado em: 14 de outubro de 2024. Disponível em: https://www.atlanticcouncil.org/in-depth-research-reports/report/the-sixth-domain-the-role-of-the-private-sector-in-warfare/.

LEVITE, Ariel – «Integrating cyber into warfighting: some early takeaways from the Ukraine conflict». Carnegie Endowment for International Peace. 18 de abril de 2023. Consultado em: 28 de setembro de 2024. Disponível em: https://carnegieendowment.org/2023/04/18/integrating-cyber-into-warfighting-some-early-takeaways-from-ukraine-conflict-pub-89544.

LONERGAN, Erica D.; LONERGAN, Shawn W.; VALERIANO, Brandon; JENSEN, Benjamin – «Putin's invasion of Ukraine didn't rely on cyberwarfare. Here's why». In *The Washington Post*. 7 de março de 2022. Consultado em: 9 de outubro de 2024. Disponível em: https://www.washingtonpost.com/politics/2022/03/07/putins-invasion-ukraine-didnt-rely-cyber-warfare-heres-why/.

LYNGAAS, Sean – «Russian military hackers take aim at Ukrainian soldiers' battle plans, US and allies say». CNN Politics. 31 de agosto de 2023. Consultado em: 11 de outubro de 2024. Disponível em: https://edition.cnn.com/2023/08/31/politics/military-hackers-russia-ukraine/index.html.

MADIEGA, Tambiama – *Russia's War on Ukraine: Digital Issues*. European Parliament, 2022.

MARQUARDT, Alex – «Musk's SpaceX says it can no longer pay for critical satellite services in Ukraine, asks Pentagon to pick up the tab». CNN Politics. 13 de outubro de 2022. Consultado em: 14 de outubro de 2024. Disponível em: https://edition.cnn.com/2022/10/13/politics/elon-musk-spacex-starlink-ukraine/index.html.

MASADA, Steven – «Protecting democratic institutions from cyber threats». Microsoft. 3 de outubro de 2024. Consultado em: 7 de outubro de 2024. Disponível em: https://blogs.microsoft.com/on-the-issues/2024/10/03/protecting-democratic-institutions-from-cyber-threats/.

MASCHMEYER, Lennart – «Assessing hybrid war: separating fact from fiction». In *CSS*. N.º 332, novembro de 2023. Consultado em: 8 de outubro de 2024. Disponível em: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CSSAnalyse332-EN.pdf.

MCLAUGHLIN, Jenna – «An inside look at Ukraine's cyber war with Russia». NPR. 4 de setembro de 2023. Consultado em: 11 de outubro de 2024. Disponível em: https://www.npr.org/2023/09/04/1197548380/an-inside-look-at-ukraines-cyber-war-with-russia.

MCLAUGHLIN, Jenna – «Ukrainian hacktivists fight back against Russia as cyber conflict deepens». NPR. 21 de novembro de 2023. Consultado em: 11 de outubro de 2024. Disponível em: https://www.npr.org/2023/11/21/1214170140/ukraine-hacktivists-cyber-russia-war.

MILLER, Maggie – «Russian invasion of Ukraine could redefine cyber warfare». POLITICO. 28 de janeiro de 2022. Consultado em: 10 de outubro de 2024. Disponível em: https://www.politico.com/news/2022/01/28/russia-cyber-army-ukraine-00003051.

MUELLER, Grace B.; JENSEN, Benjamin; VALERIANO, Brandon; MANESS, Ryan C.; MACIAS, Jose M. – «Cyber operations during the Russo-Ukrainian War». CSIS. 13 de julho de 2023. Consultado em: 13 de julho de 2024. Disponível em: https://www.csis.org/analysis/cyber-operations-during-russo-ukrainian-war.

PRZETACZNIK, Jakub; TARPOVA, Simona – *Russia's War on Ukraine*. European Parliament, 2022.

RENDER-KATOLIK, Aiden – «The IT Army of Ukraine». CSIS. 15 de agosto de 2023. Consultado em: 14 de outubro de 2024. Disponível em: https://www.csis.org/blogs/strategic-technologies-blog/it-army-ukraine.

RID, Thomas – «Cyber war will not take place». In *Journal of Strategic Studies*. Vol. 35, N.º 1, 2012, pp. 5-32.

«RUSSIA RAINS missiles down on Ukraine's capital and other cities in retaliation for Crimea bridge blast». CBS News. 10 de outubro de 2022. Consultado em: 1 de outubro de 2024. Disponível em: https://www.cbsnews.com/news/ukraine-news-russia-war-kyiv-missile-attack-putin-crimea-bridge/.

«RUSSIA REROUTES internet traffic in occupied Ukraine to its infrastructure». Reuters. 2 de maio de 2022. Consultado em: 13 de outubro de 2024. Disponível em: https://www.reuters.com/world/europe/russia-reroutes-internet-traffic-occupied-ukraine-its-infrastructure-2022-05-02/.

«RUSSIA'S CYBERATTACK activity in the Ukraine». Microsoft Threat Intelligence. 27 de abril de 2022. Consultado em: 4 de outubro de 2024. Disponível em: https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/special-report-ukraine.

«RUSSIAN THREAT actors dig in, prepare to seize on war fatigue». Microsoft Threat Intelligence. 7 de dezembro de 2023. Consultado em: 9 de outubro de 2024. Disponível em: https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/russian-threat-actors-dig-in-prepare-to-seize-on-war-fatigue.

«SAFEGUARDING UKRAINE'S data to preserve its present and build its future». Amazon. 2022. Consultado em: 10 de outubro de 2024. Disponível em: https://www.aboutamazon.com/news/aws/safeguarding-ukraines-data-to-preserve-its-present-and-build-its-future.

«SANDWORM DISRUPTS power in Ukraine using a novel attack against operational technology». Mandiant. 2023. Consultado em: 10 de outubro de 2024. Disponível em: https://cloud.google.com/blog/topics/threat-intelligence/sandworm-disrupts-power-ukraine-operational-technology.

SCHMITT, Michael N., ed. – *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, 2017.

SHORE, Jennifer – «Don't underestimate Ukraine's volunteer hackers». Foreign Policy. 11 de abril de 2022. Consultado em: 14 de outubro de 2024. Disponível em: https://foreignpolicy.com/2022/04/11/russia-cyberwarfare-us-ukraine-volunteer-hackers-it-army/.

«SIGNIFICANT CYBER incidents». CSIS. 2024. Consultado em: 4 de setembro de 2024. Disponível em: https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents.

SMITH, Brad – «Defending Ukraine: early lessons from the cyber war». Microsoft. 2022. Consultado em: 7 de outubro de 2024. Disponível em: https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/.

STATE SERVICE OF SPECIAL COMMUNICATIONS AND INFORMATION PROTECTION OF UKRAINE – «The invaders have disabled communication and the internet in Kherson region and part of Zaporizhzhia region». Government Portal. 2022. Consultado em: 2 de outubro de 2024. Disponível em: https://www.kmu.gov.ua/en/news/derzhspeczvyazku-okupanti-vidklyuchili-zvyazok-ta-internet-v-hersonskij-ta-chastini-zaporizkoyi-oblastej.

STATE SERVICE OF SPECIAL COMMUNICATIONS AND INFORMATION PROTECTION OF UKRAINE – «Russia's cyber tactics H1'2023». 2023. Consultado em: 2 de outubro de 2024. Disponível em: https://cip.gov.ua/services/cm/api/attachment/download?id=60068.

«THE HEAD of GCHQ says Vladimir Putin is losing the information war in Ukraine». The Economist. 18 de abril de 2022. Consultado em: 7 de outubro de 2024. Disponível em: https://www.economist.com/by-invitation/2022/08/18/the-head-of-gchq-says-vladimir-putin-is-losing-the-information-war-in-ukraine.

TIDY, Joe – «Ukrainian power grid "lucky" to withstand Russian cyber-attack». BBC News. 12 de abril de 2022. Consultado em: 12 de outubro de 2024. Disponível em: https://www.bbc.com/news/technology-61085480.

TIDY, Joe – «Meet the hacker armies on Ukraine's cyber front line». BBC News. 15 de abril de 2023. Consultado em: 9 de outubro de 2024. Disponível em: https://www.bbc.com/news/technology-65250356.

TIDY, Joe – «Ukrainian cyber conflict: hacking gangs vow to de-escalate». BBC News. 6 de outubro de 2023. Consultado em: 14 de outubro de 2024. Disponível em: https://www.bbc.com/news/technology-67029296.

«U.S. SUPPORT for connectivity and cybersecurity in Ukraine». U.S. Department of State. Office of the Spokesperson. 2022. Consultado em: 27 de setembro de 2024. Disponível em: https://www.state.gov/u-s-support-for-connectivity-and-cybersecurity-in-ukraine/.

«UKRAINE'S ENERGY security and the coming winter». IEA. 2024. Consultado em: 10 de outubro de 2024. Disponível em: https://www.iea.org/reports/ukraines-energy-security-and-the-coming-winter.

«UKRAINIAN HACKERS launch cyberattacks on subsidiary of major Russian Telecom». Kyiv Post. 28 de abril de 2024. Consultado em: 11 de outubro de 2024. Disponível em: https://www.kyivpost.com/post/31798.

VOO, Julia – «Lessons from Ukraine's cyber defense and implications for future conflict». In *Evolving Cyber Operations and Capabilities*. Center for Strategic and International Studies, 2023, pp. 15-22.

VOO, Julia; HEMANI, Irfan; CASSIDY, Dan; ROSENBACH, Eric – *National Cyber Power Index 2022*. Belfer Center, 2022.

VOO, Julia; HEMANI, Irfan; JONES, Simon; DESOMBRE, Winnona; CASSIDY, Dan; SCHWARZENBACH, Anina – *National Cyber Power Index 2020*. Belfer Center, 2020.

VU, Anh V.; THOMAS, Daniel R.; COLLIER, Ben; HUTCHINGS, Alice; CLAYTON, Richard; ANDERSON, Ross – «Getting bored of cyberwar: exploring the role of low-level cybercrime actors in the Russia-Ukraine conflict». In *WWW '24: Proceedings of the ACM Web Conference 2024*, pp. 1596-1607.

WATLING, Jack; DANYLYUK, Oleksandr; REYNOLDS, Nick – «Preliminary lessons from Russia's unconventional operations during the Russo-Ukrainian War, February 2022-February 2023». RUSI. Fevereiro de 2023. Consultado em: 9 de setembro de 2024. Disponível em: https://www.rusi.org/explore-our-research/publications/special-resources/preliminary-lessons-russias-unconventional-operations-during-russo-ukrainian-war-february-2022.

WATTS, Clint – «Preparing for a Russian cyber offensive against Ukraine this winter». Microsoft. 2022. Consultado em: 7 de outubro de 2024. Disponível em: https://blogs.microsoft.com/on-the-issues/2022/12/03/preparing-russian-cyber-offensive-ukraine/.

WATTS, Clint – «Russian influence and cyber operations adapt for long haul and exploit war fatigue». Microsoft. 2023. Consultado em: 7 de outubro de 2024. Disponível em: https://blogs.microsoft.com/on-the-issues/2023/12/07/russia-ukraine-digital-threat-celebrity-cameo-mtac/.

WILDE, Gavin – «Cyber operations in Ukraine: Russia's unmet expectations». Carnegie Endowment for International Peace. 12 de dezembro de 2022. Consultado em: 5 de setembro de 2024. Disponível em: https://carnegieendowment.org/2022/12/12/cyber-operations-in-ukraine-russia-s-unmet-expectations-pub-88607.

WILLETT, Marcus – «The cyber dimension of the Russia-Ukraine War». IISS. 2022. Consultado em: 7 de setembro de 2024. Disponível em: https://www.iiss.org/blogs/survival-blog/2022/10/the-cyber-dimension-of-the-russia-ukraine-war.

ZAKHARCHENKO, Kateryna – «HUR cyberattack hits Russian internet providers in occupied Crimea». Kyiv Post. 26 de junho de 2024. Consultado em: 11 de outubro de 2024. Disponível em: https://www.kyivpost.com/post/34917.