

## “PRECISO DE MUNIÇÕES, NÃO DE BOLEIA”: A GUERRA CIBERNÉTICA UCRANIANA

**Tine Munk**

Criminology and Criminal Justice Department, School of Social Science, Nottingham Trent University, Nottingham, Reino Unido

Concetualização, administração do projeto, redação do rascunho original, redação – revisão e edição

**Juan Ahmad**

Criminology and Criminal Justice Department, School of Social Science, Nottingham Trent University, Nottingham, Reino Unido

Redação – revisão e edição

---

### RESUMO

A invasão russa da Ucrânia em fevereiro de 2022 demonstrou que a guerra cibernética integra as estratégias militares modernas. Embora o exército russo tenha desenvolvido capacidades e competências cibernéticas ao longo dos anos, a Ucrânia criou rapidamente uma nova e inovadora defesa cibernética que inclui agentes públicos e privados. A utilização de plataformas de comunicação online para chegar às populações, dentro e fora do país, tem sido fundamental para o sucesso militar. O pensamento inventivo permitiu aos agentes utilizar o espaço online e desenvolver novas táticas informáticas para defender o país. A intensa presença online do presidente da Ucrânia, Zelenskyy, contrasta claramente com a do Presidente Putin da Rússia. O Presidente Zelenskyy domina a comunicação online e fala diretamente com as pessoas. A sua constante utilização de plataformas virtuais de comunicação motivou a formação de novos movimentos de resistência públicos e privados assentes no ativismo cívico e numa postura desafiadora contra a agressão russa. Vários grupos não governamentais de hackers, *hacktivistas* e ativistas criaram uma estrutura de resistência, onde cada um assumiu um papel num sistema nodal, em função das competências e dos níveis de envolvimento. Este artigo abordará como a liderança ucraniana tem desenvolvido um ato de discurso bem-sucedido que tem mobilizado inúmeros utilizadores online interna e externamente. Este ato de discurso permitiu uma nova forma de ativismo cívico online onde os intervenientes online combatem as forças militares — sem serem na sua maioria contratados pelo estado. Nos primeiros 40 dias, este ativismo provou trazer benefícios para a força militar existente defender a Ucrânia. O artigo investiga o papel da Ucrânia na luta de David e Golias e como as iniciativas da Ucrânia têm ajudado a desenvolver a sua defesa cibernética. A investigação assenta em fontes secundárias predominantemente baseadas em teoria fundamentada, onde os dados recolhidos são comparados de forma crítica com o conteúdo teórico. Todos os dados são recolhidos e analisados teoricamente com base nas abordagens sociopolíticas estabelecidas, decorrentes da análise do discurso. Esta investigação tem como horizonte temporal os primeiros 40 dias do conflito, com início a 24 de fevereiro de 2022.

### PALAVRAS-CHAVE

guerra cibernética, plataformas online, comunicação, ato de discurso, securitização, ativismo, Ucrânia

---

# "I NEED AMMUNITION, NOT A RIDE": THE UKRAINIAN CYBER WAR

## ABSTRACT

The Russian invasion of Ukraine in February 2022 has shown that cyberwarfare is integral to modern military strategies. Although the Russian army has developed cyber capabilities and capacities over the years, Ukraine has quickly created a new and innovative cyber defence that includes public and private actors. Using online communication platforms to reach out to populations, internally and externally, has been instrumental for military success. Inventive thinking has enabled the actors to utilise the online space and develop new computing tactics to defend the country. The intense online presence of Ukrainian President Zelenskyy stands in clear contrast to Russian President Putin. President Zelenskyy is mastering online communication and is speaking directly to the people. Because of his constant use of virtual communication platforms, new public and private resistance movements have formed based on civic activism and a defiant stance against Russian aggression. Various non-governmental groups of hackers, hacktivists and activists have created a structure of resistance, where each has taken on a role in a nodal system depending on skills and engagement levels. This article will focus on how the Ukrainian leadership has been able to carry out a successful speech act that has activated numerous online users internally and externally. This speech act has enabled a new form of online civic activism where online actors fight with the military forces — but mostly without being employed by the state. Within the first 40 days, this activism has proven beneficial to the existing military force to defend Ukraine. The article investigates Ukraine's role in the David and Goliath fight and how Ukraine's initiatives have helped develop its cyber defence. The research is based on secondary sources predominately based on grounded theory, where the data collected are critically compared with theoretical content. All data is theoretically sampled and analysed based on the established socio-political approaches deriving from discourse analysis. The timeframe for this research is the first 40 days of the conflict, starting on February 24 2022.

## KEYWORDS

cyberwar, online platforms, communication, speech act, securitization, activism, Ukraine

---

## 1. INTRODUÇÃO

No dia 24 de fevereiro de 2022, os veículos militares russos violaram a soberania da Ucrânia ao atravessarem as suas fronteiras com a subseqüentemente invasão de um estado soberano. Esta invasão foi a ameaça militar mais significativa na Europa desde o fim da Segunda Guerra Mundial (O'Connor, 2022, para. 5). A Rússia abriu caminho para a invasão a 21 de fevereiro ao reconhecer duas regiões rebeldes ucranianas, Donetsk e Luhansk, como estados independentes e ao entrar numa parte da Ucrânia com uma missão artificial de manutenção da paz (Roth & Borger, 2022, para. 2; United Nations, 2022, para. 4). Esta ação provocou uma onda de choque na comunidade internacional que, durante muito tempo, tinha tentado aliviar as tensões regionais através de meios diplomáticos.

O conflito ucraniano está associado ao uso de armas cibernéticas em múltiplos níveis. Uma parte da guerra cibernética espelha as ações militares tradicionais por água, terra e ar. A guerra cibernética convencional é essencial na guerra moderna, onde os

agentes atacam diretamente as vulnerabilidades dos sistemas e redes informáticas para danificar ou destruir infraestruturas críticas essenciais. Esta investigação revelou também que a comunicação e o ativismo são igualmente importantes no modelo da guerra híbrida. A guerra na Ucrânia demonstrou a capacidade de as comunicações online chegarem uma grande audiência para pedir apoio, promover um determinado argumento, e legitimar ações que de outra forma e em circunstâncias normais teriam sido rejeitadas. Quando concretizada com sucesso, a comunicação é uma arma poderosa que pode mobilizar e envolver um grande número de pessoas.

Este artigo incide sobre a comunicação online, onde um discurso bem-sucedido pode desencadear uma nova forma de ativismo e “união”, incorporando múltiplos grupos de agentes na estratégia defensiva do país. O ato de discurso, conduzido pelo Presidente Zelenskyy e outros líderes ucranianos, tem sido fundamental na mobilização de uma forma generalizada de ação cívica aliada à defesa de estado do país. A invasão e as atrocidades praticadas por soldados russos chocaram o mundo ocidental e provocaram nas pessoas um sentimento de impotência ao assistir ao desenrolar da guerra online e nos meios de comunicação social. A constante comunicação online e offline chamou a atenção para a situação na Ucrânia e manteve a guerra nos noticiários de todo o mundo. Agentes nacionais e estrangeiros apoiam o estado contra a invasão e a agressão russa. Grupos *hacktivistas* de renome e utilizadores online comuns fundiram os seus recursos e competências, recorrendo a meios ilegais e legais para apoiar a Ucrânia numa guerra injusta.

Durante a transição de uma ameaça de guerra para a invasão efetiva pela Rússia, os líderes ucranianos, em particular o Presidente Zelenskyy, equilibraram constantemente a necessidade de informar o mundo com apelos de apoio para defender o país e proteger os seus cidadãos. Não há dúvida que os líderes ucranianos ganharam a guerra de informação ao utilizarem competências de comunicação inovadoras e eficientes, incorporando vários espaços virtuais e meios de comunicação social. Inúmeros utilizadores online internos e externos têm-se mobilizado pela Ucrânia para apoiar e ajudar a “luta de David e Golias” do estado contra a agressão russa. Este artigo inclui uma investigação sobre a comunicação online assertiva e como esta tem mobilizado utilizadores online não governamentais para se envolverem numa guerra online.

As redes online relacionadas com a análise de Castells sobre o ambiente online são ainda precisas e valiosas para a compreensão dos atuais conflitos e ações. Segundo Castells (1996), “as redes constituem a nova morfologia social das nossas sociedades, e a difusão da lógica das redes modifica substancialmente o funcionamento e os resultados no processo de produção, experiência, poder e cultura” (p. 469; Hassan, 2008, p. 24). O desenvolvimento tecnológico e o uso constante de espaços online, como as redes sociais, para a comunicação num contexto global produziram mudanças significativas na forma como as pessoas interagem e comunicam, e o que acontece num país tem um impacto significativo em todo o mundo. A comunidade internacional em rede não é uma inovação impulsionada pela tecnologia; é uma parte da vida humana através do tempo e do espaço, em que as pessoas se organizam em redes humanas. No entanto, a forma

como os espaços virtuais e as novas formas de comunicação criaram uma base para a comunicação e troca de informação pode ser remetida para os novos paradigmas da tecnologia da informação que constituem uma base material para expandir a rede incluindo estruturas sociais completas (Castells, 1996, p. 469; Hassan, 2008, p. 24).

## 2. METODOLOGIA

Este artigo explora uma nova forma de ativismo online que surgiu durante os primeiros 40 dias da guerra ucraniana, onde agentes governamentais e não governamentais estiveram envolvidos na defesa do país a uma escala sem precedentes. A base teórica deste artigo combina a abordagem em rede de Castells com a teoria de segurança da Escola de Estudos de Segurança de Copenhaga para compreender o uso da comunicação e o seu impacto numa sociedade interligada. Para compreender como os líderes ucranianos captaram a atenção global e promoveram ações cívicas online fora da esfera do estado, são utilizados elementos da teoria da securitização da Escola de Copenhaga, como o ato de discurso. O ato de discurso é vital para o sucesso da comunicação com uma audiência, e confere legitimidade para contornar os processos normais do estado (Buzan et al., 1998).

O método assenta em pesquisas qualitativas secundárias, incluindo artigos académicos e noticiosos de jornais e revistas reconhecidos, e publicações nas redes sociais. A recolha de dados foi feita nos primeiros 40 dias após a invasão russa da Ucrânia a 24 de fevereiro de 2022. Os estudos de caso selecionados foram relatados dentro deste período. No entanto, até à data da redação do presente artigo, os estudos de caso não foram documentados em investigação académica. Assim, o conteúdo das redes sociais e os artigos noticiosos dos meios de comunicação social são fundamentais no registo de eventos-chave. Estas fontes ajudam a examinar a relação entre o ato de discurso e o ativismo online. Para validar o fluxo de notícias, os investigadores utilizaram meios noticiosos e revistas em língua inglesa de renome e vocacionados para o ocidente, nomeadamente a *Reuters*, *Associated Press*, *The Guardian*, *BBC News*, *The Verge*, e *Wired*, entre outros, apesar do potencial enviesamento na utilização de fontes regionais. Os novos artigos são usados para relatar eventos e não opiniões. Todos os eventos reportados foram verificados com base em informações de agências noticiosas fidedignas para garantir a qualidade do conteúdo. A informação nos meios de comunicação social e nas redes sociais são fontes importantes para compreender como os principais intervenientes no conflito em desenvolvimento comunicam e o impacto da comunicação. A recolha de dados assenta numa teoria fundamentada, em que os dados recolhidos são comparados de forma crítica com o conteúdo teórico. Para a recolha de dados foram usadas fontes como livros, capítulos, e artigos académicos revistos por pares, relatórios, artigos noticiosos, contas de redes sociais, e páginas de sites, e a pesquisa online foi realizada por palavras de pesquisa, tais como:

*Anonymous*, *cyberwar* (guerra cibernética), *cyberattacks* (ciberataques), *hacking Ukraine* (hacking Ucrânia), *hacking Russia* (Hacking Rússia), *hacktivism* (hacktivismo), *hacktivists Ukraine* (hacktivistas Ucrânia), *information warfare* (guerra de informação), *non-governmental cyber attacks* (ciberataques não

governamentais), *online attacks 2022* (ataques online 2022), *online support Ukraine* (apoio online Ucrânia), *Putin 2022*, *Russia 2022* (Rússia 2022), *social movement* (movimento social), *social actions* (ações sociais), *social media communication Ukraine* (comunicação nas redes sociais Ucrânia), *social media support Ukraine* (apoio nas redes sociais Ucrânia), *non-governmental hacking* (hacking não governamental), *hacking activities Ukraine* (atividades de hacking Ucrânia), *speech act* (ato de discurso), *Ukraine 2022* (Ucrânia 2022), *war* (guerra), *war Ukraine* (guerra Ucrânia), *Zelenskyy*, *Zelenskyy speeches 2022* (discursos de Zelenskyy 2022).

Todos os dados são teoricamente amostrados e analisados com base nas abordagens sociopolíticas estabelecidas decorrentes da análise do discurso.

### 3. COMUNICAÇÃO NAS REDES SOCIAIS

#### 3.1. REDES SOCIAIS E ESPAÇOS VIRTUAIS

A guerra da informação é definida como “o conflito ou luta entre dois, ou mais grupos no ambiente da informação” (Porche III et al., 2013, p. xv; Stupples, 2015, para. 2). Na sociedade contemporânea, a informação e a comunicação estão em constante mudança em virtude do desenvolvimento tecnológico, das interdependências, e da dependência de sistemas online interligados. A ascensão de plataformas online como o Facebook, Twitter, Instagram e TikTok tem sido decisiva para a comunicação durante um conflito em que é vital chegar a inúmeras pessoas em simultâneo. O volume e a extensão da comunicação online nas redes sociais progredem, e novos meios e métodos online têm alimentado novos tipos de ativismo político e mudança social. A comunicação online através das redes sociais e do ambiente online abrange todas as idades, etnias e geografias, sem precedentes. Este desenvolvimento inclui praticamente todos os utilizadores online; a espantosa ascensão de sites e espaços virtuais de comunicação revolucionou a forma como as pessoas comunicam e interagem com amigos, família e colegas em contextos públicos e privados, mas também como as pessoas participam na vida pública e política (Ludwig & de Ruyter, 2016, p. 124; Munk, 2022a, pp. 36–37).

São diferentes os tipos de comunicação e tecnologias interligados com as sociedades contemporâneas, tais como rádio (radiodifusão e televisão), jornais (revistas e livros) e filmes (documentários e filmes; Ahmad, 2020, p. 6; Hirst, 2018, para. 1; McQuail, 2010, p. 4). Os textos e as imagens ajudam a ilustrar eventos e retratam o comportamento das pessoas no poder, profissionalmente e em privado. As histórias da comunicação social são divulgadas com base no que a audiência acredita ser essencial, respeitando os padrões existentes de justiça e moralidade e o que é considerado comportamento aceitável. Portanto, é necessário olhar para o que é comunicado e como a informação é difundida (Dunaway & Graber, 2022, p. 5). A comunicação e a radiodifusão online podem influenciar a opinião pública e alcançar uma vasta audiência. A existência de vários

espaços virtuais é útil para partilhar e visualizar eficazmente as questões da guerra e divulgar propaganda e informação de forma equitativa. Assim, os meios de comunicação social podem ser uma plataforma de persuasão e mobilização, podendo assim apresentar um tópico específico de forma positiva ou negativa (Ahmad, 2020, pp. 6–7; McQuail, 2010, pp. 136, 151–152).

### 3.2. O PODEROSO ATO DE DISCURSO

A Ucrânia não tem recursos cibernéticos comparáveis aos da Rússia. Portanto, concentra-se em reforçar as suas táticas de defesa online e offline, já que a sua principal função é proteger pessoas e propriedades e manter o território. A tática de guerra da informação ucraniana inclui o uso de um comunicador eficaz, o Presidente Zelenskyy. Os discursos e vídeos do presidente ucraniano são armas poderosas para disseminar conhecimento e pedir ajuda e apoio, jogando com a simpatia e culpa que o mundo ocidental e os aliados naturais da Ucrânia sentem. Portanto, a utilização de tecnologias informáticas para comunicar tem provado ser oportuna e rentável. Estas diferentes camadas de envolvimento de ciberdefesa não devem ser subestimadas. Observam-se e utilizam-se, legal e ilegalmente, formas novas e inovadoras (Milmo, 2022b; Munk, 2022b; Paul, 2022; Trackray, 2022).

No espectro político, a comunicação é essencial para dar legitimidade a diferentes decisões que tradicionalmente não seriam aceitáveis. O ato de discurso é integrado na abordagem da Escola de Copenhaga, uma prática discursiva que liga a segurança a uma questão particular e a enquadra como uma ameaça. Buzan et al. (1998) argumentaram que as questões de segurança devem cumprir um limiar rigorosamente definido que permita que os problemas sejam deslocados para fora das áreas políticas normais. O processo de securitização é, portanto, “o movimento que conduz a política além das regras estabelecidas e enquadra a questão ou como um tipo especial de política, ou como acima da política” (Buzan et al., 1998, p. 23; Hough, 2018; Munk, 2015, pp. 33, 101). Através de um ato de discurso bem-sucedido, os problemas são apresentados e dramatizados como uma prioridade urgente. Se o ato de discurso for eficaz, confere a um agente/agência legitimidade para o mover para fora dos processos democráticos normais (Buzan et al., 1998, p. 26; Glover, 2011). O ato de discurso é uma parte essencial do processo, já que as questões de segurança ultrapassam posições ou procedimentos tradicionais. No entanto, é demasiado limitado para compreender que o ato de discurso constitui uma preocupação genuína do estado, uma vez que o processo não está apenas ligado à segurança de um estado soberano ou a valores particulares (Munk, 2015, pp. 33, 105).

No conflito ucraniano, muitas pessoas optaram por se envolver no ativismo online, impulsionado pela comunicação constante entre os líderes ucranianos e os cidadãos que lutam para defender o território. Contudo, nem todas as preocupações de segurança podem ser securitizadas. A verdadeira questão e o processo podem ser influenciados

pela história, posição geográfica e estrutural do estado (Buzan & Hansen, 2009, p. 34). Portanto, o ato de discurso é usado de forma diferente pela Rússia e pela Ucrânia. A tática ucraniana é vibrante, inclusiva e inovadora, pois o estado luta pela sobrevivência. Precisa de um amplo nível de apoio e aceitação para incluir medidas extraordinárias em tempo de guerra. Portanto, os comunicadores ucranianos alcançam uma grande audiência a vários níveis, governamental / não governamental e interno/externo, servindo-se de canais de comunicação online para divulgar amplamente as mensagens. A comunicação russa, por outro lado, assenta em meios de comunicação antiquados que parecem rígidos, burocráticos e desatualizados. Enquanto a comunicação ucraniana é amplamente distribuída, a comunicação russa é dirigida principalmente a um grupo restrito e selecionado de dirigentes.

As ações realizadas por agentes-chave incluem alguns elementos de excecionalismo. Por exemplo, os meios e métodos tradicionais ilegais online, ou seja, *hacking*, *defacement*, e comprometimento de dados, são encorajados tanto por agentes governamentais como não governamentais neste conflito. Os atos de discurso políticos implicam o poder de organizar as mentes e opiniões das pessoas e são ferramentas instrumentais para as controlar e conduzir. Através deste processo, vários tipos de comunicação podem alcançar uma grande audiência se forem corretamente comunicados. A comunicação a uma audiência receptiva é fundamental para estabelecer e manter relações sociais, expressar sentimentos e promover ideias, políticas e programas. O objetivo do ato é promover as intenções e o contexto do orador para receber legitimidade para agir, o que pode ser o movimento de securitização. Apesar de o *hacking* ser um conceito desenvolvido ao longo dos anos, não existem definições claras de *hacking*. As Nações Unidas têm tentado criar definições ao longo dos anos, mas a instituição não conseguiu obter apoio para as suas iniciativas (Munk, 2018, pp. 239–240, 2022a, p. 87). A tipologia da *hacking* inclui “acesso ilegal”, “acesso não autorizado”, ou “intrusão ilegal”. A Convenção do Conselho da Europa sobre o Cibercrime (Convention on Cybercrime, 2001) criminaliza o acesso ilegítimo a um computador (Artigo 2), a interceção ilegítima (Artigo 3), a interferência em dados (Artigo 4) e o uso abusivo de dispositivos (Artigo 5). A Ucrânia é também um estado signatário, ratificando a convenção em 2006 (Ahmad, 2020, p. 9; Convention on Cybercrime, 2001, pp. 3–4; Council of Europe, 2022; Munk, 2022a, pp. 204–206). Apesar de ter sido criminalizado, o *hacking* tem sido aceite como uma ferramenta para atacar sistemas e redes russos — tal como a Rússia tem usado os seus múltiplos recursos informáticos para atacar a Ucrânia e derrubar infraestruturas vitais antes e durante a guerra (Ahmad, 2022, pp. 7–10; Munk, 2022b). Como afirmam Buzan et al. (1998), “se, com o argumento da prioridade e urgência de uma ameaça existencial, o agente de securitização tiver conseguido libertar-se de procedimentos ou regras a que de outra forma estaria vinculado, assistimos a um ato de securitização” (p. 25).

## 4. PRESENÇA NAS REDES SOCIAIS E A IMAGEM DE UM LÍDER

### 4.1. UCRÂNIA

O Presidente Zelenskyy tem uma presença online expressiva desde o primeiro dia do conflito. Comunica no Twitter e outras redes sociais, publica vídeos curtos e aparece em transmissões em direto. Com a tag @ZelenskyyUa, está constantemente disponível como a voz do governo ucraniano (Zelenskyy, s.d.). Zelenskyy reage com provocação à invasão e à guerra em curso em todas as mensagens. Quando os vídeos o mostram de pé numa rua de Kiev, reforça a moral, simbolizando um comandante-chefe que sofre as mesmas dificuldades que os ucranianos comuns (CNN, 2022; Mulvey, 2022, paras. 2, 5, 9, 12). O estatuto de celebridade que Zelenskyy obteve durante os primeiros dias da guerra deu-lhe uma plataforma de comunicação poderosa e uma atenção constante da comunicação social de modo algum partilhada com o seu homólogo russo.

Na Ucrânia, a invasão e a guerra que se seguiu criaram laços entre utilizadores online nacionais e de outros países que podem ser associados à noção de sociedades em rede de Castells. O acesso a múltiplos espaços online mantém o governo ucraniano no controlo da narrativa. Ao fazê-lo, desafia o monopólio tradicional dos poderosos meios de comunicação para manter o conflito nos noticiários de todo o mundo (Siapera, 2018, p. 47). Contudo, o recurso às redes sociais para a comunicação não substitui as principais fontes de notícias. Pelo contrário, a presença online ativa funciona como um acelerador para gerar interesse nos principais eventos, fazer progredir uma determinada narrativa ou contrapor a propaganda do estado adversário (Newman et al., 2014, p. 139). Embora as plataformas online sejam úteis para a comunicação direta, são também uma mais-valia para a transmissão indireta de mensagens online através do efeito de bola de neve, onde o texto e as imagens são partilhados e redistribuídos para além do público original. O ato de discurso online tem duas vertentes. Em primeiro lugar, a presença online é essencial para manter uma audiência informada sobre a situação. Paralelamente, os comunicadores mantêm-se no controlo da narrativa. Em segundo lugar, é usado tradicionalmente onde os agentes políticos obtêm legitimidade para contornar os processos convencionais num país devastado pela guerra que luta pela sobrevivência. Esta comunidade online foi concebida para ajudar e apoiar a Ucrânia, alimentada por um sentimento de impotência como catalisador de ação.

A citação "preciso de munições, não de boleia" tornou-se viral depois de Zelenskyy ter rejeitado uma oferta dos Estados Unidos para evacuar de Kiev nos primeiros dias da guerra (Braithwaite, 2022; Freedland, 2022, para. 8; The Associated Press, 2022). Esta mensagem é considerada o protótipo do estadismo digital. Zelenskyy tem feito apresentações em direto em parlamentos de todo o mundo, incluindo a União Europeia, o Reino Unido, a Alemanha, Israel e os Estados Unidos, onde profere constantemente discursos virtuais como parte da sua estratégia para obter apoio (Freedland, 2022, paras. 12–13; Guinness, 2022; Parry, 2022; Scott, 2022; Watson, 2022). Graças à comunicação global online, as pessoas estão habituadas a seguir em direto eventos relevantes à medida que estes se desenrolam. No entanto, isto também provoca um certo cansaço



das notícias. As pessoas ficam emocionalmente distantes e dessensibilizadas pelo fluxo constante de imagens de bombardeamentos e atrocidades de pontos críticos globais. As transmissões aumentam frequentemente a cobertura noticiosa para ganhar a atenção dos média (Jewkes, 2015, p. 33). Isto significa que as pessoas responsáveis pelo ato de discurso devem equilibrar constantemente a sua reportagem com o interesse das pessoas, outros eventos mundiais, e o interesse do público pelo tema. A liderança ucraniana tem sido eminente no seu equilíbrio, já que a audiência online continua a aumentar o apoio e a envolver-se ativamente na defesa.

Embora o discurso verbal seja essencial para a comunicação, certas imagens e símbolos repetitivos são ferramentas poderosas para criar associações com o ato de discurso original. O uso de símbolos na política não é novidade. Os símbolos em ação são eficazes em ilustrar uma determinada mudança de postura ou de paradigma. Em 1970, Willy Brandt, o então chanceler da República Federal da Alemanha, ajoelhou-se diante do Memorial de Varsóvia em honra dos heróis judeus do Gueto de 1943 e isso foi interpretado como símbolo de uma nova era e de mudanças na política alemã do pós-guerra (Rauer, 2006, p. 258). O uso de símbolos e comportamentos específicos foram profundamente integrados na política. O valor do símbolo nas ações de Zelenskyy é visível no discurso à nação, onde ele e o grupo de liderança são filmados a passear por Kiev na primeira noite após a invasão russa. Esse vídeo assinala várias coisas: o governo permanece em Kiev, age em solidariedade com os cidadãos ucranianos, e não teme as ações do Kremlin ("Video: Ukrainian President Zelensky Says Country's Leaders Remain in Kyiv", 2022). As ações performativas da liderança ucraniana viabilizam o ato de discurso ao comunicar a mensagem em todo o mundo recorrendo a vários métodos de comunicação diferentes, repetindo palavras, imagens ou slogans reconhecidos online e offline. Anteriormente, o Presidente Zelenskyy dirigia-se oficialmente à nação ucraniana a partir do gabinete presidencial, de fato e gravata. A partir da invasão, os discursos internos e externos de Zelenskyy foram proferidos em locais neutros para evitar revelar a sua localização. Veste habitualmente a sua t-shirt improvisada com a bandeira ucraniana ou outros símbolos de estado (Buncombe, 2022; Freedland, 2022, para. 7; Stanage, 2022, para. 2). Esta t-shirt tornou-se um símbolo da sua liderança e resistência à Rússia. É tendência em sites comerciais, bem como uma figura como um Lego, vendida para apoiar a Ucrânia, como símbolo da sua liderança. A icónica t-shirt permite a Zelenskyy destacar-se e demonstrar que pertence/permanece com os ucranianos durante este período difícil (Burton, 2022; Myustee, 2022; Picclick, 2022).

#### 4.2. RÚSSIA

Enquanto o Presidente da Ucrânia Zelenskyy mantém uma posição de dignidade, determinação, coerente e proficiente no seu discurso online, o seu homólogo russo é visto de forma diferente (Mulvey, 2022, para. 3; Smith, 2022b, paras. 2, 4). O presidente russo Putin continua a ser uma figura distante. Quando aparece na comunicação social, ou está sentado ao fundo de uma vasta sala, na ponta de uma longa mesa, comunicando online usando um monitor de computador gigante ou sentado numa cadeira gigantesca

(Holmes, 2022; Saul, 2022; Walker, 2022, para. 7). Na sua aparência, Putin parece pálido, frio, retraído, agressivo, errático e rancoroso. Por exemplo, na tensa conversa entre o Presidente Putin e Naryshkin, chefe dos serviços secretos estrangeiros, Putin interrompeu o chefe de espionagem várias vezes, pedindo-lhe raivosamente para “falar abertamente” (“‘Speak Plainly!’: Putin Has Tense Exchange With His Spy Chief – Video”, 2022; Walker, 2022, para. 10).

Outros discursos incluíram declarações agressivas sobre a Ucrânia, a Organização do Tratado do Atlântico Norte, e todos os que se interpõem no caminho. Em vez de um estadista russo unificador e líder que usa o discurso para construir ativamente apoio, Putin ameaçou qualquer um que questionasse esta invasão, apelando a uma “limpeza natural” da “escória e dos traidores” (CBS/AP, 2022; “‘Scum and Traitors’: Putin Threatens Russians Who Oppose War in Ukraine – Video”, 2022; Smith, 2022b). Esta narrativa negativa parece ser uma parte da propaganda russa. Putin repetiu estas afirmações no seu comício de “unidade” (2022) em Moscovo, no aniversário da anexação da Crimeia, onde apareceu finalmente para fazer um discurso de 5 minutos perante uma audiência (Fisher, 2022; “Russian State TV Cuts Away From Putin at Pro-Russia Rally – Video”, 2022; Sauer, 2022).

O discurso russo visa promover o poder e o controlo, com o apoio da máquina de propaganda russa que afirma que a guerra é uma “operação especial” e que a Ucrânia constitui uma ameaça direta para a Rússia e para a população russa. O verdadeiro ato de discurso conduzido por Putin espelha o ato de discurso delineado pela Escola de Copenhaga, onde o aparelho estatal está no controlo da narrativa e a censura é imposta à comunicação social. É um processo manipulador, na medida em que está unicamente nas mãos do orador enquadrar as questões de segurança e determinar como conduzir o ato de discurso (Munk, 2015, p. 105; Salter, 2008, p. 328). O processo parece premeditado, dirigido a um público escolhido e promovido para a aceitação do arquivo (Munk, 2015, p. 105). Contudo, o aparelho estatal russo não tem a mesma infraestrutura de comunicação que a Ucrânia e não pode gerar o mesmo nível de apoio interno e externo através de vários meios de comunicação online e offline. Por conseguinte, o discurso russo é apenas dirigido à liderança do Kremlin que apoiará sempre o Presidente Putin por medo de represálias.

## 5. ATIVISMO POLÍTICO

O ativismo é definido dentro de um contexto específico. É motivado pelo confronto e desagrado com políticas e práticas específicas, e conduzido para alcançar mudanças através de vários meios, tais como protestos, marchas, discursos e cânticos, entre outros (Anderson & Herr, 2007). O ativismo decorrente da intensa comunicação ucraniana assenta em valores, fundamentalmente entendido como ativismo político estreitamente ligado aos sentimentos das pessoas sobre o mundo e ao que mais lhes interessa, como o certo e o errado (Munk, 2022a, p. 31). As redes sociais, o ciberespaço e as tecnologias informáticas mudaram a forma como as pessoas se podem ligar instantaneamente umas às outras. Enquanto isso, as tecnologias informáticas criam uma oportunidade sem precedentes para disseminar informação e inspirar e influenciar outras pessoas (Lewis et al., 2014; Munk, 2022a, pp. 33–34).

O ativismo online está frequentemente associado à mobilização política, que inclui as tecnologias e redes informáticas. No entanto, esta forma de ciberativismo não é necessariamente ilegal. Os utilizadores usam espaços online para protestar ou apoiar causas políticas online e offline (Lutkevich & Bacon, 2021, para. 1; Munk, 2022a, p. 201; Sauter, 2014, p. 26). O ambiente online permite aos grupos alcançar uma grande audiência através das fronteiras tradicionais e sociais para disseminar informação e criar consciência sobre as causas, táticas e ferramentas (Ahmad, 2020, p. 16; Kremling & Parker, 2017). Diferentes agentes têm sido vozes na sua crítica à Rússia e apoio à Ucrânia ao defenderem a soberania e liberdade da Ucrânia. O apelo do ator norte-americano Arnold Schwarzenegger ao povo russo numa mensagem no Twitter é uma forma de demonstrar solidariedade para com a Ucrânia e chegar à população russa para a informar sobre a guerra (Schwarzenegger, 2022; *Ukraine: Arnold Schwarzenegger's Anti-War Video Trends on Russian Social Media – Video*, 2022).

As munições pedidas por Zelenskyy nos primeiros dias da guerra têm demonstrado assumir muitos formatos e formas diferentes. Grupos *hacktivistas* bem conhecidos misturam-se com utilizadores online comuns para derrotar a Rússia online. O *hacktivism*, como conceito, funde *hacking* e ativismo, que muitas vezes tem sido implantado contra instituições, empresas, ou estados poderosos. Apesar de terem um nível razoável de apoio entre o público, as suas atividades não são consideradas legítimas e caem no âmbito do crime cibernético. O sucesso do ato de discurso conduzido por funcionários ucranianos e a constante ênfase na guerra por parte dos meios de comunicação social tem surtido efeito. Consequentemente, surgiram diferentes formas de ativismo, ou seja, legal e ilegal, governamental e não governamental. A ativação de outros grupos na sociedade é essencial.

Foram desenvolvidos todos os tipos de ações para apoiar a defesa da Ucrânia, onde os hackers conseguiram perturbar o tráfego de dados no Kremlin e nas páginas do site da Duma e obter acesso aos serviços de comunicação social do estado, bancos e empresas. Nem todas as ações são ilegais. Inúmeros utilizadores online realizam atividades dentro da esfera legal, tais como a divulgação de contrapropaganda, a recolha de informação e o combate à desinformação online. Os especialistas em publicidade têm um papel na conceção e divulgação de anúncios para sensibilizar para a guerra na Rússia e Bielorrússia, contornando a censura e o encerramento de plataformas (Stokel-Walker & Milmo, 2022). O determinante comum para estes agentes é a confiança na liderança da Ucrânia e no facto de acreditarem que as suas ações ajudam a derrotar a Rússia.

## 5.1. HACKERS, HACKTIVISTAS E ATIVISTAS

### 5.1.1. O EXÉRCITO DAS TECNOLOGIAS DE INFORMAÇÃO E OS HACKERS

A Ucrânia está a construir um exército voluntário de tecnologia de informação (TI) para ajudar a melhorar a sua defesa. No entanto, várias das suas atividades consistem em pirataria informática e ataques de negação de serviço distribuído (DDoS) que

invadem ilegalmente corporações e alvos governamentais. Dois dias após a invasão russa, o vice-primeiro-ministro da Ucrânia e o ministro para a transformação digital, Fedorov, anunciaram num tweet a criação de um exército voluntário de TI. O tweet incluía um apelo para impedir as empresas de tecnologia de trabalharem com a Rússia e uma tentativa de atrair talentos de informática, tais como criadores, ciberespecialistas, designers, redatores e publicitários, para se envolverem na nova fronteira online (Burgess, 2022, para. 2; Stokel-Walker & Milmo, 2022). Ao contrário de muitas outras iniciativas privadas, o exército de TI é um representante direto do estado, sendo as tarefas atribuídas aos voluntários em função do seu envolvimento e competências informáticas. As tarefas são distribuídas num canal do Telegram, o “IT Army of Ukraine” (exército TI da Ucrânia). Mais de 300.000 pessoas subscreveram o canal 3 semanas após este anúncio, e os números aumentaram desde então (Burgess, 2022; Milmo, 2022a, para. 2; Newman, 2022). Estas ações são um resultado claro de um discurso bem-sucedido, onde a questão foi enquadrada como uma ameaça existencial, e uma audiência aceitou que o estado contornasse as regras e processos habituais, ou seja, incorporando o *hacking* e outras formas de ataque ilegal nas ferramentas disponíveis. O poder político e os espaços virtuais têm benefícios significativos quando combinados. Utilizando os espaços online e criando um canal no Telegram, é possível mobilizar e “empregar” um grande número de agentes voluntários que podem participar em ações online diretas ou trabalhar na Internet (Wolfsfeld, 2022, p. 5). Contudo, os agentes políticos ainda precisam de equilibrar o ato de discurso com a necessidade de mobilizar muitos voluntários para ajudar na defesa online — e não usar a mesma tática da Rússia. A boa vontade do governo ucraniano está ligada à comunicação clara e ao ato de discurso. A presença online de Zelenskyy e agentes governamentais, o desprezo da Rússia pelas leis internacionais e o seu ataque não provocado a um país soberano têm sido fundamentais para a formação deste extenso exército informático voluntário.

Embora a Ucrânia tenha já recrutado muitos voluntários de TI nacionais, o apelo foi também disseminado online e outros voluntários internacionais inscreveram-se através do Telegram. Este envolvimento de cidadãos estrangeiros motivou uma advertência severa das autoridades ocidentais sobre os perigos destas operações privadas. Em primeiro lugar, o *hacking* e atividades similares são criminalizados, e os hackers violariam a lei nacional para ajudar a Ucrânia a partir do estrangeiro (Ahmad, 2020, p. 7; Milmo, 2022a, paras. 3–4, 8; Munk, 2022a, pp. 204–207). Em segundo lugar, foram manifestadas preocupações com o facto destas ações poderem involuntariamente alastrar a outras áreas, permitindo a Putin afirmar que o ocidente ataca a Rússia — ou que o ataque também afeta a Ucrânia, ou seja, *worms* ou vírus informáticos (Burgess, 2022, para. 13; Milmo, 2022a, para. 9). No entanto, ao contrário do ato de discurso ucraniano, estes avisos não tiveram o efeito esperado, já que muitos hackers estrangeiros continuam envolvidos em ações de apoio à Ucrânia.

### 5.1.2. HACKTIVISTAS

O *hacktivismo* combina técnicas e ferramentas de *hacking* com ativismo, e permite a disseminação de uma determinada mensagem política. Não é apenas o exército informático que usa meios ilegais para lutar contra a Rússia. Ao contrário dos alicerces políticos tradicionais, o ambiente online permite um novo tipo de ativismo onde as pessoas podem conectar-se e procurar possibilidades alternativas de ação, independentemente da sua localização (Castells & Kumar, 2014, p. 95; Sorell, 2015, p. 392). No início do conflito, o grupo internacional *hacktivista* Anonymous e os seus membros declararam guerra à Rússia. Ao fazê-lo, justificaram o recurso a meios e métodos excepcionais, apesar do seu estatuto não governamental. Contudo, os diferentes grupos de *hacking* têm falado online e comunicado com a rede replicando o ato de discurso (Anonymous, s.d.; Coker, 2022; Milmo, 2022b). De acordo com a teoria de redes de Castells (1996), Anonymous intervém simultaneamente em questões locais e globais. Como todos os atores estão interligados online, operam a nível internacional, criando assim um poder enorme, como se viu nas 4 primeiras semanas que se seguiram à invasão russa da Ucrânia. Anonymous é um grupo hacker descentralizado, que dedica os seus esforços e competências de *hacking* à promoção dos direitos à privacidade online, internet livre e anti censura. O grupo é conhecido pelas suas operações permanentes contra estados, empresas, associações e outros agentes influentes, tais como #OPPayback, #OPAvengerAssange, e pelo seu envolvimento nos protestos da Primavera Árabe (Ahmad, 2020, p. 18; Karagiannopoulos, 2018, p. 16; Li, 2013, p. 307; Munk, 2022a, p. 215; Sorell, 2015, pp. 393–397).

Grupos como o Anonymous estão a reagir ao ato de discurso das autoridades ucranianas nos diferentes pedidos de ajuda online. Os grupos *hacktivistas* usam vários meios e métodos criminalizados semelhantes ao exército informático. Estas práticas ganharam ímpeto durante a guerra, e é possível usá-las graças a um ato de discurso eficaz. Durante as primeiras 4 semanas da guerra, Anonymous liderou com êxito campanhas contra a Rússia, como *hacking* e ataques DDoS contra a base de dados do Ministério da Defesa russo e páginas do site do Kremlin (Milmo, 2022b, para. 3). Os *hacktivistas* invadiram ainda vários canais de televisão estatais russos, tais como Russia 24, Channel 1, e Moscow 24, onde os programas foram substituídos por várias imagens informando sobre a invasão da Ucrânia, mensagens antiguerra, música e símbolos ucranianos (Anonymous TV, 2022; Milmo, 2022b, para 4; The Kyiv Independent, 2022). O grupo assumiu também os créditos por um *defacement* de dados de rastreio marítimo que renomeou o super iate de Putin "FCKPTN" e mudou o seu destino para "Inferno" (Maritime Industry News, 2022, para. 1; Newman, 2022, para. 6; Smith, 2022a).

Anonymous não é o único grupo a intervir neste conflito. O Distributed-Denial-of-Secrets (DDoSecrets) divulgou 15 conjuntos diferentes de informações russas obtidas junto de outros grupos *hacktivistas*, tais como a obtenção ilegal de 820GB de dados pelo Roskomnadzor russo (Coker, 2022; Collier et al., 2022, para. 18). Contudo, estas atividades de fuga de informação são ilegais, e o DDoSecrets já está sob investigação nos Estados Unidos a propósito das fugas de dados da BlueLeaks em 2020 (Munk, 2022a, p.

230). Outros grupos de *hacktivismo* adulteraram páginas de sites russos e substituíram conteúdos por mensagens pró-ucranianas ou anti Putin. Alguns grupos, por exemplo, adulteraram uma página do site do Instituto Russo de Pesquisa Espacial e divulgaram presumivelmente dados da agência espacial russa, Roscosmos (Newman, 2022, para. 1).

### 5.1.3. OUTROS ATIVISTAS ONLINE

Os ativistas online têm-se inspirado na constante comunicação da liderança ucraniana. Num dos seus muitos discursos, o Presidente Zelenskyy pediu aos utilizadores russos do TikTok, cientistas, médicos, bloggers, e comediantes de *stand-up*, que agissem e ajudassem a vencer a guerra (Chayka, 2022; Paul, 2022). A geração TikTok/geração Z já demonstrou o seu ativismo durante as eleições presidenciais de 2020 nos Estados Unidos e os protestos “BlackLivesMatter” na sequência do assassinato de George Floyd. Os sites de redes sociais são essenciais na condução destas ações cívicas, já que o conteúdo gerado pelo utilizador é disseminado rapidamente. Este tipo de mobilização/comunicação enquadra-se no ato de discurso original que pede ajuda e apoio. As redes sociais funcionam como sites de *microblogging* onde as notícias são amplamente disseminadas apesar de não serem fiáveis (Jewkes, 2015, p. 73). Sim, as imagens criadas nos telemóveis, textos e e-mails que circulam são comunicações eficazes. Como plataforma de rede social, o TikTok é conhecido por ser instável e descontextualizado com música vibrante, mas é também uma plataforma de comunicação online popular (Ahmad, 2020, pp. 16, 41–42; Chayka, 2022; Munk, 2022a, pp. 222–224).

Os vídeos com a tag #Ukraine obtiveram mais de 30.000.000.000 de visualizações na plataforma em 4 semanas. Contudo, existem questões relacionadas com a utilização do TikTok para distribuir informação. O algoritmo da empresa determina que são lançados dados dentro do *feed* de notícias com base na preferência do algoritmo e no envolvimento do utilizador. O elemento central do TikTok é a forma como a plataforma permite aos utilizadores online carregar videoclipes e áudios sem referências. Portanto, é quase impossível verificar o conteúdo. Infelizmente, a geração TikTok está menos preocupada com a verificação da informação. Está mais interessada em alcançar o objetivo através da criação ou promoção de um vídeo eficaz que chame a atenção (Clayton & Dyer, 2022; Hern, 2022b; Paul, 2022). Por exemplo, “Ghost of Kyiv” (fantasma de Kiev) mostra um jato russo a ser abatido. Mas esse vídeo é de um jogo de vídeo não relacionado com o conflito. No entanto, isso não impede que o vídeo continue a ser partilhado (Chayka, 2022, para. 8; Hern, 2022, para. 5).

Há muitas pessoas empenhadas em apoiar a Ucrânia recorrendo a meios e métodos legais. Estes são, sem dúvida, armas poderosas para a defesa do país. A Alphabet Inc. suspendeu o carregamento de novas avaliações geradas por utilizadores na plataforma, após um inevitável influxo de declarações políticas. As declarações foram carregadas em campos de comentários onde os utilizadores podiam interagir e deixar as opiniões. Por exemplo, Anonymous encorajou os utilizadores online a colocar comentários

sobre empresas e destinos turísticos russos, ucranianos e bielorrussos no Google Maps. Estas críticas formariam um plano de informação essencial, contornando a censura. O Anonymous encorajou os seus 7.700.000 de seguidores a irem ao Google Maps, encontrarem um restaurante ou negócio, e enviarem uma avaliação com informação sobre o que está a acontecer na Ucrânia (Anonymous, 2022; Baynes, 2022). Por exemplo, uma captura de ecrã de uma avaliação do TripAdvisor, publicada numa página do Twitter do Anonymous (2022), afirmou: “a comida era excelente! Infelizmente, o Putin estragou o nosso apetite ao invadir a Ucrânia. Faça frente ao seu ditador, pare de matar pessoas inocentes! O seu governo está a mentir-lhe. Acorde!”.

Outros utilizadores argumentaram que dar cinco estrelas na avaliação é importante para evitar arruinar o negócio, pois é provável que sejam pequenas empresas familiares/pequenas empresas (Anonymous, 2022; Baynes, 2022). A Alphabet Inc. agiu rapidamente para bloquear novas avaliações, pois a campanha violou a política da empresa contra avaliações falsas, copiadas, despropositadas, abusivas ou difamatórias. Foram colocadas mensagens semelhantes no TripAdvisor. Em vez de avaliar um restaurante, café, ou loja, surgiu um texto com informações sobre a guerra. O sistema de moderação do TripAdvisor registou o aumento de avaliações falsas. Por isso, a secção de avaliação foi temporariamente suspensa para prevenir publicações arriscadas de ativistas e a empresa encaminhou os seus utilizadores para o fórum da sua comunidade, onde publicou informações sobre a guerra (Baynes, 2022; Deighton, 2022, para. 7; Hamilton, 2022; Smith, 2022c).

## 6. CONCLUSÃO

Este artigo apresenta apenas um retrato das atividades desenvolvidas durante os primeiros 40 dias. No entanto, surgiu um padrão de comunicação onde a Ucrânia combinou atos de discurso de securitização com outros tipos de comunicação, recorrendo a texto, vídeos, transmissões em direto, símbolos e comportamentos reconhecíveis.

O Presidente Zelenskyy provavelmente preferiria receber mais aviões, tanques e mísseis, mas ainda precisa de ganhar a guerra online. Até agora, a liderança ucraniana tem comunicado com sucesso com inúmeras pessoas interna e externamente. Estas comunicações constantes tornaram-se uma parte valiosa do armamento do governo para defender o país. A verdadeira guerra dos média já foi ganha por Zelenskyy e pelo seu uso magistral das redes sociais para diferentes tipos de comunicações e apelos diretos ao vivo para pedir ajuda. É interessante como as pessoas em todo o mundo reagiram positivamente a estes tipos de comunicação e o nível de empatia que os ucranianos têm recebido.

As redes sociais e a comunicação online conquistaram uma posição de destaque na política moderna. O que significa que o processo de securitização pode ser amplificado online. O ato de discurso pode ser associado ao processo tradicional de legitimação para mover o objeto de referência para fora dos processos normais. Os políticos contemporâneos estão profundamente empenhados em comunicar com uma audiência online sobre a política quotidiana que não precisa de ser enquadrada como ameaça

à segurança. Alimentados pela constante presença online de Zelenskyy e pelo apelo à ação, cidadãos de todo o mundo têm sido atraídos para o conflito através do envolvimento em ativismo político de baixo nível, *hacking* e *hacktivismo*. A comunicação governamental online e as atividades cívicas serão espelhadas em futuros conflitos. Isto significa que a guerra propriamente dita é travada em duas frentes, uma frente oficial, onde o estado comanda as ações militares. A segunda frente é o exército voluntário, com um nível diferente de envolvimento, competências e incitamento à participação. No entanto, este exército voluntário e não governamental é autónomo e só estará envolvido enquanto lutar por uma causa justa. As novas munições são as competências das pessoas e o envolvimento no conflito e o seu impacto não pode ser subestimado.

**Tradução: Anabela Delgado**

## REFERÊNCIAS

- Ahmad, J. (2020). 'Hacking or not hacking... that's the question'. *Definitional challenges and hacking practices*. MDX Library
- Anderson, G., & Herr, K. (2007). Introduction. In G. Anderson & K. Herr (Eds.), *Encyclopedia of activism and social justice* (pp. 19–27). Sage.
- Anonymous [@YourAnonNews]. (s.d.). *Tweets* [Perfil de Twitter]. Twitter. Retirado a 27 de março 2022 de [https://twitter.com/YourAnonNews?ref\\_src=twsrc%5Egoogle%7Ctwcamp%5Eserp%7Ctwgr%5Eauthor](https://twitter.com/YourAnonNews?ref_src=twsrc%5Egoogle%7Ctwcamp%5Eserp%7Ctwgr%5Eauthor)
- Anonymous. [@YourAnonNews]. (2022, 28 de fevereiro). *Translation: The food was great! Unfortunately, Putin spoiled our appetites by invading Ukraine. Stand up to your dictator, stop killing* [Tweet]. Twitter. <https://twitter.com/YourAnonNews/status/1498341870774235138>
- Anonymous TV. [@YourAnonTV]. (2022, 26 de fevereiro). *JUST IN: #Russian state TV channels have been hacked by #Anonymous to broadcast the truth about what happens in #Ukraine* [Vídeo anexado] [Tweet]. Twitter. [https://twitter.com/YourAnonTV/status/1497678663046905863?ref\\_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1497678663046905863%7Ctwgr%5E%7Ctwcon%5E%5E1\\_&ref\\_url=https%3A%2F%2Fwww.theguardian.com%2Fworld%2F2022%2Ffeb%2F27%2Fanonymo-us-the-hacker-collectiv](https://twitter.com/YourAnonTV/status/1497678663046905863?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1497678663046905863%7Ctwgr%5E%7Ctwcon%5E%5E1_&ref_url=https%3A%2F%2Fwww.theguardian.com%2Fworld%2F2022%2Ffeb%2F27%2Fanonymo-us-the-hacker-collectiv)
- Baynes, M. (2022, 2 de março). 'Food was great! Unfortunately Putin spoiled our appetites by invading Ukraine' - *TripAdvisor disables Russian reviews*. SkyNews. <https://news.sky.com/story/food-was-great-unfortunately-putin-spoiled-our-appetites-by-invading-ukraine-tripadvisor-disables-russian-reviews-1255968>
- Braithwaite, S. (2022, 26 de fevereiro). *Zelensky refuses US offer to evacuate, saying 'I need ammunition, not a ride'*. CNN. <https://edition.cnn.com/2022/02/26/europe/ukraine-zelensky-evacuation-intl/index.html>
- Buncombe, A. (2022, 18 de março). How Ukrainian president Zelensky's simple green t-shirt became an iconic message of defiance. *The Independent*. <https://www.msn.com/en-gb/news/world/how-ukrainian-president-zelensky-s-simple-green-t-shirt-became-an-iconic-message-of-defiance/ar-AAVftjX>
- Burgess, M. (2022, 27 de fevereiro). Ukraine's volunteer 'IT army' is hacking in uncharted territory. *Wired*. <https://www.wired.co.uk/article/ukraine-it-army-russia-war-cyberattacks-ddos#:~:text=The%20country%20has%20enlisted%20thousands,the%20war%20effort%20against%20Russia.&text=Vladimir%20Putin's%20attack%20on%20Ukraine,the%20country's%20towns%20and%20cities>



- Burton, J. (2022, 17 de março). Zelensky lego figures released to raise money for Ukraine refugees. *Newsweek*. <https://www.newsweek.com/zelensky-lego-figure-charity-ukraine-refugees-1689010>
- Buzan, B., & Hansen, L. (2009). *The evolution of international security studies*. Cambridge University Press.
- Buzan, B., Wæver, O., & de Wilde, J. (1998). *Security. A new framework for analysis*. Lynne Rienner.
- Castells, M. (1996). *The rise of the network society, Vol. 1. The information age: Economy, society and culture*. Blackwell.
- Castells, M., & Kumar, M. (2014). A conversation with Manuel Castells. *Berkeley Planning Journal*, 27(1), 93–99. <https://escholarship.org/content/qt2ns059h3/qt2ns059h3.pdf>
- CBS/AP. (2022, 18 de março). *Putin calls opponents "scum and traitors" as Moscow announces new crackdown on "false information"*. CBS News. <https://www.cbsnews.com/news/putin-opponents-scum-traitors-repression/>
- Chayka, K. (2022, 3 de março). Watching the world's "first TikTok war". *The New Yorker*. <https://www.newyorker.com/culture/infinite-scroll/watching-the-worlds-first-tiktok-war>
- Clayton, J., & Dyer, J. (2022, 5 de março). *Ukraine war: The TikToker spreading viral videos*. BBC News. <https://www.bbc.co.uk/news/technology-60613331>
- CNN. (2022, 26 de fevereiro). *Zelensky post video in the streets of Kyiv. Anderson Cooper 360*. <https://edition.cnn.com/videos/world/2022/02/26/zelensky-selfie-street-video-vpx.cnn>
- Coker, J. (2022, 11 de março). Anonymous claims to have leaked over 360,000 files from Russian Federal Agency. *Infosecurity Magazine*. <https://www.infosecurity-magazine.com/news/anonymous-leaked-files-russian/>
- Collier, J., Dong, S., & Arouzi, A. (2022, 22 de março). *Hackers, new and veteran, target Russia with one of cyber's oldest tools*. NBC News. <https://www.nbcnews.com/tech/security/hackers-new-veteran-target-russia-one-cybers-oldest-tools-rcna20652>
- Convention on cybercrime, 23 de Novembro 23 de 2001, <https://rm.coe.int/1680081561>
- Council of Europe. (2022, 27 de março). Chart of signatures and ratifications of Treaty 185. <https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treaty=185>
- Deighton, K. (2022, 2 de março). Tripadvisor, Google Maps suspend reviews of some Russian listings. *The Wall Street Journal*. <https://www.wsj.com/livecoverage/russia-ukraine-latest-news-2022-03-02/card/tripadvisor-google-maps-suspend-reviews-of-some-russian-listings-vM2no1PgGDmMkL2TSvPZ#:~:text=The%20suspensions%20were%20made%20in,off%20from%20other%20media%20platforms>
- Dunaway, J. L., & Graber, D. A. (2022). *Mass media and American politics* (11.<sup>a</sup> ed.). Sage.
- Fisher, M. (2022, 24 de fevereiro). Putin's case for war, annotated. *The New York Times*. <https://www.nytimes.com/2022/02/24/world/europe/putin-ukraine-speech.html>
- Freedland, J. (2022, 25 de março). A key reason Putin's bloody invasion is faltering? He's no match for Zelenskiy's iPhone. *The Guardian*. <https://www.theguardian.com/commentisfree/2022/mar/25/churchill-iphone-volodymyr-zelenskiy-ukraine-west>
- Glover, N. (2011, 9 de outubro). Does security exist outside of the speech act? *E-International Relations*. <https://www.e-ir.info/2011/10/09/does-security-exist-outside-of-the-speech-act/>

- Hamilton, I. A. (2022, 3 de março). *Google and TripAdvisor disable restaurant reviews in Russia after they were flooded with protests against the Ukraine invasion*. Business Insider. <https://www.businessinsider.com/google-tripadvisor-disable-reviews-russia-ukraine-2022-3?r=US&IR=T>
- Hassan, R. (2008). *The information society*. Polity Press.
- Hern, A. (2022, 21 de março). TikTok algorithm directs users to fake news about Ukraine war, study says. *The Guardian*. <https://www.theguardian.com/technology/2022/mar/21/tiktok-algorithm-directs-users-to-fake-news-about-ukraine-war-study-says>
- Hirst, K. K. (2018, 10 de dezembro). *Understanding mass media and mass communication*. Thoughtco. <https://www.thoughtco.com/mass-media-and-communication-4177301>
- Holmes, O. (2022, 8 de fevereiro). Putin's massive table: Powerplay or paranoia? *The Guardian*. <https://www.theguardian.com/world/2022/feb/08/vladimir-putin-massive-table>
- Hough, P. (2018). *Understanding global security*. Routledge.
- Jewkes, Y. (2015). *Media and crime*. Sage.
- Karagiannopoulos, V. (2018). *Living with hacktivism: From conflict to symbiosis*. Springer International Publishing AG.
- Kremling, J., & Parker, A. (2017). *Cyberspace, cybersecurity, and cybercrime*. Sage.
- Lewis, K., Gray, K., & Meierhenrich, J. (2014). The structure of online activism. *Sociological Science*, 1, 1–9. <https://doi.org/10.15195/v1.a1>
- Li, X. (2013). Hacktivism and the first amendment: Drawing the line between cyber protests and crime. *Harvard Journal of Law & Technology*, 27(1), 302–323. <http://jolt.law.harvard.edu/articles/pdf/v27/27HarvJLTech301.pdf>
- Ludwig, S., & de Ruyter, K. (2016). Decoding social media speak: Developing a speech act theory research agenda. *Journal of Consumer Marketing*, 33(2), 124–144. <https://doi.org/10.1108/JCM-04-2015-1405>
- Lutkevich, B., & Bacon, M. (2021, maio). What is hacktivism? *Techtarget*. <https://www.techtarget.com/searchsecurity/definition/hacktivism>
- Maritime Industry News. (2022, 1 de março). *Hackers rename Putin's superyacht 'FCKPTN' in maritime data breach*. <https://marineindustrynews.co.uk/hackers-rename-putins-superyacht-fckptn-in-maritime-data-breach/>
- McGuinness, D. (2022, 17 de março). *Ukraine's Zelensky calls on Germany to tear down the Russian wall*. BBC News. <https://www.bbc.co.uk/news/world-europe-60777050>
- McQuail, D. (2010). *McQuail's mass communication theory* (6.<sup>a</sup> ed.). Sage.
- Milmo, D. (2022a, 18 de fevereiro). Amateur hackers warned against joining Ukraine's 'IT army'. *The Guardian*. <https://www.theguardian.com/world/2022/mar/18/amateur-hackers-warned-against-joining-ukraines-it-army>
- Milmo, D. (2022b, 27 de fevereiro). Anonymous: The hacker collective that has declared cyberwar on Russia. *The Guardian*. <https://www.theguardian.com/world/2022/feb/27/anonymous-the-hacker-collective-that-has-declared-cyberwar-on-russia>
- Mulvey, S. (2022, 26 de fevereiro). *Ukraine's Volodymyr Zelensky: The comedian president who is rising to the moment*. BBC News. <https://www.bbc.co.uk/news/world-europe-59667938>

- Munk, T. (2015). *Cyber-security in the European region: Anticipatory governance and practices* [Tese de doutoramento, The University of Manchester]. The University of Manchester. [https://www.research.manchester.ac.uk/portal/en/theses/cybersecurity-in-the-european-region-anticipatory-governance-and-practices\(6658eec7-cc61-4c84-9054-ea40cf405ed9\).html](https://www.research.manchester.ac.uk/portal/en/theses/cybersecurity-in-the-european-region-anticipatory-governance-and-practices(6658eec7-cc61-4c84-9054-ea40cf405ed9).html)
- Munk, T. (2018). Policing virtual spaces: Public and private online challenges in a legal perspective. In M. Den Boer (Ed.), *Comparative policing from a legal perspective* (pp. 228–254). EE publishing.
- Munk, T. (2022a). *The rise of politically motivated cyber attacks*. Routledge.
- Munk, T. (2022b, 9 de março). *Onlinekrig: Rusland mod Ukraine - og verden*. Jyllands Posten. <https://jyllands-posten.dk/debat/kronik/ECE13800745/onlinekrig-rusland-mod-ukraine-og-resten-af-verden/>
- Myustee. (2022). *Zelensky green tee shirt Ukraine*. <https://myustee.com/product/pkr-ukrainian-president-wearing-ukrainian-armed-forces-shirt/>
- Newman, L. A. (2022, 3 de março). Hacktivists stoke pandemonium amid Russia's war in Ukraine. *Wired*. <https://www.wired.com/story/hacktivists-pandemonium-russia-war-ukraine/>
- Newman, N., Dutton, W. H., & Blank, G. (2014). Social media and the news: Implications for the press and society. In M. Graham & W. H. Dutton (Eds.), *Society and the internet* (pp. 132–148). Oxford University Press.
- O'Connor, M. (2022, 24 de fevereiro). *Russia attack on Ukraine catastrophe for Europe, say Boris Johnson*. BBC News. <https://www.bbc.co.uk/news/uk-60504204>
- Parry, M. (2022, 20 de março). Watch live as Zelensky addresses Israel's parliament in video call. *The Independent*. <https://uk.news.yahoo.com/watch-live-zelensky-addresses-israel-161544575.html>
- Paul, K. (2022, 20 de março). TikTok was 'just a dancing app'. Then the Ukraine war started. *The Guardian*. <https://www.theguardian.com/technology/2022/mar/19/tiktok-ukraine-russia-war-disinformation>
- Picclick. (2022). *Zelensky green t-shirt tactical support Ukrainian shirt stand with Ukraine flag*. <https://picclick.com.au/zelensky-green-T-Shirt-Tactical-Shield-Stand-With-165382407015.html>
- Porche III, I. R., Paul, C., York, M., Serena, C. C., Sollinger, J. M., Axelband, E., Min, E. Y., & Held, B. J. (2013). *Redefining information warfare boundaries for an army in a wireless world*. Rand Corporation.
- Rauer, V. (2006). Symbols in action: Willy Brandt's Kneefall at the Warsaw Memorial. In J. C. Alexander, B. Giesen, & J. L. Mast (Eds.), *Social performance: Symbolic action, cultural pragmatics, and ritual* (pp. 257–282). Cambridge University Press.
- Roth, A., & Borger, J. (2022, 21 de fevereiro). Putin orders troops into eastern Ukraine on 'peace-keeping duties'. *The Guardian*. <https://www.theguardian.com/world/2022/feb/21/ukraine-putin-decide-recognition-breakaway-states-today>
- Russian state TV cuts away from Putin at pro-Russia rally – video. (2022, 18 de março). *The Guardian*. <https://www.theguardian.com/world/video/2022/mar/18/russian-state-tv-cuts-away-from-putin-at-pro-russia-rally-video>
- Salter, M. B. (2008). Securitization and desecuritization: A dramaturgical analysis of the Canadian Air Transport Security Authority. *Journal of International Relations and Development*, 11(4), 321–349. <https://doi.org/10.1057/jird.2008.20>
- Sauer, P. (2022, 18 de março). Putin praises Russian' unity' at rally as glitch cuts state TV broadcast. *The Guardian*. <https://www.theguardian.com/world/2022/mar/18/putin-praises-russian-unity-at-rally-but-state-tv-broadcast-is-cut-off>

- Saul, D. (2022, 15 de fevereiro). Putin's long tables explained: Why he puts some leaders, including Germany's Scholz, at an extreme distance. *Forbes*. <https://www.forbes.com/sites/dereksaul/2022/02/15/putins-long-tables-explained-why-he-puts-some-leaders-including-germanys-scholz-at-an-extreme-distance/?sh=7fbc9d0d70fb>
- Sauter, M. (2014). *The coming swarm*. Bloomsbury Academics.
- Schwarzenegger, A. [@Schwarzenegger] (2022, 17 de março). *I love the Russian people. That is why I have to tell you the truth. Please watch and share* [Tweet]. Twitter. <https://twitter.com/schwarzenegger/status/1504426844199669762>
- Scott, J. (2022, 8 de março). *Ukraine: Volodymyr Zelensky to address UK MPs in commons*. BBC News. <https://www.bbc.co.uk/news/uk-politics-60655003>
- 'Scum and traitors': Putin threatens Russians who oppose war in Ukraine – video. (2022, 17 de março). *The Guardian*. <https://www.theguardian.com/world/video/2022/mar/17/scum-and-traitors-putin-threatens-russians-who-oppose-war-in-ukraine-video>
- Siapera, E. (2018). *Understanding new media* (2.<sup>a</sup> ed.). Sage.
- Smith, A. (2022a, 28 de fevereiro). Anonymous trolls Putin by renaming yacht 'FCKPTN' and sending it to 'Hell' by hacking maritime data. *The Independent*. <https://www.independent.co.uk/tech/anonymous-vladimir-putin-yacht-fckptn-b2024780.html>
- Smith, A. (2022b, 17 de março). 'Scum and traitors': Under pressure over Ukraine, Putin turns his ire on Russians. NBC News. <https://www.nbcnews.com/news/world/scum-traitors-pressure-ukraine-putin-turns-ire-russians-rcna20410>
- Smith, A. (2022c, 24 de março). Google Maps suspends reviews as Russian landmarks flooded with photos of captured soldiers and news clips. *The Independent*. <https://www.independent.co.uk/tech/google-maps-russian-landmarks-photos-reviews-b2027638.html>
- 'Speak plainly!': Putin has tense exchange with his spy chief – video. (2022, 22 de fevereiro). *The Guardian*. <https://www.theguardian.com/world/video/2022/feb/22/speak-plainly-putin-tense-exchange-spy-chief-ukraine-video>
- Sorell, T. (2015). Human rights and hacktivism: The cases of Wikileaks and Anonymous. *Journal of Human Rights Practices*, 7(3), 391–410. <https://doi.org/10.1093/jhuman/huv012>
- Stanage, N. (2022, 16 de março). *Five takeaways from Zelensky's virtual address to congress*. The Hill. <https://thehill.com/homenews/senate/598428-five-takeaways-from-zelenskys-virtual-address-to-congress>
- Stokel-Walker, C., & Milmo, D. (2022, 15 de março). 'It's the right thing to do': The 300,000 volunteer hackers coming together to fight Russia. *The Guardian*. <https://www.theguardian.com/world/2022/mar/15/volunteer-hackers-fight-russia>
- Stupples, D. (2015, 26 de novembro). *The next war will be an information war, and we're not ready for it*. The Conversation. <https://theconversation.com/the-next-war-will-be-an-information-war-and-were-not-ready-for-it-51218>
- The Associated Press. (2022, 26 de fevereiro). *Live updates: Zelenskyy declines US offer to evacuate Kyiv*. AP NEWS. <https://apnews.com/article/russia-ukraine-business-europe-united-nations-kyiv-6ccba0905f1871992b93712d3585f548>
- The Kyiv Independent [@KyivIndependent]. (2022, 7 de março). *Hacking group Anonymous interrupts Russian state TV programs with footage of Russia's full-scale invasion of Ukraine and an anti-war* [Tweet]. Twitter. <https://twitter.com/KyivIndependent/status/1500631918584467464>

Trackray, L. (2022, 7 de março). Tripadvisor blocks some Russian reviews as customers use it to protest war. *The Independent*. <https://www.independent.co.uk/travel/news-and-advice/tripadvisor-blocks-russia-reviews-war-protest-b2030028.html>

Ukraine: Arnold Schwarzenegger's anti-war video trends on Russian social media. (2022, 18 de março). BBC News. <https://www.bbc.co.uk/news/world-us-canada-60794809>

United Nations. (2022, 22 de fevereiro). *Secretary-general says Russian Federation's recognition of 'Independent' Donetsk, Luhansk violate Ukraine's sovereignty, territorial integrity* [Press release]. <https://www.un.org/press/en/2022/sgsm21153.doc.htm>

Video: Ukrainian President Zelensky says country's leaders remain in Kyiv. (2022, 25 de fevereiro). *Wall Street Journal*. <https://www.wsj.com/video/video-ukrainian-president-zelensky-says-countrys-leaders-remain-in-kyiv/CFBBD1E0-2208-4379-A93E-85DA5CEC9228.html>

Walker, S. (2022, 21 de fevereiro). Putin's absurd, angry spectacle will be a turning point in his long reign. *The Guardian*. <https://www.theguardian.com/world/2022/feb/21/putin-angry-spectacle-amounts-to-declaration-war-ukraine>

Watson, K. (2022, 14 de março). *Zelensky to deliver virtual address to congress on Wednesday*. CBS News. <https://www.cbsnews.com/news/volodymyr-zelensky-ukraine-president-us-congress-virtual-address/>

Wolfsfeld, G. (2022). *Making sense of media and politics* (1.<sup>a</sup> ed.). Routledge.

Zelenskyy, V. [@@ZelenskyyUa]. (s.d.). *Tweets* [Perfil de Twitter]. Twitter. Retirado a 2 de abril de 2022 de [https://twitter.com/ZelenskyyUa?ref\\_src=twsrc%5Egoogle%7Ctwcamp%5Eserp%7Ctwgr%5Eauthor](https://twitter.com/ZelenskyyUa?ref_src=twsrc%5Egoogle%7Ctwcamp%5Eserp%7Ctwgr%5Eauthor)

## NOTAS BIOGRÁFICAS

Tine Munk tem como área de investigação o cibercrime e a segurança cibernética, com destaque para o cibercrime de motivação política e os ataques em grande escala. Ela dedica-se à investigação de agentes, motivações, meios e métodos, e relações de poder.

ORCID: <https://orcid.org/0000-0003-2356-8806>

Email: [tine.munk@ntu.ac.uk](mailto:tine.munk@ntu.ac.uk)

Morada: Nottingham Trent University, 50 Shakespeare Street, Nottingham, NG1 4FQ

Juan Ahmad tem como tema de investigação de doutoramento a guerra cibernética e o uso desordens informativas como arma em conflitos. Ele dedica-se à investigação de guerras híbridas, armas online, e cibersegurança e estratégias online.

ORCID: <https://orcid.org/0000-0003-0556-676X>

Email: [Juan.ahmad2021@my.ntu.ac.uk](mailto:Juan.ahmad2021@my.ntu.ac.uk)

Morada: Nottingham Trent University, 50 Shakespeare Street, Nottingham, NG1 4FQ

**Submetido: 05/04/2022 | Aceite: 08/06/2022**



Este trabalho encontra-se publicado com a Licença Internacional Creative Commons Atribuição 4.0.