Comunicação e Sociedade, vol. 42, 2022, pp. 221–241
https://doi.org/10.17231/comsoc.42(2022).4021

"I Need Ammunition, Not a Ride": The Ukrainian Cyber War

Tine Munk
Criminology and Criminal Justice Department, School of Social Science, Nottingham Trent University, Nottingham, United Kingdom
Conceptualization, project administration, writing - original draft, writing - review & editing

Juan Ahmad
Criminology and Criminal Justice Department, School of Social Science, Nottingham Trent University, Nottingham, United Kingdom
Writing – review & editing

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

"Preciso de Munições, Não de Boleia": A Guerra Cibernética Ucraniana

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

1. Introduction

On February 24 2022, Russian military vehicles violated Ukraine's sovereignty by crossing the borders into Ukraine and the subsequent invasion of a sovereign state. This invasion has been the most significant military threat to Europe since the end of World War II (O'Connor, 2022, para. 5). Russia paved the way for the invasion on February 21 by recognising two Ukrainian rebel regions, Donetsk and Luhansk, as independent states and entering a part of Ukraine on an artificial peace-keeping mission (Roth & Borger, 2022, para. 2; United Nations, 2022, para. 4). This action sent a shockwave through the international society that, for a long time, had tried to ease the regional tensions using diplomatic means.

Embedded in the Ukrainian conflict is the use of cyberweapons on multiple levels. One part of cyber warfare mirrors traditional military actions by air, water, and land.

Conventional cyberwar is essential in modern warfare, where actors directly attack vulnerabilities in computer systems and networks to damage or destroy essential critical infrastructure. This research has also uncovered that communication and activism are equally important in the hybrid warfare model. The war in Ukraine has demonstrated the power of online communications to reach a large audience to seek support, further a particular argument, and legitimise actions that would otherwise have been rejected under normal circumstances. When it is done successfully, communication is a powerful weapon that can activate and engage a vast amount of people.

This article focuses on online communication, whereby a successful speech can trigger a new form of activism and "togetherness", incorporating multiple groups of actors into the country's defence strategy. The speech act, conducted by President Zelenskyy and other Ukrainian leaders, has been instrumental in mobilising a widespread form of civic action in alliance with the state's defence of the country. The invasion and the atrocities conducted by Russian soldiers have shocked the western world and left people feeling powerless while watching the war unfolding online and in mass media. The constant online and offline communication has drawn attention to the situation in Ukraine and kept the war in the news feed worldwide. Nationals and foreign actors support the state against Russian invasion and aggression. Well-known hacktivist groups and ordinary online users have merged their resources and capabilities, using illegal and legal means to support Ukraine in an unjust war.

During the transition from a threat of war to the actual invasion by Russia, the Ukrainian leaders, in particular President Zelenskyy, have constantly balanced the world's need for information against calls for support to defend the country and protect its citizens. Undoubtedly, the Ukrainian leadership won the information warfare by using innovative and highlighted efficient communication skills incorporating various virtual spaces and social media. Numerous internal and external online users have rallied around Ukraine to support and help the state's "David versus Goliath fight" against Russian aggression. Embedded in this article is an investigation of assertive online communication and how it has activated non-governmental online users to engage in an online war.

The online networks linked to Castells' analysis of the online environment are still accurate and valuable for understanding current conflicts and actions. According to Castells (1996), "networks constitute the new social morphology of our societies, and the diffusion of networking logic substantially modifies the operation and outcomes in the process of production, experience, power, and culture" (p. 469; Hassan, 2008, p. 24). The technological development and the constant use of online spaces, such as social media, for communication in a global context have made significant changes in how people interact and communicate, and what is happening in one country has a substantial impact worldwide. The networked international community is not an innovation prompted by technology; it has been a part of human life throughout time and space, where people have organised themselves in human networks. Nevertheless, the way virtual spaces

and new communication forms have created a foundation for communication and information exchange can be referred back to new information technology paradigms which make a material foundation to expand the network to include entire social structures (Castells, 1996, p. 469; Hassan, 2008, p. 24).

2. Methodology

This article explores a new form of online activism that emerged during the first 40 days of the Ukrainian war, where governmental and non-governmental actors were involved in the country's defence on an unprecedented scale. The theoretical foundation of this article combines Castells' networked approach with the Copenhagen School of Security Studies' theory on security to understand the use of communication and its impact in an interconnected society. Elements of the Copenhagen School's securitization theory, such as the speech act, are used to understand how Ukrainian leaders have captured attention globally and fostered online civic actions outside the sphere of the state. The speech act is vital due to the successful communication with an audience, and legitimacy is provided to circumvent the normal processes of the state (Buzan et al., 1998).

The method is based on secondary qualitative research, including academic and news articles from well-recognised news outlets, periodical sources, and social media posts. The timeframe for the data collection is the first 40 days after the Russian invasion of Ukraine on February 24 2022. The case studies selected have been reported within this timeframe. However, they have not been documented in academic research as events unfolded at the time of writing. Therefore, social media content and mass media news articles have an important place to record key events. These sources help examine the relationship between the speech act and online activism. To validate the news stream, the researchers have used well-established western-oriented English-speaking news outlets and periodicals, such as *Reuters*, *Associated Press*, *The Guardian*, *BBC News*, *The Verge*, and *Wired*, among others, despite the potential bias in using regional sources. New articles are used to report events, not opinions. All reported events have been fact-checked against trustworthy news outlets' reports to ensure the quality of the content. Mass media and social media reporting are important sources in a developing conflict understanding how key actors are communicating and the impact of the communication. The data collection is based on grounded theory, where the data collected are critically compared with theoretical content. Sources such as academic books, chapters, peer-reviewed articles, reports, news articles, social media accounts, and web pages have been used to collect data, and the online research is based on search words, such as:

> Anonymous, cyberwar, cyberattacks, hacking Ukraine, hacking Russia, hacktivism, hacktivists Ukraine, information warfare, non-governmental cyber attacks, online attacks 2022, online support Ukraine, Putin 2022, Russia 2022, social movement, social actions, social media communication

Ukraine, social media support Ukraine, non-governmental hacking, hacking activities Ukraine, speech act, Ukraine 2022, war, war Ukraine, Zelenskyy, Zelenskyy speeches 2022.

All data are theoretically sampled and analysed based on the established socio-political approaches deriving from discourse analysis.

3. Social Media Communication

3.1. Social Media and Virtual Spaces

Information warfare is defined as "the conflict or struggle between two or more groups in the information environment" (Porche III et al., 2013; p. xv; Stupples, 2015, para. 2). In contemporary society, information and communication are constantly changing due to technological development, interdependencies, and the reliance on interconnected online systems. The rise of online platforms such as Facebook, Twitter, Instagram and TikTok has been a game-changer for communicating during a conflict where it is vital to reach out to numerous people simultaneously. The volume and extent of online social media communication are progressing, and new online means and methods have fuelled new types of political activism and social change. Online communications using social media and the online environment spans all ages, ethnicities and geographies unprecedentedly. This development includes virtually all online users; the spectacular rise of websites and virtual communication spaces has revolutionised how people communicate and interact with friends, family, and colleagues in public and private contexts, but also how people partake in public life and politics (Ludwig & de Ruyter, 2016, p. 124; Munk, 2022a, pp. 36–37)

Different types of communication and technologies are entwined in contemporary societies, such as radio (broadcasting and television), newspapers (magazines and books), and films (documentaries and movies; Ahmad, 2020, p. 6; Hirst, 2018, para. 1; McQuail, 2010, p. 4). Text and images help illustrate events and portray people's behaviour in power, professionally and privately. Media stories are circulated based on what the audience believes is essential, conforming to existing standards of justice and morality and what is deemed acceptable behaviour. Therefore, it is necessary to look at what is communicated and how information is circulated (Dunaway & Graber, 2022, p. 5). Online communication and broadcasting can influence public opinion and reach a large audience. Various virtual spaces are helpful for effectively sharing and visualising issues in the war and spreading propaganda and information on an equal footing. Therefore, mass media can be a platform for persuasion and mobilisation, thus, can present a specific topic positively or negatively (Ahmad, 2020, pp. 6–7; McQuail, 2010, pp. 136, 151–152).

3.2. The Powerful Speech Act

Ukraine does not have cyber capabilities that can match Russia like-for-like. Therefore, Ukraine focuses on strengthening its online and offline defence tactics, as its primary function is to protect people and properties and hold the territory. The Ukrainian information war tactic includes using an effective communicator, President Zelenskyy. The Ukrainian president's speeches and video clips are potent weapons to spread knowledge and ask for help and support, playing on the sympathy and guilt that the western world and natural allies of Ukraine have. Therefore, using computer technologies to communicate has proved to be timely and cost-effective ammunition. These different layers of cyber-defensive engagement should not be underestimated. New and innovative forms are observed and used in legal and illegal ways (Milmo, 2022b; Munk, 2022b; Paul, 2022; Trackray, 2022).

On the political spectrum, communication is essential to give legitimacy to different decisions that traditionally would not be acceptable. The speech act is integrated into the Copenhagen School's approach, a discursive practice that links security to a particular issue and frames it as a threat. Buzan et al. (1998) have argued that security issues need to meet a strictly defined threshold that allows the problems to be moved outside normal political areas. The securitization process is, therefore, "the move that takes politics beyond the established rules of the game and frames the issue either as a special kind of politics or as above politics" (Buzan et al., 1998, p. 23; Hough, 2018; Munk, 2015, pp. 33, 101). Through a successful speech act, problems are presented and dramatised as an urgent priority. If the speech act is successful, it gives an agent/ agency legitimacy to move it outside the normal democratic processes (Buzan et al., 1998, p. 26; Glover, 2011). The speech act is a necessary part of the process as the security issues are moved beyond the traditional stands or procedures. Yet, it is too narrow to understand that speech act as a pure state concern, as the process is not only linked to the security of a sovereign state or particular values (Munk, 2015, pp. 33, 105).

In the Ukrainian conflict, many people have chosen to get involved in online activism, prompted by the constant communication between Ukrainian leaders and citizens fighting to defend the territory. Yet, it is not all security concerns which can be securitised. The actual issue and the process can be influenced by the state's history, geographical and structural position (Buzan & Hansen, 2009, p. 34). Therefore, the speech act is used differently by Russia and Ukraine. The Ukrainian tactic is vibrant, inclusive and innovative as the state is fighting for survival. They need a broad level of support and acceptance to involve exceptional measures in wartime. Therefore, Ukrainian communicators are reaching out to a large audience on multiple levels, governmental/non-governmental and internal/external, using online communication routes to spread the messages widely. In comparison, Russian communication is based on old-fashioned means of communication that appear stiff, bureaucratic and outdated. Where Ukrainian communication is broadly distributed, Russian communication is mainly directed to a small, selected group of officials.

Some elements of exceptionalism are included in actions taken by key actors. For example, traditional illegal online means and methods, that is, hacking, defacement, and data compromises, are encouraged by both governmental and non-governmental actors in this conflict. Political speech acts include the power to organise people's minds and opinions and are instrumental tools to control and direct people. Through this process, various types of communication can reach a large audience if communicated correctly. Communication to a receptive audience is instrumental for establishing and maintaining social relationships, expressing feelings and promoting ideas, policies and programmes. The act aims to advance the speaker's intentions and context to receive legitimacy to act, which can be the securitization move. Despite hacking being a concept developed over the years, there are no clear hacking definitions. United Nations has attempted to create definitions over the years, but the institution has failed to gain support for its initiatives (Munk, 2018, pp. 239–240, 2022a, p. 87). The hacking typology includes "illegal access", "unauthorised access", or "illegal intrusion". The Council of Europe's Convention on Cybercrime (2001) criminalises illegal access to a computer (Article 2), illegal interception (Article 3), data interference (Article 4), and misuse of devices (Article 5). Ukraine is also a signatory state, ratifying the convention in 2006 (Ahmad, 2020, p. 9; Convention on Cybercrime, 2001, pp. 3–4; Council of Europe, 2022; Munk, 2022a, pp. 204–206). Despite being criminalised, hacking has been accepted as a tool to attack Russian systems and networks — just as Russia has used its numerous computer capabilities to attack Ukraine and take down critical infrastructure before and during the war (Ahmad, 2022, pp. 7–10; Munk, 2022b). As stated by Buzan et al. (1998),

> if, by means of an argument about the priority and urgency of an existential threat, the securitising actor has managed to break free of procedures or rules he or she would otherwise be bound by, we are witnessing an act of securitisation. (p. 25)

4. Social Media Presence and the Image of a Leader

4.1. Ukraine

From day one of the conflict, Ukrainian President Zelenskyy has had a significant online presence, where he communicates on Twitter and other social media, posting short videos and appearing in live broadcasts. Using the tag @ZelenskyyUa, he has constantly been available as the voice of the Ukrainian government (Zelenskyy, n.d.). Zelenskyy responds defiantly to the invasion and the ongoing war in all posts. When video clips show him standing on a street in Kyiv, he boosts morale, symbolising a commander-in-chief who suffers the same hardship as ordinary Ukrainians (CNN, 2022; Mulvey, 2022, paras. 2, 5, 9, 12). The celebrity status that Zelenskyy obtained during the first days of the war

has given him a powerful communication platform and constant mass media attention in a way that is not shared with his Russian counterpart.

In Ukraine, the invasion and the following war have created bonds between internal and external online users that can be linked to Castells' notion of networked societies. Access to numerous online spaces keeps the Ukrainian government in control of the narrative. Doing so challenges the traditional monopoly of powerful media to keep the conflict in the news feeds worldwide (Siapera, 2018, p. 47). However, using social media for communication does not replace core news outlets. Instead, the active online presence acts as an accelerator to generate interest in main events, progress a particular narrative or counter state propaganda from the adversary state (Newman et al., 2014, p. 139). Although online platforms are helpful for direct communication, they also have value for indirectly conveying messages online using a snowballing effect, where text and images are shared and reshared beyond the original audience. The online speech act goes in two directions. Firstly, the online presence is essential to keep an audience informed about the situation. At the same time, the communicators stay in control of the narrative. Secondly, it is used traditionally where political actors get legitimacy to circumvent conventional processes in a war-torn country fighting for survival. This online community is designed to help and support Ukraine, fuelled by a sense of powerlessness as a trigger for action.

The quote "I don't need a ride, I need ammunition" went viral after Zelenskyy rejected an offer from the United States to evacuate from Kyiv in the early days of the war (Braithwaite, 2022; Freedland, 2022, para. 8; The Associated Press, 2022). This message is considered to be the prototype of digital statesmanship. Live broadcast presentations have been shown in parliaments worldwide, such as the European Union, United Kingdom, Germany, Israel and the United States, where constantly Zelenskyy delivered virtual addresses as a part of his strategy to gain support (Freedland, 2022, paras. 12–13; McGuinness, 2022; Parry, 2022; Scott, 2022; Watson, 2022). Due to global online communication, people are used to following significant events live when they unfold. Yet, this also creates a level of news fatigue. People are becoming emotionally distanced and desensitised due to the constant flow of images of bombings and atrocities from global hotspots. The broadcasts often escalate the news coverage to gain media attention (Jewkes, 2015, p. 33). That means that the people in charge of the speech act must constantly balance their reporting against the interest of people, other world events, and the audience's engagement with the topic. The Ukrainian leadership has been eminent in balancing these as the online audience has continued to increase support and become actively engaged in the defence.

Although verbal speech is essential for communication, particular repeating images and symbols are powerful tools for creating associations with the original speech act. The use of symbols in politics is not new. Symbols in action are powerful to illustrate a particular stance or paradigm change. In 1970, when Willy Brandt, the then chancellor of the German Federal Republic, kneeled in front of the Warsaw Memorial in honour of Jewish heroes of the 1943 Ghetto was perceived as symbolising a new era and changes

in Germany's postwar politics (Rauer, 2006, p. 258). The use of symbols and particular behaviours have been deeply integrated into politics. The symbol value in Zelenskyy's actions is visible in the address to the nation, where he and the leadership group are filmed walking around Kyiv the first night after the Russian invasion. This film signals several things: the government remain in Kyiv, acts in solidarity with the Ukrainian citizens, and does not fear Kremlin's actions ("Video: Ukrainian President Zelensky Says Country's Leaders Remain in Kyiv", 2022). The performative actions of the Ukrainian leadership enable the speech act by communicating the message worldwide using several different communicative methods by repeating recognised words, images or slogans online and offline. Previously, President Zelenskyy was officially addressing the Ukrainian nation from the presidential office, wearing a suit and tie. Since the invasion, Zelenskyy's internal and external addresses have been conducted in neutral places to avoid revealing his location. He predominately wears his makeshift t-shirt with the Ukrainian flag or other state symbols (Buncombe, 2022; Freedland, 2022, para. 7; Stanage, 2022, para. 2). This t-shirt has become a symbol of his leadership and resistance toward Russia. It is trending on commercial online websites, and a charity Lego-like figure is sold in support of Ukraine, symbolising his leadership. The iconic t-shirt enables Zelenskyy to stand out and demonstrate that he is a part of/stands together with Ukrainians during this challenging time (Burton, 2022; Myustee, 2022; Picclick, 2022).

4.2. Russia

While Ukraine's President Zelenskyy remains in a position where he remains dignified, resolute and well-articulated online, his Russian counterpart is perceived differently (Mulvey, 2022, para. 3; Smith, 2022b, paras. 2, 4). Russia's President Putin remains a distant figure. When he appears in mass media, he is either sitting far away in a vast room, by the end of a long table, communicating online using a giant computer monitor or sitting in an oversized chair (Holmes, 2022; Saul, 2022; Walker, 2022, para. 7). In his appearance, Putin appears pale, cold, withdrawn, aggressive, erratic, and spiteful. For example, in the tense exchange between President Putin and Naryshkin, chief of the foreign intelligence service, Putin interrupted the spy chef several times, angrily asking him to "speak plainly" ("'Speak Plainly!': Putin Has Tense Exchange With His Spy Chief – Video", 2022; Walker, 2022, para. 10).

Other speeches have included aggressive rants about Ukraine, North Atlantic Treaty Organization, and everyone who stands in the way. Instead of being a unifying and leading Russian statesman using the speech act actively to build up support, Putin threatened anyone who questioned this invasion by calling for a "natural cleansing" of "scum and traitors" (CBS/AP, 2022; "'Scum and Traitors': Putin Threatens Russians Who Oppose War in Ukraine – Video", 2022; Smith, 2022b). This negative-loaded narrative seems to be a part of Russian propaganda. Putin repeated these claims at his "unity" rally (2022) in Moscow on the anniversary of the annexation of Crimea, where he for once appeared

to deliver a 5-minute speech in front of an audience (Fisher, 2022; "Russian State TV Cuts Away From Putin at Pro-Russia Rally – Video", 2022; Sauer, 2022).

The Russian speech act aims to promote power and control, supported by the Russian propaganda machine claiming that the war is a "special operation" and that Ukraine constitutes a direct threat to Russia and the Russian population. The actual speech act conducted by Putin mirrors the speech act outlined by the Copenhagen School, where the state apparatus is in control of the narrative and censorship has been imposed on mass media. The process is manipulative as it is solely in the speaker's power to frame the security issues and determine how to conduct the speech act (Munk, 2015, p. 105; Salter, 2008, p. 328). The process appears premeditated, directed to a chosen audience and promoted to archive acceptance (Munk, 2015, p. 105). However, the Russian state apparatus does not have the same communication infrastructure as Ukraine and cannot generate the same level of support internally and externally using various online and offline media. Therefore, the Russian speech act is only directed at the Kremlin leadership that always will support President Putin for fear of reprisals.

5. Political Activism

Activism is defined within a specific context. It is driven by confrontation and displeasure with particular policies and practices, and it is conducted to achieve changes through various means, such as protests, marches, speeches, and singing, among others (Anderson & Herr, 2007). The activism deriving from the intense Ukrainian communication is value-based, primarily understood as political activism closely linked to people's feelings about the world and what matters most to them, such as right and wrong (Munk, 2022a, p. 31). Social media, cyberspace and computer technologies have changed the way people can connect instantly with each other. At the same time, computer technologies create an unprecedented opportunity for distributing information and inspiring and influencing other people (Lewis et al., 2014; Munk, 2022a, pp. 33–34).

Online activism is often associated with political mobilisation, which includes computer technologies and networks. However, this form of cyberactivism is not necessarily illegal. The users use online spaces to protest or support political causes online and offline (Lutkevich & Bacon, 2021, para. 1; Munk, 2022a, p. 201; Sauter, 2014, p. 26). The online environment allows groups to reach a large audience across traditional and social borders to distribute information and create awareness about causes, tactics, and tools (Ahmad, 2020, p. 16; Kremling & Parker, 2017). Different actors have been vocal in their critique of Russia and support of Ukraine by defending Ukraine's sovereignty and freedom. The United States actor Arnold Schwarzenegger's appeal to the Russian people in a Twitter message is one way to show solidarity with Ukraine and reach out to the Russian population to inform them about the war (Schwarzenegger, 2022; *Ukraine: Arnold Schwarzenegger's Anti-War Video Trends on Russian Social Media – Video, 2022*).

The ammunition Zelenskyy called for in the early days of the war has shown to take many different shapes and forms. Well-known hacktivist groups are mingling with

ordinary online users to defeat Russia online. Hacktivism, as a concept, merges hacking and activism, which often has been deployed against powerful institutions, businesses, or states. Despite having a reasonable level of support among the public, their activities are not considered legitimate and fall within the scope of cybercrime. The successful speech act conducted by Ukrainian officials and the constant focus on the war by mass media has had an effect. Different forms of activism have consequently appeared, that is, legal and illegal, governmental and non-governmental. The activation of other groups in society is essential.

All types of actions have been deployed to support Ukraine's defence, where hackers have been able to disrupt the data traffic on Kremlin and the Duma's webpages and gain access to state-owned media services, banks and companies. Not all of these actions are illegal. A large number of online users carry out activities within the legal sphere, such as circulating counterpropaganda, collecting information, and fighting online disinformation. Advertising specialists have a role in designing and disseminating adverts to raise awareness about the war in Russia and Belarus by circumventing censorship and platform closures (Stokel-Walker & Milmo, 2022). The common determinator for all these actors is a belief in the leadership of Ukraine and that their actions help defeat Russia.

5.1. Hackers, Hacktivists and Activists

5.1.1. The Information Technology Army and Hackers

Ukraine is building a volunteer information technology (IT) army to help enhance its defence. However, several activities are based on hacking and distributed denial-of-service (DDoS) attacks illegally breaking into corporations and governmental targets. Two days into the Russian invasion, Ukraine's deputy prime minister and the minister for digital transformation, Fedorov, announced in a tweet the establishment of a volunteer IT army. The tweet included a plea to stop tech companies from working with Russia and an attempt to attract computer-savvy talents, such as developers, cyber-specialists, designers, copywriters, and marketers, to engage in the new online frontier (Burgess, 2022, para. 2; Stokel-Walker & Milmo, 2022). Contrary to many other private initiatives, the IT army is a direct proxy of the state, where tasks are assigned to volunteers depending on their engagement and computing skills. A Telegram channel, the "IT Army of Ukraine", is where the assignments are distributed. More than 300,000 people subscribed to the channel 3 weeks after this announcement, and the numbers have increased since (Burgess, 2022; Milmo, 2022a, para. 2; Newman, 2022). These actions are a clear outcome of a successful speech where the area has been framed as an existential threat, and an audience has given acceptance for the state to circumvent the usual rules and processes, that is, by incorporating hacking and other illegal attack forms in the toolbox. Political power and virtual spaces have significant benefits when combined. By using the

online spaces and creating a Telegram route, it is possible to mobilise and "employ" a large number of voluntary actors who can either engage in direct online actions or work the web (Wolfsfeld, 2022, p. 5). However, the political actors still need to balance the speech act with the need to activate many volunteers to help with the online defence — and not using the same tactic as Russia. The goodwill the Ukrainian government enjoyed is linked to clear communication and the speech act. Zelenskyy and governmental actors' online presence, Russia's disregard for international laws, and its unprovoked attack on a sovereign country have been instrumental in forming this extensive volunteer IT army.

Although Ukraine now has recruited many internal IT volunteers, the call was also circulated online, and foreign volunteers signed up via the Telegram channel. This engagement by foreign nationals led to a stern warning from western officials about the dangers of these private operations. Firstly, hacking and similar activities are criminalised, and hackers would break the national law to help Ukraine from abroad (Ahmad, 2020, p. 7; Milmo, 2022a, paras. 3–4, 8; Munk, 2022a, pp. 204–207). Secondly, concerns have been raised that these actions might unintentionally spill over to other areas enabling Putin to claim that the west attacks Russia — or that the attack impacts Ukraine too, that is, cyber worms or viruses (Burgess, 2022, para. 13; Milmo, 2022a, para. 9). Yet, compared with the Ukrainian speech act, these warnings have not had the anticipated effect, as many foreign hackers are still involved in actions supporting Ukraine.

5.1.2. Hacktivists

Hacktivism combines hacking techniques and tools with activism, enabling a particular political message to be delivered. It is not only the IT army using illegal means to fight against Russia. Contrary to traditional political foundations, the online environment enables a new type of activism where people can connect and pursue alternative possibilities of action regardless of where they are placed (Castells & Kumar, 2014, p. 95; Sorell, 2015, p. 392). Early in the conflict, the international hacktivist group Anonymous and affiliates declared war on Russia. By doing so, they have been able to justify their use of exceptional means and methods despite their non-governmental status. However, the different hacking groups have been vocal online and communicated with the network by replicating the speech act (Anonymous, n.d.; Coker, 2022; Milmo, 2022b). In line with Castells (1996) network theory, Anonymous simultaneously act on local and global issues. Since all the actors are interlinked online, they operate on the international level, creating a powerful force, as seen in the first 4 weeks after the Russian invasion of Ukraine. Anonymous is a decentralised hacker collective, dedicating its efforts and hacking skills to promoting the rights to online privacy, free internet and anti-censorship. The group is known for their long-term operations against states, businesses, associations and other power full actors, such as #OPPayback, #OPAvengeAssange, and its involvement in the Arab Spring protests (Ahmad, 2020, p. 18; Karagiannopoulos, 2018, p. 16; Li, 2013, p. 307; Munk, 2022a, p. 215; Sorell, 2015, pp. 393–397).

Groups like Anonymous are reacting to the speech act by the Ukrainian officials online calls for help. Hacktivist groups use various criminalised means and methods similar to the IT army. These practices have gained momentum during the war, and it is acceptable to use them due to a successful speech act. During the first 4 weeks of the war, Anonymous successfully conducted campaigns against Russia, such as hacking and DDoS attacks against the Russian ministry of defence database and the Kremlin's web pages (Milmo, 2022b, para. 3). Hacktivists have also hacked into several Russian state television channels, such as Russia 24, Channel 1, and Moscow 24, where shows were replaced by various footage informing about the invasion of Ukraine, anti-war messages, Ukrainian music and symbols (Anonymous TV, 2022; Milmo, 2022b, para. 4; The Kyiv Independent, 2022). The group has also taken credit for a marine tracking data defacement renaming Putin's superyacht "FCKPTN" and changing its destination to "Hell" (Maritime Industry News, 2022, para. 1; Newman, 2022, para. 6; Smith, 2022a).

Anonymous is not the only group operating in this conflict. The Distributed-Denial-of-Secrets (DDoSecrets) released 15 different sets of Russian information obtained from other hacktivist groups, such as realising 820GB of illegally obtained data from the Russian Roskomnadzor (Coker, 2022; Collier et al., 2022, para. 18). However, these leaking activities are illegal, and DDoSecrets is already under investigation in the United States regarding the BlueLeaks data dump in 2020 (Munk, 2022a, p. 230). Other hacktivism groups have defaced Russian webpages and replaced content with pro-Ukrainian or anti-Putin messages. For example, groups have defaced a webpage belonging to the Russian Space Research Institute and have presumably leaked data from the Russian space agency, Roscosmos (Newman, 2022, para. 1).

5.1.3. Other Online Activists

Online activists have been inspired by the constant communication from the Ukrainian leadership. In one of his many speeches, President Zelenskyy asked Russian TikTok users, scientists, doctors, bloggers, and stand-up comedians, to step up and help win the war (Chayka, 2022; Paul, 2022). The TikTok generation/generation Z has already demonstrated their activism during the United States 2020 presidential election and the "BlackLivesMatter" protests after the murder of George Floyd. Social media sites are essential in conducting these civic actions as user-generated content is spread quickly. This type of mobilisation/communication fits into the original speech act that asks for help and support. Social media acts as microblogging sites where news is distributed widely despite being unreliable (Jewkes, 2015, p. 73). Yes, images created on mobile phones, texts and emails circulated are powerful communications. As a social media platform, TikTok is known for being choppy and decontextualised with upbeat music, but it is also a popular online communication platform (Ahmad, 2020, pp. 16, 41–42; Chayka, 2022; Munk, 2022a, pp. 222–224).

Videos tagged #Ukraine have received more than 30,000,000,000 views on the platform within 4 weeks. However, there are issues related to using TikTok to distribute information. The company's algorithm determines what data is pushed within the news feed based on the algorithm's favour and user engagement. The core element of TikTok is how the platform enables online users to upload video clips and soundbites without references. Therefore, it is nearly impossible to verify content. Unfortunately, the TikTok generation is less concerned about the verification of information. They are more interested in reaching the goal by creating or promoting a powerful video that catches attention (Clayton & Dyer, 2022; Hern, 2022b; Paul, 2022). For example, "Ghost of Kyiv" shows a Russian jet being shot down. But this footage is from a video game unrelated to the conflict. Yet, that does not stop the video from being shared further (Chayka, 2022, para. 8; Hern, 2022, para. 5).

Numerous people are engaged in supporting Ukraine using legal means and methods. Undoubtedly, these provide powerful ammunition to the country's defence. Alphabet Inc. suspended new user-generated reviews from being uploaded on the platform after an inevitable influx of political statements. Statements were uploaded in comment fields where users could interact and leave reviews. For example, Anonymous encouraged online users to post reviews on Russian, Ukrainian and Belarusian businesses and tourist destinations on Google Maps. These reviews would form an essential information plank by circumventing censorship. Anonymous encouraged its 7,700,000 followers to go to Google Maps, find a restaurant or business, and upload a review that includes information on what is happening in Ukraine (Anonymous, 2022; Baynes, 2022). For example, a screenshot of a TripAdvisor review, uploaded on an Anonymous (2022) Twitter page, stated: "the food was great! Unfortunately, Putin spoiled our appetites by invading Ukraine. Stand up to your dictator, stop killing innocent people! Your government is lying to you. Get up!".

Other users argued that giving five stars in the review is important to avoid ruining the business as they are most likely to be small family-owned/small businesses (Anonymous, 2022; Baynes, 2022). Alphabet Inc. moved quickly to block new reviews, as the campaign violated the company's policy against fake, copied, off-topic, abusive or defamatory reviews. Similar messages were placed on TripAdvisor. Instead of reviewing a restaurant, café, or shop, a text emerged with information about the war. TripAdvisor's moderating system picked up the increase in fake reviews. Therefore, the review section was temporarily suspended to prevent activists' risky postings. Instead, the company directed its users to their community forum, where information about the war was posted (Baynes, 2022; Deighton, 2022, para. 7; Hamilton, 2022; Smith, 2022c).

6. Conclusion

The areas covered in this article show only a snapshot of the actions conducted within the first 40 days. However, a communication pattern has emerged where Ukraine has combined securitization speech acts with other types of communications using text, video clips, live broadcasts, symbols and recognisable behaviours.

President Zelenskyy would probably prefer more flights, tanks and missiles, but he still needs to win the online war. So far, the Ukrainian leadership has successfully communicated with numerous people internally and externally. These constant communications have become a valuable part of the government's weaponry to defend the country. The actual media war is already won by Zelenskyy and his masterful use of social media for different types of communications and direct live appeals for help. It is interesting how positive people worldwide have reacted to these types of communications and the level of goodwill the Ukrainians have received.

Social media and online communication have obtained a prominent position in modern politics. This means that the securitization process can be amplified online. The speech act can be linked to the traditional use of obtaining legitimacy for moving the referent object outside the normal processes. Contemporary politicians are deeply engaged in communicating with an online audience about everyday politics that does not need to be framed as security threats. Fuelled by Zelenskyy's constant online presence and call for action, citizens worldwide have been drawn to the conflict by engaging in low-level political activism, hacking and hacktivism. Online governmental communication and civic activities will be mirrored in future conflicts. This means that the actual war is fought on two fronts, one on the official front, where the state directs military actions. The second front is the voluntary army, which has a different level of engagement, skills, and incitement to be involved. However, this voluntary, non-governmental army is autonomous and is only engaged as long as it fights for a just cause. The new ammunition is people skills and engagement in the conflict, and the impact cannot be underestimated.

References

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]. (n.d.). *Tweets* [Twitter profile]. Twitter. Retrieved March 27, 2022, from https://twitter.com/YourAnonNews?ref_src=twsrc%5Egoogle%7Ctwcamp%5Eserp%7Ctwgr%5Eauthor

Anonymous. [@YourAnonNews]. (2022, February 28). *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, February 26). *JUST IN: #Russian state TV channels have been hacked by #Anonymous to broadcast the truth about what happens in #Ukraine* [Video attached] [Tweet]. Twitter. https://twitter.com/YourAnonTV/status/1497678663046905863?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1497678663046905863%7Ctwgr%5E%7Ctwcon%5Es1_&ref_url=https%3A%2F%2Fwww.theguardian.com%2Fworld%2F2022%2Ffeb%2F27%2Fanonymous-the-hacker-collectiv

Baynes, M. (2022, March 2). *'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-12555968

Braithwaite, S. (2022, February 26). *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, March 18). 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, February 27). 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, March 17). 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, March 18). *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, March 3). 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, March 5). *Ukraine war: The TikToker spreading viral videos.* BBC News. https://www.bbc.co.uk/news/technology-60613331

CNN. (2022, February 26). *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, March 11). 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, March 22). *Hacktivists, new and veteran, target Russia with one of cyber's oldest tools.* NBC News. https://www.nbcnews.com/tech/security/hacktivists-new-veteran-target-russia-one-cybers-oldest-tools-rcna20652

Convention on cybercrime, November 23, 2001, https://rm.coe.int/1680081561

Council of Europe. (2022, March 27). Chart of signatures and ratifications of Treaty 185. https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185

Deighton, K. (2022, March 2). 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* (11th ed.). Sage.

Fisher, M. (2022, February 24). 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, March). 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, October 9). 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, March 3). *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, March 21). 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, December 10). *Understanding mass media and mass communication.* Thoughtco. https://www.thoughtco.com/mass-media-and-communication-4177301

Holmes, O. (2022, February). 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, May). What is hacktivism? *Techtarget*. https://www.techtarget.com/searchsecurity/definition/hacktivism

Maritime Industry News. (2022, March 1). *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, March 17). *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* (6nd ed.). Sage.

Milmo, D. (2022a, February 18). 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, February 27). 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, February 26). *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* [Doctoral dissertation, 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

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 publising.

Munk, T. (2022a). *The rise of politically motivated cyber attacks.* Routledge.

Munk, T. (2022b, March 9). *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, March 3). 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, February 24). *Russia attack on Ukraine catastrophe for Europe, say Boris Johnson*. BBC News. https://www.bbc.co.uk/news/uk-60504204

Parry, M. (2022, March 20). 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, March 20). 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 Warshaw 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, February 21). 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, March 18). *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, March 18). 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, February 15). 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, March 17). *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, March 8). *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, March 17). *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* (2nd ed.). Sage.

Smith, A. (2022a, February 28). 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, March 17). *'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, March 24). 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, February 22). *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. J*ournal of Human Rights Practices*, *7*(3), 391–410. https://doi.org/10.1093/jhuman/huv012

Stanage, N. (2022, March 16). *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, March 15). '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, November 26). *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, February 26). *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, March 7). *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, March 7). 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, March 18). BBC News. https://www.bbc.co.uk/news/world-us-canada-60794809

United Nations. (2022, February 22). *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, February 25). *Wall Street Journal*. https://www.wsj.com/video/video-ukrainian-president-zelensky-says-countrys-leaders-remain-in-kyiv/CFFBD1E0-2208-4379-A93E-85DA5CEC9228.html

Walker, S. (2022, February 21). 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, March 14). *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* (1st ed.). Routledge.

Zelenskyy, V. [@@ZelenskyyUa]. (n.d.). *Tweets* [Twitter profile]. Twitter. Retrieved April 2, 2022, from https://twitter.com/ZelenskyyUa?ref_src=twsrc%5Egoogle%7Ctwcamp%5Eserp%7Ctwgr%5Eauthor

Biographical Notes

Tine Munk's research area is cybercrime and cybersecurity, emphasising politically motivated cybercrime and large-scale attacks. Tine Munk is interested in researching actors, motivations, means and methods, and power relations.

ORCID: https://orcid.org/0000-0003-2356-8806
Email: tine.munk@ntu.ac.uk
Address: Nottingham Trent University, 50 Shakespeare Street, Nottingham, NG1 4FQ

Juan Ahmad's doctoral study is related to cyberwarfare and the use of information disorder as a weapon in conflicts. Juan Ahmad is interested in researching hybrid warfare, online weapons, and online cyber-security and strategies.

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

Email: Juan.ahmad2021@my.ntu.ac.uk
Address: Nottingham Trent University, 50 Shakespeare Street, Nottingham, NG1 4FQ

Submitted: 05/04/2022 | Accepted: 08/06/2022