Public Networked Discourses in the Ukraine-Russia Conflict: 'Patriotic Hackers' and Digital Populism*

Tetyana Lokot

School of Communications, Dublin City University

ABSTRACT

This paper explores the self-presentation and online discursive practices of grassroots hacker collectives on both sides of the Ukraine-Russia conflict within a larger geopolitical climate of a contested globalisation agenda and a growing fear of cyber warfare. Both pro-Russian and pro-Ukrainian hacker groups engage in DDoS attacks, malware distribution and leaking stolen information from the opposing side. They also use social media to enter the broader political discourse around the conflict. The paper analyses the Twitter posts of both collectives to reveal key modes of online practices and key discursive themes in the context of the conflict, such as political activism, information warfare, hacker ethics and patriotism. The study elucidates how these groups use their social media presence to construct a 'patriotic hacker' identity for themselves, to delegitimise their opponents and ultimately, to connect to the broader populist discourse, where issues of patriotism, sovereignty and nationhood are contested.

INTRODUCTION

On 1 June 2017 Russian President Vladimir Putin held a press event with international news agencies as part of his participation in the Petersburg International Economic Forum. Responding to a question about possible Russian meddling in elections in Germany, Putin unequivocally denied the Kremlin's involvement in any hacking attacks or interference in the 2016 US presidential vote, saying these hackers could have come from any country.[1] He did, however, have an interesting corollary to add:

*This article is based on the author's contribution to a roundtable at the annual conference of the International Affairs Standing Committee of the Royal Irish Academy, titled 'Retreat from Globalisation? Brexit, Trump and the New Populism', which took place at the Royal Irish Academy in Dublin on 31 May 2017. This research was supported in part by funding under the 2016–17 Journal Publication Scheme of the Faculty of Humanities and Social Sciences, Dublin City University.

[1]John Fraher and Ilya Arkhipov, 'Putin says patriotic hackers could be fighting for Russia', *Bloomberg*, 1 June 2017, available at: https://www.bloomberg.com/news/articles/2017–06–01/putin-says-patriotic-hackers-could-be-fighting-for-russia-j3eb8n22 (accessed 6 September 2017).

Author's e-mail: tanya.lokot@dcu.ie

Irish Studies in International Affairs, Vol. 28 (2017), 1–18

doi: https://doi.org/10.3318/ISIA.2017.28.9

> Hackers are free people, like artists: they wake up in a good mood and they start painting. It's the same with hackers, if they woke up and read about something happening in international relations, and if they're patriotically inclined, they will do their part.[2]

Putin's remark indicates the broader ongoing debate about the role of 'rogue' non-state actors in geopolitical events and their amorphous relationship with nation states in cases such as elections, military conflicts and civic uprisings. This paper explores the self-presentation and online identity performance of self-proclaimed grass-roots hacker collectives on both sides of the Russia-Ukraine conflict. Specifically, it is interested in the role hackers play in this arena beyond their efforts to disrupt or damage opponents and their alleged ties to nation states. How does the discourse generated by hackers and around them shape the public's understanding of the parties to the conflict and contribute to the overall political climate around these events?

The conflict between Ukraine and Russia that began shortly after the Euromaidan protests in the spring of 2014 is a curious phenomenon that most have stopped short of calling a war.[3] In the spring of 2014, Russia annexed the Crimean Peninsula (officially Ukrainian territory), and later covertly supported armed separatist rebellions in the Donetsk and Luhansk regions of eastern Ukraine, providing weapons, military training, troops and equipment, and humanitarian aid.[4] Beyond explicit and covert military activity on the ground, Russia and pro-Russian forces have also engaged in what has been termed 'hybrid warfare'—manipulating information about and coverage of the conflict through state media propaganda and social media astroturfing, engaging in diplomatic games and resorting to other 'active measures', including hacking, leaks and DDoS attacks on Ukrainian websites and infrastructure.[5,6] Especially on the cyber warfare front, the Ukrainian side has often responded in kind. A key issue in the context of these digital attacks is that identifying the actors behind them is difficult, and it isn't always possible to explicitly identify whether these activities are supported by state actors or are the work of digital vigilantes acting independently on either side. Increasingly, however, we can observe these 'rogue' individuals and groups entering the public limelight.

While the military action in Crimea and, for the past three years, parts of eastern Ukraine occupied by Russia-supported separatist forces has been bloody and ongoing, a no less ardent battle has been waged online. Both pro-Russian and pro-Ukrainian hacker groups actively engage in DDoS attacks, malware distribution and leaking stolen information from 'the other side'. They also use social media to enter the broader political discourse around

[2]Lenta.Ru, 'Putin compares hackers to free artists' ['Путин сравнил хакеров со свободными художниками'], 1 June 2017, available at: https://lenta.ru/news/2017/06/01/hudohakeri/ (6 September 2017).

[3]The Euromaidan protests started in Ukraine in November 2013 in response to the refusal of then president Viktor Yanukovych to sign the Association Agreement with the EU, and lasted into the spring of 2014, becoming a broader pro-European movement against government corruption, abuse of power and police brutality.

[4]Maria Snegovaya, 'Putin's information warfare in Ukraine: Soviet origins of Russia's hybrid warfare', *Russia Report 1* (September 2015).

[5]Ralph D. Thiele, 'Crisis in Ukraine: the emergence of hybrid warfare', *ISPSW Strategic Series* 347 (2015), 1–13.

[6]Andy Greenberg, 'How an entire nation became Russia's test lab for cyberwar', *WIRED*, 20 June 2017, available at: https://www.wired.com/story/russian-hackers-attack-ukraine/ (6 September 2017).

the conflict and to create and manage public identities and profiles online. The most influential among these groups are CyberBerkut, a pro-Russian hacker group, and Ukrainian Cyber Alliance, a pro-Ukrainian collective. Both groups have an active online presence, chiefly on social media platforms such as Twitter and Facebook.

The paper examines the discourse in the Twitter posts of both collectives during the conflict period (2014–17) in the context of extremist hacking as an emerging part of modern hybrid warfare. This study is chiefly concerned with understanding how these groups manage the discourse about their activity online by way of narrating their own exploits and making meaning of their actions.

The paper poses the following research questions:

1. To what ends do hackers in the Ukraine-Russia conflict engage in public and political discourse on social media? What kind of direct action and discursive action do these groups engage in online?
2. What are the specific discursive approaches that pro-Russian and pro-Ukrainian hackers employ during the conflict to construct their own identity and that of their opponents on social media? How do these discursive identities resonate with the broader political/geopolitical discourse?

The analysis reveals key modes of social media discourse (such as promoting political views or linking to leaks) and its key themes in the context of the conflict, such as political extremism, information warfare, hacker ethics, grass-roots activism and patriotism. The paper also considers the differences between how each group discusses these themes and uses them to frame their own identity and that of their opponents. With added analysis of the exploitation of other Twitter platform mechanics (e.g., hashtags, retweets, mentions and embedded content) by each hacker group, the paper elucidates how these groups use their social media presence to engage in a 'politics of spectacle' that contributes to the growing populist sentiment that is framed and promoted differently on both sides of the conflict. Through their public online discourse the hacker groups construct a 'patriotic hacker' identity and attempt to establish their side as the one with greater 'moral authority', while at the same time seeking to 'other' their foes and the side they represent as a less legitimate party to the conflict.

The research takes on board Maura Conway's recent suggestions to expand research on online extremism and terrorism, specifically by widening the range of types of extremism studied and in engaging with interdisciplinary approaches such as internet, society and technology studies.[7] The paper also heeds Conway's call for engaging in deeper analyses of online extremist activity and discourse by examining them through the lens of a larger set of political concerns and positing connections between online extremist actors' behaviour and the growing global trends towards nationalism and populism in modern hybrid conflicts.

HACKERS IN THE LIMELIGHT

The politics of hacking

The debates about who hackers are and what exactly they do go back to the early days of the internet and beyond. Overall, the hacking community has always

[7]Maura Conway, 'Determining the role of the internet in violent extremism and terrorism: six suggestions for progressing research', *Studies in Conflict and Terrorism* 40 (1) (2016), 77–98.

been composed of a diverse set of individuals who may be said to share some common principles such as freedom, privacy, meritocracy and access.[8] Though these values are not exclusive to hackers, those who adopt the label have refashioned these ongoing political concerns through technological means, demonstrating the relevance of these moral and legal issues for the digital age. Gradually, though, the hacking community has shifted from being preoccupied with the politics of technology to a concern with politics writ large, as evident from hackers taking active roles in anarchist and anti-globalisation movements.[9]

An important point to be made about the history of hacking is that the 'community' as such is an amalgamation of different groups and individuals who share some similarities, but also differ significantly in their motivations, values and how-I-came-to-hacking stories—and, importantly, not every activity hackers engage in is intrinsically illegal (in fact, most are perfectly within legal bounds). This difference in what Coleman terms hacker 'genealogies' has led to the emergence of different genres of hacking, from open-source software culture to unauthorised hacking for profit to state-sponsored hacking and cyber warfare.[10] The debates about the ethics of hacking have been ongoing since its early days, but due to its rhizomatic nature, they remain ambiguous and open to interpretation and contestation.[11,12]

One such debate revolves around the legitimacy of hackers' political participation. Though hacking has been stereotyped as destructive and inherently malicious, there are those who argue it can be a legitimate form of activism. Brian Still argues that 'hacktivism' as a form of disobedience or disruption is increasingly used to challenge the authority of oppressive regimes, and Molly Sauter cites the examples of DDoS attacks perpetrated by Anonymous, a loose collective of hackers and other internet users, against Amazon and PayPal after these companies attempted to block the activities of whistle-blower website Wikileaks in 2010.[13,14] Whether aimed at nation states or corporate entities, the grass-roots, bottom-up nature of these efforts emerges as a key condition for recognition of their activist claims, often coupled with public messaging or manifesto-style communiqués posted online to explain the significance of the hack.

On the other side of the spectrum is state-sponsored hacking, which experts often place in the same category as industrial espionage, as the targets include not just communication networks and data repositories, but also financial systems, energy grids and other crucial infrastructure.[15] Some groups have been directly implicated as nation state actors (among them China's military-based Unit 61398, Bashar al-Assad-friendly Syrian

[8]Gabriella Coleman, 'The anthropology of hackers', *The Atlantic*, 21 September 2010, available at: http://www.theatlantic.com/technology/archive/2010/09/the-anthropology-of-hackers/63308/ (6 September 2017).

[9]Jeffrey S. Juris, *Networking futures: the movements against corporate globalization* (Durham and London, 2008), 96.

[10]Coleman, 'The anthropology of hackers'.

[11]Steven Levy, *Hackers: heroes of the computer revolution* (New York, 1st edn, 1984).

[12]The term 'rhizomatic' here is informed by the work of Gilles Deleuze and Félix Guattari who saw a 'rhizome'—a network of roots with no explicit centre—as an alternative to centralised systems.

[13]Brian Still, 'Hacking for a cause', *First Monday* 10 (9) (2016), available at: http://firstmonday.org/ojs/index.php/fm/article/view/1274/1194 (6 September 2017).

[14]Molly Sauter, *The coming swarm: DDOS actions, hacktivism, and civil disobedience on the internet* (New York and London, 2014).

[15]Bernard Everett, 'Optically transparent: the rise of industrial espionage and state-sponsored hacking', *Computer Fraud & Security* 10 (2013), 13–16.

Electronic Army, as well as groups affiliated with governments in Israel and Iran) or found to have direct ties to non-state groups, such as Hamas' Gaza Cybergang, Hezbollah-affiliated Qadmon or IS-supporting hackers.[16] But more often than not, finding explicit evidence of a state running hacker groups proves difficult. Particularly in recent years, security experts and intelligence officials have pointed to several groups and individuals, including APT (Advanced Persistent Threat) 28, Fancy Bear and Guccifer 2.0 as having ties to the Russian foreign intelligence service and other state agencies. These groups have been implicated in the disruption of the 2016 US election through interfering in American voter registration systems and leaking the emails from the hacked Democratic National Committee (DNC) servers. But unlike the case of China's fairly organised government hackers, there is little tangible evidence to connect the DNC hackers to Russia's state security apparatus.[17] At least in part, this is because these hacking teams do not operate as official structures within the hierarchy of state or military bureaucracy, but instead work in loose groups under assumed identities, resorting to opportunistic manoeuvres and borrowing software and malware solutions from other sources instead of running a sterile, secretive in-house development lab.

Having only a tenuous connection to the state and those in power offers hackers another opportunity: that of presenting themselves as independent actors or free agents, and thus, of having the potential to shape public opinion with the work they do beyond official state propaganda. As Alexander Klimburg notes, a modern state's cyber power (or really, its power overall) requires coordinating operational and policy efforts within government structures, within international alliances and with non-state actors, including industry experts and civil society.[18] But posing as non-state actors, regardless of the level of their connection to state bodies, leaves hacker collectives with a certain amount of discursive freedom to frame their activities and narratives as 'grass-roots activism', potentially inviting more sympathy or even greater trust from the public. This is why it is especially important to be attentive to the self-presentation work hacker groups do in public, as well as to their more direct and clandestine efforts to disrupt infrastructure, bring down websites and leak information from hacked email servers.

Identity performance, spectacle and online discourse

Social media today provide important spaces for public and private identity performances and are routinely used by various actors to create and maintain presences, as well as shape public opinion about themselves. Digital platforms help construct all kinds of selves for individuals and communities: Manuel Castells distinguishes between legitimising identities, used by dominant actors such as governments to extend and rationalise their hegemonic dominance in societies; resistance identities, employed by counter-publics vying to overthrow the dominant status quo and present alternative ideas; and project identities, built by social actors who seek to redefine their position in society and thereby transform

[16]OWL Cybersecurity, 'A survey of nation sponsored hackers', blog post, 30 April 2017, available at: https://www.owlcyber.com/blog/2017/2/23/nation-state-sponsored-hackers (6 September 2017).

[17]Andrew E. Kramer and Andrew Higgins, 'In Ukraine, a malware expert who could blow the whistle on Russian hacking', *New York Times*, 16 August 2017, available at: https://www.nytimes.com/2017/08/16/world/europe/russia-ukraine-malware-hacking-witness.html (6 September 2017).

[18]Alexander Klimburg, 'Mobilising cyber power', *Survival* 53 (1) (2011), 41–60: 43.

the overall social structure or some layer thereof.[19] This last form of identity construction emerges as key for hacker collectives in the context of this study, as these hackers seek to transform the public's image of them as a community and to reconfigure their role within the political and social discourse. To do this, they supplement their more habitual digital activity with increasingly active participation in the discursive networks underpinned by social media platforms.

The performative, public nature of hackers' online discursive work seems to represent the *front stage* where the actors manage the public's impressions and articulate particular elements of their identity. According to Erving Goffman, the front stage is in a dialectic relationship with a *backstage*, a more secretive space where the authentic, secret self resides.[20] For hacking communities (and individuals), the backstage is represented by their direct action, most of which occurs online and is generally kept under wraps. Backstage activities may include hacking government and media websites; DDoS attacks on state systems, energy grids, transport networks, banking systems; malware distribution and spear-phishing attacks via email; and leaks of stolen information such as email content, contacts, financial records, sensitive data or other personal information (a form of exposing known as doxing). These actions are the essential work of hackers, but they gain meaning only when placed in the context of motivations and reasoning for the act itself. This is where front-stage performance becomes important. Still draws a comparison between traditional hacker community websites, usually fairly closed communities where hackers post about their exploits, and the more outward-directed online manifestos and declarations of activist hackers that allow them to share ideas and profess support for particular causes, thereby explaining their actions.[21] Creating a social media presence allows hackers to further expand the front stage (while preserving the backstage to some extent), by entering and participating in the existing political and social conversations in these networks and renegotiating their identities in terms of power and access to the public eye. Inserting themselves into the public agenda in this way also allows the hackers to counter existing mainstream media narratives about themselves, which have heretofore overwhelmingly equated hackers with criminals.[22] Such front-stage discursive action may include establishing and maintaining social media accounts and websites; reporting on hacker activity and 'successes'; producing PR and publicity materials such as press-releases and manifestos; and networking with other actors. But as hackers enter the 'politics writ large' arena, they can also be observed joining in political debates and throwing their weight behind particular causes, parties and individuals. Especially in conflicts and crises, this discursive work can also take on a flavour of 'us vs them', expanding the identity performance and constructing it in opposition to a less legitimate 'other'.

As part of a hybridised identity performance, the discursive practices of hackers become just as important as their actual (mostly covert) work of hacking, if not more so. In these networked spaces, their actions and their meaning are amplified and inscribed in existing political and social processes, generating additional debate around the hackers' activity and motivations. While this public

[19]Manuel Castells, *The power of identity. The information age: economy, society, and culture, Volume II* (Chichester, 2nd edn, 2011).

[20]Erving Goffman, *The presentation of self in everyday life* (London, 1978).

[21]Still, 'Hacking for a cause'.

[22]Molly Sauter, 'Kevin Mitnick, the *New York Times*, and the media's conception of the hacker', in Jeremy Hunsinger and Andrew Schrock (eds), *Making our world: the hacker and maker movements in context* (New York, forthcoming). Available at: https://ssrn.com/abstract=2943042 (6 September 2017).

presence bears certain risks for the traditionally private members of the hacker community, it also offers opportunities. Coleman notes that despite their habitual secrecy, there has historically been a certain affinity for spectacle among hackers (stemming from their reactions to surveillance and their entanglement with phreaking and hoaxer cultures, and later, the culture of trolling).[23] The spectacular nature of social media discourse is also a way for hackers to make their clandestine activity more readily understandable in the context of a political moment, a crisis or a conflict—'to dramatise the unseen and expose associations elusive to the eye'.[24] Social media networks allow hackers to add the tactics of spectacle to their political arsenal in the service of whatever cause or ideological project they're supporting, be it pro-state, pro-terrorist group, pro-activist group, anti-establishment, anti-corporate or anti-government. By engaging in this kind of spectacular public discourse, hackers are able to articulate their imagined identity in political, moral and affective terms. Examining their online utterances and social media practices can thus prove fruitful in understanding how the hackers' constructed identity fits into the broader political and ideological context.

METHODOLOGY AND RESEARCH DESIGN

Online ethnography

Understanding the online discursive practices of a particular user group (hackers) on social media is best achieved through online ethnography—a non-reactive approach to observation by a passive observer.[25] Such an approach, also known as digital or virtual ethnography, allows us to unobtrusively observe the social media activity and the content (discourse) it generates over a period of time and to collect extant data without directly engaging with the subjects (although participatory ethnographies are also possible).[26] Observing how technology is used by people—in this case, to construct identities and generate or enter existing discourses—is a key element of digital ethnography, with the researcher's field being the networked space of connections and communication exchanges rather than a geographic location of a material site.

Twitter as an ethnographic space is problematic since it is a large, public site, and that makes it difficult to draw the boundaries of enquiry.[27] It becomes an even more complex task when we acknowledge that Twitter is just one of many online platforms and spaces that hacker communities inhabit. In this case, a network field site approach suggested by Jenna Burrell seems more productive: it reframes a particular platform as a single part of a 'network composed of fixed and moving points including spaces, people, and objects'.[28] Twitter, then, is perceived as one of many network nodes used by our community of interest, including other social media platforms, other online or offline locations, and content. Online ethnography on a particular network field site can be further

[23]Gabriella Coleman, 'Phreaks, hackers, and trolls: the politics of transgression and spectacle', in Michael Mandiberg (ed.), *The social media reader* (New York and London, 2012), 99–119: 102.

[24]Stephen Duncombe, *Dream: re-imagining progressive politics in an age of fantasy* (New York, 2007), 156–57.

[25]Janet Salmonds, *Doing qualitative research online* (Thousand Oaks, 2015), 119.

[26]Christine Hine, *Virtual ethnography* (Thousand Oaks, 2000).

[27]Alice E. Marwick, 'Ethnographic and qualitative research on Twitter', in Katrin Weller *et al.* (eds), *Twitter and society* (New York, 2014), 109–22.

[28]Jenna Burrell, 'The field site as a network: a strategy for locating ethnographic research', *Field Methods* 21 (2) (2009), 181–99: 189.

delimited by focusing on a specific set of accounts or keywords, informed by prior research or existing context.

Focusing on Twitter as a platform of choice for this study has its limitations, as interactions between groups and discursive connections may be transient and difficult to pin down. But since this study is mostly concerned with how communities construct identities online, and less with how they interact with one another, the benefits of Twitter as a coherent networked environment that offers multiple affordances for self-presentation and identity performance outweigh the limitations.

For the purposes of this enquiry, unstructured ethnographic observation was conducted on a number of designated Twitter accounts of key hacker groups that identify as pro-Russian or pro-Ukrainian. The sampling choice was informed by the researcher's prior knowledge of the overall context of the Russia-Ukraine conflict and the platform environment and affordances. Twitter observations were supplemented by a review of complementary online materials linked to or embedded by the group accounts in their tweets for comprehensive analysis and triangulation.

The accounts on which observation was conducted and whose content was analysed include two most influential and active hacker collectives in the Ukraine-Russia conflict: 1) CyberBerkut (https://twitter.com/cyberberkut2), a pro-Russian hacker group; 2) Ukrainian Cyber Alliance, a pro-Ukrainian hacker collective comprised of three key subgroups, each with their own account: Falcons Flame (https://twitter.com/16ff255/), Trinity (https://twitter.com/opstrinity) and RUH8 (https://twitter.com/_ruhate_). These publicly accessible accounts were observed and examined in their entirety to collect the practices and the discourse in the posts of both collectives during the conflict period (2014–17). Each account was observed in the desktop browser iteration of Twitter throughout 2016 and 2017, to garner general information such as account bio and tweeting practices. Additionally, tweets were collected using Sifter, an online tool that grants access to historical Twitter data. Extant data collection yielded hundreds of Twitter posts (1,671 in total, as of early August 2017) and additional linked content from related platforms, including websites, blogs, Facebook pages, videos and multimedia, providing a rich framework from which insights were drawn through further analysis and comparisons.

Analysing online discourse and practices

As a social media platform with particular affordances, Twitter imposes its own vernacular on users, offering them a set of formats and features that become part of the networked communication practices and can define how certain interactions or performances occur. Twitter posts as online discourse are condensed, chronological, discrete, shareable, embeddable and networked. All of these characteristics influence the strategies individuals and communities choose in order to perform their identities and participate in certain broader political and ideological discourses. Beyond the actual content of Twitter posts, features such as retweets and mentions emerge as discursive markers of connection and engagement with larger frameworks of meaning and action, while the use of hashtags allows us to theorise about Twitter discourse as 'searchable talk', a set of overlapping discursive spaces where attention, outrage or empathy can be focused.[29]

[29]Hongqiang Zhu, 'Searchable talk as discourse practice on the internet: the case of "#bindersfullofwomen"', *Discourse, Context & Media* 12 (2016), 87–98.

Moreover, the inclusion of links to external online platforms and embedded multimedia content helps to create a complex, multi-layered infrastructure of online discourse that is best understood as a practice and not just as static content posted at certain intervals and then preserved as an archive.

There are a number of approaches to analysing social media content as speech. Both textual (or content) analysis and discourse analysis yield important insights, allowing for finding meaning and interpreting the patterns in a corpus of data on various levels: descriptive, interpretive and explanatory. For instance, in her study of networked identity performance on Twitter, Zizi Papacharissi used content analysis to determine descriptive features of Twitter posts such as trending hashtags and @replies, as well as strategies for performativity.[30] Papacharissi then applied discourse analysis to the same sample of tweets to arrive at a deeper interpretation of the performative practices and the vernacular of the 'polysemic' networked self.[31] As a means of revealing 'how texts are constructed', discourse analysis is essential when seeking to understand the broader ideological structures and entanglements of power on which the discourse rests.[32] In the present case of hackers engaging in a public performance of their identities online, such linguistic and textual expressions can indeed be understood as social practice, where what is being said is as important as how and why these discourses appear in the public sphere. By applying the three-stage model of discourse analysis (encompassing the descriptive, the interpretive and the explanatory stages) to both the contents of the Twitter posts and the platform features that wrap around them, it is possible to reveal the hierarchies of power and dominant ideologies underpinning the conflict the hacker groups are party to and to illuminate the processes of legitimation and delegitimation of particular ideas or actors in this context.[33,34]

The Twitter accounts selected for this study were analysed using content analysis and discourse analysis applied to the accounts as a whole, including account data and metadata, the corpus of tweets collected from each account and the platform-specific features and practices used by the account holders. All of these elements were subjected to the process of horizontalisation, where every statement and act was taken to be of equal value before assigning categories and eliciting meanings.[35] These were coded to elicit key themes and patterns in the discourse around hacker activities and statements in the context of the Ukraine-Russia conflict. Such a contextualised analysis allows for a rich, multi-layered canvas of descriptive findings, supplemented by interpretive and explanatory analysis of the spectacular public performance and self-presentation strategies of pro-Russian and pro-Ukrainian hacker groups online.

DISCURSIVE PRACTICES OF HACKER COLLECTIVES IN THE UKRAINE-RUSSIA CONFLICT

The grass-roots hacker collectives operating on both sides of the Ukraine-Russia conflict have enjoyed significant public attention thanks to initial (and ongoing)

[30]Zizi Papacharissi, 'Without you, I'm nothing: performances of the self on Twitter', *International Journal of Communication* 6 (2012), 1989–2006.

[31]Papacharissi, 'Without you, I'm nothing', 1993.

[32]Norman Fairclough, *Language and power* (Harlow, 2nd edn, 2011), 89.

[33]Norman Fairclough, *Critical discourse analysis: the critical study of language* (New York and Oxford, 2nd edn, 2013).

[34]Theo Van Leeuwen, 'Legitimation in discourse and communication', *Discourse & Communication* 1 (1) (2007), 91–112.

[35]Clark Moustakas, *Phenomenological research methods* (Thousand Oaks, 1994).

media coverage of their activities, and that attention has only grown as they have cultivated their social media profiles during the time of the conflict. Though individuals behind these groups have reported extensively on their exploits and many of the specific attacks have been documented, little is known about the actors themselves.[36] Neither CyberBerkut nor Ukrainian Cyber Alliance are explicitly state-run, but their practices reportedly enjoy tenuous approval from government officials.[37] The hacktivist groups have at various times been rumoured to pass information to law enforcement and state security services as well as collaborating with other activist groups.[38] On both sides, the hackers do not always share the official government point of view on the particulars of the conflict, but choose to publicly ally themselves with either Ukraine or Russia as a country and a party to the conflict.

CyberBerkut is a pro-Russian hacker group, comprised of at least four individuals, which has interfered in a number of Ukrainian government and military networks and has leaked official documents, aiming to embarrass and undermine the Ukrainian side. Security researchers claim CyberBerkut are likely Ukrainians or Russians with links to Ukraine, most probably supporters of the country's pro-Russian former president Viktor Yanukovych, who was ousted in 2014 in the wake of the Euromaidan protest.[39] The pro-Russian hackers first garnered attention with a series of DDoS (distributed denial of service) attacks on a number of Western and Ukrainian institutions, including NATO and the Ukrainian Ministry of Defence. They also claim responsibility for the massive hacking attack on the servers of Ukraine's Central Election Commission in May 2014, when they attempted to interfere with the software used in announcing the results of a Presidential Election (the hack did not sway the outcome of the election). [40] Some reports allege that CyberBerkut might be one of the aliases for the infamous Russian hacker group Fancy Bear, implicated in the hack of the DNC and tied to Russian interference in the US elections. Most recently, in the summer of 2017, CyberBerkut released a cache of stolen emails alleging that Hillary Clinton had colluded with Ukraine during the US election.[41] Most of the stolen data that CyberBerkut hackers obtain is released through their website or through Pastebin, an info dump website often frequented by hackers, and then promoted on their various social media channels.

Ukrainian Cyber Alliance is a much looser collective of several different groups and individuals (anywhere between 10 and 15 people overall) who joined forces to battle their pro-Russian counterparts and wreak havoc on the Russian state and military officials. Although its various members have been operating since the spring of 2014, the Alliance was formed in the spring of 2016, and is comprised of the Falcons Flame and Trinity groups and a lone hacker called RUH8, with occasional participation from certain members of the CyberHunta,

[36]Tim Maurer and Scott Janz, 'The Russia-Ukraine conflict: cyber and information warfare in a regional context', *The International Relations and Security Network* 17 (2014).

[37]Jeff Stone, 'Meet CyberBerkut, the pro-Russian hackers waging anonymous-style cyberwarfare against Ukraine', *International Business Times*, 17 December 2015, available at: http://www.ibtimes.com/meet-cyberberkut-pro-russian-hackers-waging-anonymous-style-cyberwarfare-against-2228902 (6 September 2017).

[38]Christopher Miller, 'Inside the Ukrainian "hacktivist" network cyberbattling the Kremlin', *Radio Free Europe/Radio Liberty*, 2 November 2016, available at: https://www.rferl.org/a/ukraine-hacktivist-network-cyberwar-on-kremlin/28091216.html (6 September 2017).

[39]Stone, 'Meet CyberBerkut'.

[40]Greenberg, 'How an entire nation became Russia's test lab for cyberwar'.

[41]Kramer and Higgins, 'In Ukraine, a malware expert who could blow the whistle on Russian hacking'.

yet another pro-Ukrainian hacktivist group.[42] Ukrainian Cyber Alliance hackers state their mission is to 'expose Kremlin meddling in Ukraine', and they've also openly admitted that CyberBerkut is their Russian/pro-Russian counterpart and is therefore also one of their targets. The Ukrainian hackers' notable achievements in the conflict include hundreds of hacked and exposed email inboxes and social media profiles of pro-Russian separatists and their 'Russian curators'. Their most recent star moment came in October 2016 with the massive leak of more than a gigabyte of e-mails and text documents from the allegedly hacked inbox of one of Russian President Putin's key aides, Vladislav Surkov (who also happens to be the Russian government's point person for international negotiations on the ongoing conflict in eastern Ukraine).[43] The Alliance has its own Facebook page, but no Twitter account. Instead, each of its constituent parts—Falcons Flame, Trinity and RUH8—runs their own Twitter feed as part of their joint social media presence.

Key textual and discursive practices

Analysis of 1,671 Twitter posts from the CyberBerkut account and the three Ukrainian Cyber Alliance accounts yields a wealth of observations about how the hacker collectives use their social media presence to do self-presentation work and construct their identities in particular ways. There are several layers of data in the posts that lend themselves to various depths of meaning and interpretation. On a superficial level, there is the content of the posts themselves, including the words or sentences, embedded images or videos, the use of external links, and so on. On the same level are the affordances of Twitter as a platform used in each post, such as retweets, mentions or hashtags. All of these reveal *what* the hacker groups talk about or *what* they do in this public space and, to some extent, *how* they produce meaning from their discourse and practices. Examining the content and the use of platform affordances generates descriptive findings that are nonetheless illuminating and that feed into a deeper analysis of the hackers' discursive practices.

For both the pro-Russian CyberBerkut hackers and the Ukrainian Cyber Alliance, the majority of Twitter posts reported on their achievements and successes. CyberBerkut, for instance, boasted about hacking the PC of Ukraine's chief military prosecutor and about taking down several 'fascist' (nationalist) Ukrainian websites, while the allied Ukrainian hackers reported taking down pro-Russian news websites and doxing the Russian military who fought alongside separatist forces in Ukraine. While CyberBerkut's reports were mostly declarative or linked to their website, the Ukrainian Cyber Alliance also linked to mainstream media coverage of their successes, along with links to their own webpages. Both groups added screen captures of key hacks and leaked material as additional proof of their work. On a more conceptual level, the hackers also occasionally shared links to manifestos or mission statements justifying their work and, in the case of Ukrainian Cyber Alliance's RUH8 account, even linked to a Facebook post with philosophical musings about the role of hacking in propaganda and persuasion efforts during conflicts. These contributed to the construction of the public hacker identity on Twitter.

[42]Miller, 'Inside the Ukrainian "hacktivist" network cyberbattling the Kremlin'.

[43]Shaun Walker, 'Kremlin puppet master's leaked emails are price of return to political frontline', *Guardian*, 26 October 2016, available at: https://www.theguardian.com/world/2016/oct/26/kremlin-puppet-masters-leaked-emails-vladislav-surkov-east-ukraine (6 September 2017).

Beyond directly reporting on their work, both sets of hacktivists frequently named specific individuals and organisations involved in the conflict, including activists, government officials, military personnel, journalists and others. These names often featured as the victims of hacking activity and were often 'exposed' as key operatives on the opposing side when their personal email inboxes or webpages were hacked. In several instances, both sides also mentioned their hacker 'nemesis' in the context of the conflict, mostly to jeer at their incompetence (Ukrainian Cyber Alliance at one point posted a scan of a passport which it claimed belonged to one of the members of CyberBerkut). The pro-Russian group used Twitter to recruit likeminded volunteers to join their team.

Both the pro-Russian and the pro-Ukrainian hackers actively attempted to contextualise their discourse and work in the broader conflict situation by offering additional detail on the events. In their tweets, CyberBerkut and Ukrainian Cyber Alliance established who were the key actors and parties to the conflict, as well as offering commentary on the political and military situation. CyberBerkut often tweeted about Ukraine and Western states, as well as pro-Russian separatist rebels in the conflict, but barely mentioned direct Russian involvement, presenting the Kremlin as an innocent bystander. Ukrainian Cyber Alliance gave Russia the centre stage, frequently mentioning Russian officials and military figures, as well as drawing clear connections between Russian forces and the separatist militias in eastern Ukraine. Both collectives also exposed various foreign and international actors allegedly participating in the conflict behind the scenes: pro-Ukrainian hackers claimed to have evidence of foreign fighters joining pro-Russian separatist ranks, while CyberBerkut accused US think-tanks of lobbying for lethal weapons for the Ukrainian side and even of fomenting a 'colour revolution' in Russia akin to the Ukrainian Euromaidan protest.

In terms of using the features afforded by Twitter as a platform, there were many similarities between the two groups. Both of them used links quite heavily, linking to their other social media pages and websites, but Ukrainian Cyber Alliance linked to other media and activist ally websites, while CyberBerkut remained fairly insular. Because the Ukrainian hackers operated several Twitter accounts, they also retweeted each other and their allies quite a lot—in fact, retweets make up the bulk of their Twitter activity. Hashtags were used pervasively by both collectives to connect their activity to existing discourses, such as #Ukraine, #Russia, #ATO (anti-terrorist operation, the term official Ukraine uses for the conflict), or to frame the conflict in a specific light (Ukrainian hackers were quite fond of the hashtags #TheHague and #HagueCourt, referring to Russia's military activity in Ukraine as crimes that should be investigated in the International Criminal Court). Hashtags promoting the collectives themselves—#CyberBerkut and #UCA, respectively—were used frequently, especially in tweets containing reports of successful operations. Textual content was augmented with embedded images and videos: though CyberBerkut's early tweets were mostly text-only, they quickly caught up with Ukrainian Cyber Alliance, whose accounts actively employed multimedia and even branded content with their own logo.

The initial findings of this analysis don't just reveal the content and feature choices of the hacker groups on Twitter, but can also be interpreted as markers of certain discursive practices that these groups engaged in. Applying this interpretivist paradigm informs our understanding beyond what subjects and themes were discussed and extends it to asking *how* the hacker collectives chose to produce these meanings and share them. This interpretive stage can further

illuminate the performative work and identity construction that hackers do on social media.

The hackers' most visible discursive practice—framing their hacking activity in particular ways on a public platform—is evident from a prevalence of discourse about their own actions. First of all, the hacker groups are able to present themselves as more public actors, combining reports on their clandestine work with more outwardly oriented messages such as manifestos, philosophical musings and political demands. This is a potent example of how social media can enable a convergence of the backstage and the front-stage performances, collapsing public and private contexts into an experience that is at once spectacular and intimate.[44] Second of all, both CyberBerkut and Ukrainian Cyber Alliance explicitly frame themselves as grass-roots actors, distancing themselves from the state and embracing terms such as 'partisan' or 'guerrilla'. This also serves to promote a collective identity that is more authentic, personalised and may drive the social media audience to be more sympathetic to the hackers' agenda.

Another discursive strategy the hacker groups employ is embedding their work and their performance in the broader political and social context of the conflict between Russia and Ukraine. By connecting their activities and opinions to other events and trends within the ongoing struggle, and by placing themselves alongside other actors such as government officials, military structures, international bodies, media outlets and activist groups, the hackers at once give their actions more meaning and rationalise themselves as legitimate actors on a par with every other participant in the conflict. This contextual embedding not only gives them legitimacy, but normalises their hacking as a routine part of conflict, a daily element of hybrid warfare and a form of political expression.

Finally, the public performances of pro-Russian and pro-Ukrainian hacker groups not only become a seemingly natural part of the grass-roots activism and a routine element of the hybrid war, but allow the hackers to refashion their own identities, to impose their interpretations on the identities of their foes and, ultimately, to reshape the meaning of the political situation as a whole. By discussing their motivations and values, by sharing moral judgements about their opponents and by labelling various actors and phenomena—often with highly charged terms such as 'fascist', 'anti-fascist', 'genocide', 'junta', 'terrorist'—each group draws its own map of the conflict, defining the parties engaged in it (who is fighting) as well as the relative moral stances of each (who is the bad guy). Such moral evaluation and labelling isn't limited to the hackers on the opposing side, but stretches to encompass the opposing side as a whole.[45] Because discursively each hacker group has already embedded itself in the broader networked context of the conflict and is now performing as part of a 'people', whether of pro-Ukrainian or pro-Russian persuasion, it is able to interpret the value of their work in undermining particular actors in the conflict as serving a greater purpose. As they redefine the very meaning and the causes of the conflict itself through their spectacular performance online, the hackers are thus able to discursively legitimise themselves and their allies and at once to delegitimise their opponents, the work they do and the values—and people—they stand for or represent.

[44]Papacharissi, 'Without you, I'm nothing', 1990.
[45]Van Leeuwen, 'Legitimation in discourse and communication'.

CONSTRUCTING THE 'PATRIOTIC HACKER' DISCOURSE

The findings from the descriptive analysis of the text and the features of hacker groups' Twitter communications and the interpretive analysis of their discursive practices combine to inform the third, explanatory stage of discourse analysis. Here, the analysis seeks to explain how the discourse feeds into and reflects the 'sociocultural practice' surrounding the text.[46] By considering the ideological and social structures in which the text is produced and consumed, we can speculate about how the rules and norms of these structures affect how the text is understood and how sociopolitical meaning is created through discourse. Van Dijk outlines a similar 'social-cognitive' model to explain the relationship between the textual practice and the sociocultural practice, mediated at the discursive level.[47] The aim of this multi-layered approach to analysis is to understand the links between 'texts, discourse practices, and sociocultural practices' in identifying how hacker groups construct their identities on social media as part of a particular sociocultural environment and how their discursive performances contribute to shaping the broader discourse around the conflict.[48]

In the case of the ongoing confrontation between Russia and Ukraine, social media have been used extensively to promote conflicting (and often false) narratives of the situation and to impose or subvert certain values, moral tone and ideological colouring of particular aspects of the conflict.[49,50] Many of these attempts at framing and manipulation of public opinion stemmed from strategic state narratives and ideology, but were buttressed (or in some cases, subverted) by grass-roots discursive activity on social network platforms. Recent research has shown that both Russia and Ukraine take propagation and dissemination of strategic narratives about the conflict quite seriously and consider these battles in the digital and communications domains a part of the ongoing 'information war' that is as crucial as the military, economic and other aspects of the confrontation.[51] Especially in the networked social media sphere, those who craft state communications and propaganda strategy in Russia (and, increasingly, in Ukraine) are well aware of its potential for 'mobilising its supporters, demonising its enemy, demoralising its enemy's government and armed forces, and legitimising its own actions'.[52] Apart from attempts to control and police social media discourse through censorship of particular topics or resources and blocking key pages, a less ham-handed and more nuanced opportunity to manipulate discussions and opinions is presented by seemingly independent or grass-roots actors whose own discursive practices feed into and align with the strategic state narratives. From the above interpretive analysis, we have already seen that pro-Ukrainian and pro-Russian hacker collectives are actively working to embed

[46]Fairclough, *Critical discourse analysis*.

[47]Teun A. Van Dijk, 'Principles of critical discourse analysis', *Discourse & Society* 4 (2) (1993), 249–83.

[48]Norman Fairclough, *Media discourse* (London, 1995).

[49]Mykola Makhortykh and Yehor Lyebyedyev, '# SaveDonbassPeople: Twitter, propaganda, and conflict in Eastern Ukraine', *The Communication Review* 18 (4) (2015), 239–70.

[50]Anastasiia Bezverkha and Tetyana Lokot, '#Krymnash (#CrimeaIsOurs): the discursive (de) legitimation of the annexation of Crimea', presented at the 2016 Critical Studies Research Group Conference on Resistance (Brighton, 2016).

[51]Stephen Hutchings and Joanna Szostek, 'Dominant narratives in Russian political and media discourse during the Ukraine crisis', in Agnieszka Pikulicka-Wilczewska and Richard Sakwa (eds), *Ukraine and Russia: people, politics, propaganda and perspectives* (Bristol, 2015), 173–85.

[52]Elina Lange-Ionatamishvili, Sanda Svetoka and Kenneth Geers, 'Strategic communication and social media in the Russia Ukraine conflict', *Cyber War in perspective: Russian aggression against Ukraine* (Tallinn, 2015).

themselves in the broader political discourse around the conflict and to exert certain power on how the understanding of the conflict and the reasons behind it are being shaped. But how do their efforts align with the strategic narratives of Russia and Ukraine?

In some ways, the conflict initiated by Russia on Ukrainian soil with the annexation of Crimea in 2014, and later, with support of the separatist rebellions in eastern Ukraine, was the culmination of an ongoing renegotiation of collective identities of Russians and Ukrainians in light of the complex historical relationship between the two countries. Scholars note that Russia's public strategic narratives during the conflict, beyond grievances with Western meddling, have centred on the concept of 'Russian nationhood' and the idea of the 'Russian world', a grand nation-building effort that the Russian state has intensified under President Vladimir Putin.[53,54] This populist narrative emerged from an identity crisis in Russia in the wake of the Soviet collapse and attempts to reconcile the state's former imperial greatness and the USSR's status as a major global player with a world where the centres of power have shifted significantly during the last 30 years. In the context of the conflict, this narrative has found its shape in language that calls for rescuing Russian 'compatriots' and 'ethnic Russians' on hostile soil, designating 'national traitors' and defining 'traditional values'.[55]

At the same time, Ukraine has been reconfiguring its own collective identity, suspended for a time between close historical, cultural and economic ties with Russia and an emerging narrative of Ukraine as 'part of Europe'.[56] In a contest for greater agency that has been ongoing since Ukraine gained independence in 1991, the country has long struggled to form its own idea of 'a sovereign nation', and the idea of sovereignty only gained urgency with the start of the conflict in 2014. Because of the complexities of its close relationship with Russia, exemplified by ethnic, lingual and familial interpenetration of the populations of the two countries, the proximity of Russian influence has been interpreted differently by the split identities co-existing within Ukraine: some saw it as a threat to Ukrainian nationhood, while others looked upon it more favourably as a continuation of a long-term cohabitation with mutual benefits. However, since 2014, the strategic narratives of the Ukrainian state have embraced notions of sovereign power, a stronger military, a unique cultural history and even nationalist ideals (heretofore problematic because of a tense history of nationalist Ukrainian organisations and criticism of existing far-right political factions), battling for greater agency in light of the Russian ambition to impose its own kind of 'nationhood' upon Ukrainians.

Though these warring strategic narratives are clearly at odds with each other, the hacker collectives operating within these discourses in the networked realm have managed to create a popular, and even populist, identity that rests on an essentially similar concept—that of patriotism. Through such identity performance, they are able to inscribe their activity into the broader narrative of the struggle in a manner that clearly indicates their alignment with a particular party to the conflict and explicates their motivations for engaging in the hacking activities as part of the confrontation.

[53]Hutchings and Szostek, 'Dominant narratives in Russian political and media discourse during the Ukraine crisis'.

[54]Valentina Feklyunina, 'Soft power and identity: Russia, Ukraine and the "Russian world(s)"', *European Journal of International Relations* 22 (4) (2016), 773–96.

[55]Hutchings and Szostek, 'Dominant narratives in Russian political and media discourse during the Ukraine crisis'.

[56]Feklyunina, 'Soft power and identity'.

Public construction and self-presentation of patriotism among journalists, more traditional political activists and active citizens, including in the online spaces, has been investigated to some extent by researchers.[57] But if we accept that hacker activity, hackers' backstage disruptive work, can be political and that through front-stage discursive practices these groups increasingly articulate their politics online, we can claim that there can exist a 'patriotic hacker' identity. While performing patriotism is highly context-dependent and clearly spectacular in nature, we can argue that it allows hackers to present themselves as a legitimate element of a greater strategic narrative in the conflict, and to discredit their opponents as unpatriotic traitors and rob them of agency by branding them 'the losing side'.

In their investigation of journalists' performances of patriotism online, Avshalom Ginosar and Igor Konovalov identify three main discursive indicators of patriotism: the adoption of governmental framing, expressions of solidarity and 'ignoring the enemy's narratives and positions'.[58] Because we've identified that hacker groups in the Russia-Ukraine conflict engage in public online discourse around current events in the conflict, including discourse about their own role in the conflict, we can speculate that these indicators might also apply. There are, however, some interesting distinctions that relate to how hackers construct their own identity within the context of the confrontation, especially in relation to state actors. While their interpretation of the causes and dynamics of the conflict may at times coincide with that of the government (Russian or Ukrainian), the hacker groups do not always adopt the state frame, can afford to disagree with it and actively attempt to distance themselves from the government by identifying themselves as independent, grass-roots actors working on their own initiative. Patriotism, for them, emerges as a viable motivation for such independent action. In fact, the solidarity they express in their online discourse, is not so much solidarity with the state or its officials, but solidarity with the nation or the people: ethnic Russians, Russian speakers and pro-Russian separatists on one side; and Ukrainian citizens, volunteer or regular military Ukrainian troops, and Ukrainian activists on the other side. Finally, instead of ignoring the narrative of the opposing side, the hacker groups seek to actively discredit and delegitimise them by exposing their corrupt nature and less effective hacking and cyber warfare tactics and by labelling them as traitors in contrast to their own patriotic identity.

The 'patriotic hacker' performance allows the groups to construct their patriotism as part of a larger strategic narrative within the conflict and to secure its appeal to popular sentiment shaped by these narratives, be it the Russian idea of 'nationhood' and the 'Russian world', or the Ukrainian idea of 'sovereign agency' and 'national pride'. Thus authorised, the hacker groups further legitimise their identity and practices through moral evaluation as they use their spectacular social media performance to establish themselves and their chosen side as a greater 'moral authority' in the conflict, compared to their foes.[59]

Being 'patriotic' as a public identity for hackers in the conflict emerges as a valid political alternative to neutrality, objectivity or lack of alliances, markedly different

[57]Zhou Kui, 'The misplaced "apology": rethinking China's Internet patriotism', *positions: asia critique* 23 (1) (2015), 49–58; Nigel James, 'Militias, the patriot movement, and the internet: the ideology of conspiracism', *The Sociological Review* 48 (S2) (2000), 63–92; Avshalom Ginosar and Igor Konovalov, 'Patriotism on the internet: journalists' behavior and user comments', *Media, War & Conflict* 8 (3) (2015), 368–83.

[58]Ginosar and Konovalov, 'Patriotism on the internet', 371.

[59]Van Leeuwen, 'Legitimation in discourse and communication'.

from the meritocratic, pro-digital freedom stance of hacker collectives in the past. Patriotism is offered as a viable discursive stance so that the hackers feel validated in aligning themselves with a particular party in the conflict, expressing solidarity with a nation and its people. The 'patriotic hacker' identity also implies a certain sense of righteousness when engaging in activity that government and law enforcement officials may not be able to publicly engage in themselves, but may condone when it is done by independent third parties in the name of political gain.

Patriotism, therefore, emerges as a convenient identity marker that validates hackers as public actors and at once offers convincing and fairly transparent motivations for their engagement in the conflict. But because the pro-Russian CyberBerkut and the pro-Ukrainian Ukrainian Cyber Alliance both frame their patriotism by embedding it into markedly different strategic narratives of their side's involvement in the conflict, the notion of 'patriotic hacking' remains contested and open to various interpretations. In this complex context of overlapping narratives and performative identities, patriotism might even be considered a floating signifier, as conceptualised by Ernesto Laclau and Chantal Mouffe: a societal concept or term open to constant contestation and re-articulation via very different ideological frames.[60] Because the signifier is open to interpretation, it may have different meaning for different groups or individuals, represent different signifieds, and, ultimately, mean whatever its constructors want it to mean.[61] In the case of the 'patriotic hacker' construct, the two opposing sides seek to impose their own ideological frame upon the concept of patriotism and to fix its meaning—a task that ultimately proves futile, as its ambiguity is key to the continuing discursive struggle.

CONCLUSIONS AND DISCUSSION

Area studies research into the role of digital media in post-Soviet states shows that social media can be a space for self-identification and democratic voices, but also a tool for autocratic stability, especially in countries with totalitarian or neo-authoritarian regimes.[62,63] Investigating how specific state and civic actors navigate this hybrid discursive space is therefore valuable, as it informs our understanding of the changing configurations of language and power in the modern era when digital technology and media increasingly permeate political and social life.

This study focused on the self-presentation and online discursive practices of grass-roots hacker collectives on both sides of the Ukraine-Russia conflict to reveal the key ways in which they construct and communicate their identity within the broader context of the confrontation. Employing textual and discourse analysis to examine the hacker groups' presence and activity on Twitter, the research found that these collectives actively make specific choices about the content they post or link to on Twitter and about the use of certain platform-specific features. This results in a set of specific discursive practices: first, the hackers are able to frame their hacking activity by presenting themselves as more public actors online and by discussing their activity as independent and explicitly grass-roots. They are also able to legitimise and normalise their hacking

[60]Ernesto Laclau and Chantal Mouffe, *Hegemony and socialist strategy: towards a radical democratic politics* (London 2001).

[61]Daniel Chandler, *Semiotics: the basics* (New York and Oxford, 3rd edn, 2017).

[62]Sarah Oates, *Revolution stalled: the political limits of the internet in the post-Soviet sphere* (New York, 2013).

[63]Seva Gunitsky, 'Corrupting the cyber-commons: social media as a tool of autocratic stability', *Perspectives on Politics* 13 (1) (2015), 42–54.

activity through embedding their work and their identity performance in the broader political and social context of the conflict between Russia and Ukraine. Finally, through discursive practice, the hacker collectives refashion their own identities, impose their interpretations on the identities of their opponents and influence the meaning of the political situation as a whole, further validating their role in the political turmoil surrounding the conflict.

The research also found that by collapsing their backstage activity with front-stage performance the pro-Russian and pro-Ukrainian hackers are able to embed themselves in the broader strategic narratives of the opposing sides of the conflict and to avail of these narratives in creating their discursive identity. This identity is refashioned through the concept of a 'patriotic hacker'—a floating signifier that allows each group to imbue the term with its own set of meanings and, while contested, becomes a convenient marker of popular appeal, moral value and belonging. Thus, both pro-Russian and pro-Ukrainian hacker groups use social media to enter the broader populist discourse around the conflict on Europe's edge, re-imagining the notions of patriotism, sovereignty and statehood. The analysis of public discursive practices and strategies on the pro-Russian side reveals it to be part of a larger populist push to pitch the Ukraine-Russia conflict as a clash of pro-Western, 'immoral' Ukrainian forces and the 'properly patriotic' Russian and pro-Russian forces defending Russian 'nationhood' and the 'Russian world', reasserting Russia's desire for a dominant geopolitical stance. On the Ukrainian side of the hacker discourse, the constructed patriotism emerges as a defence of self-reliance, sovereignty and 'national pride', helping portray Ukraine as an independent state opposing a Russia with unjustified imperial ambitions.

The inward-directed patriotic hacker identities and discourses that emerge from this research are perhaps echoes of a broader global turn towards populist rhetoric and nationalist sentiment sweeping across Europe and the Western world in reaction to various political, cultural and military threats. But on a smaller scale, this discursive work signifies a shift from hacktivism as work of disobedience and disruption to patriotic hacking as ideological work that is inextricably tied with mainstream politics and populist political rhetoric. Given the rising concern with cyber warfare it is important to further research how hackers (both grass-roots and state-sponsored ones) articulate the nature and value of their work in terms of the broader political discourse. Future research would do well to consider the complex dance these seemingly independent actors engage in with state actors and how their discursive relationships help preserve the hegemonic status quo of particular ideologies—or tear down hostile hegemonic regimes.

Another important reflection stemming from the study of discursive practices of hacker groups in the Russia-Ukraine conflict is that in the hybrid media system, online performance of patriotism emerges as an inextricable part of 'being patriotic'. In this case, hacker groups perform their patriotism as part of their public discursive identity, thereby legitimising their hacking activity and lending their patriotic identity additional weight by embedding themselves in the broader political context. With the proliferation of populist political discourses, especially in areas undergoing or prone to political, ethnic or religious conflict, it is worth examining in more detail the meanings various participants in the conflict ascribe to vague, yet highly charged concepts such as 'patriotism', 'nationalism', 'extremism' or 'terrorism', and understanding how these networked discourses resonate with existing strategic narratives of nation states or non-state actors and with popular opinion.