




PUTIN'S 'LITTLE GREY MEN': RUSSIA'S POLITICAL TECHNOLOGISTS AND THEIR METHODS



Security, Crime and Intelligence
Innovation Institute

Sefydliad Arloesedd Diogelwch,
Troseddu a Chudd-wybodaeth

September
2024



The research reported in this document was funded by UK Government.

EXECUTIVE SUMMARY

This report analyses the role and work of political technologists in Russia, and how they contribute to the design and delivery of the Kremlin's domestic and foreign policy. Although well established as a concept in Russian political culture, there has been a recent revival of interest in the art, craft and science of political technology. In the current geopolitical climate, a small number of technologists are acquiring significant status, reputation and riches as a result of their contributions to various state-directed influence operations at home and abroad.

The methodology of political technology involves a variety of techniques and tools, configured to deliver influence, persuasion and social control. Some of these are overt and very familiar to academics and researchers in the West, others are more covert, deceptive and manipulative. In detailing these methods, this report pays particular attention to where they are engaged in forms of digital influence engineering. The specific role of political technology in these processes appears to be: (1) researching social and political issues, events and communications platforms. For the purposes of target identification and selection, where induced information effects might articulate with broader strategic aims; and (2) the design of operational strategy that shapes and directs the actions of operators 'on the ground'.

To date, much recent Western analysis of Russia's influence and information operations has focused upon cataloguing and assessing their digital assets and impacts, and where possible, attributing activities to particular entities. There has also been significant accompanying commentary on how these operations contribute to the Kremlin's overarching geopolitical strategy and posture. Introducing political technology into this picture, as a kind of middle tier involved in translating strategic policy into defined campaigns and interventions deliverable by tasked operatives, both enriches and alters our understanding. Notably, it shifts analytic attention 'upstream' from where it has typically been directed, affording a more 'strategic' perspective.

This approach helps to connect state-backed information manipulation activities and deceptive digital communications to wider efforts of espionage and political, economic and cultural subversion that are the focus of Russia's long-established 'active measures' doctrine. The value of this more upstream focus is that it is better able to detect interactions between information operations and disinformation campaigns, and other modes of covert influence, deception and persuasion.

The four headline findings of this research are:

1. Open-source research suggests there are over 500 political technologists currently working within Russia. They perform a variety of roles with some more directly connected with state and intelligence agencies. Evidence has identified political technologists operating in Russia, Ukraine, several European nations, Africa and Latin America. This confirms how significant these figures are to the Kremlin's global strategy.
2. Political technologists appear to have a key role in drawing up strategic 'country plans' for the Kremlin. The aim of these plans can range from seeking to extend and expand political and popular 'soft power' support for Russia and its geopolitical objectives, through to destabilisation and subversion.
 - Evidence is presented of a Russian plan for the Presidential election in the US in 2024. A 'workable agenda' is identified around exploiting the societal 'wedge issues' of: immigration; nationalism and popular sovereignty; identity politics and culture wars. The likely intention is to take advantage of societal and political tensions surrounding these problems by using disinformation campaigns and information manipulation.
 - Elements of possible plans for Germany, Poland and Serbia are also reported from the same source. Comparing these plans, it is possible to identify patterns in terms of how they are conceived and constructed.
3. A detailed account of the work of the specialist political technology organisation the Social Design Agency (SDA) is provided. It describes some of the operators responsible for: the increasingly high-profile Doppelgänger operation; working closely with the associated media outlet 'Reliable Recent News'; and generating other websites 'domain spoofing' legitimate global media outlets.
 - Doppelgänger also uses very large numbers of batch created, disposable, 'bot' accounts on mainstream social media networks to exploit high profile stories and trending hashtags. They have been detected engaging with a wide spectrum of stories and narratives, from trying to undermine international support and funding for Ukraine, through to online conspiracies about the health of the Princess of Wales.
 - The Social Design Agency and its key partner Structura National Technologies have also been responsible for innovations in the organisation and conduct of information operations and political propaganda. One involved building a monument to former Russian political leader Zhirinovskiy in the gaming platform Minecraft, attracting an audience of at least 12,000 players.
 - Even more striking was the implementation of 'Cyber-Zhirinovskiy', an AI based interactive 'chat-bot' trained using the speeches and writings of the now deceased former senior political figure who was reputedly a significant influence on Putin's thinking about nationalism. The AI avatar looks and sounds like Zhirinovskiy, and answers prepared questions about current topics and issues to find out what Zhirinovskiy would have thought about such matters were he still alive. This is significant because it shows the large language models underpinning the technology are already in use and could be trained to emulate the speech and thought patterns of any political or cultural leader. Indeed, they are ideal candidates for this because there is lots of publicly available material to train the AI models with.
 - Russian government contracting data allows us to trace how these firms have been recipients of investment from agencies associated with the Russian Presidential Administration over a number of years to develop these kinds of technologies. They now seem to be receiving 'closed contracts' for their digital influencing services.
4. Another aspect of the analysis identifies how, during the Brexit vote in London in 2016, one high-profile political technologist with close connections to the Kremlin was 'on the ground' in Mayfair conducting 'participant observation', sharing pictures of polling stations with his social media followers in Russia. He also met in person with a number of senior UK political figures. In the same year, he visited the United States. In 2024 this individual is using the knowledge and skills he acquired during these visits to help deliver a new Masters degree in 'information warfare' established by Moscow State University.

INTRODUCTION

In November 2023, an online conference ‘Trends in Political Technologies’ was convened and attended by many of Russia’s leading political technologists, and researchers in political science, election campaigning and marketing. Informed by analysis of a range of public data sources, one presentation set out what was described as a “workable agenda” for the 2024 US Presidential election. This presumably refers to exploiting the social conflicts and concerns highlighted in the material presented, where it is assessed that launching influence operations will have a disruptive effect on American politics, society, and economy. The key issues highlighted were:

- **Immigration;**
- **Economic populism;**
- **Culture wars and social identity and**
- **A general message of ‘popular sovereignty’.**

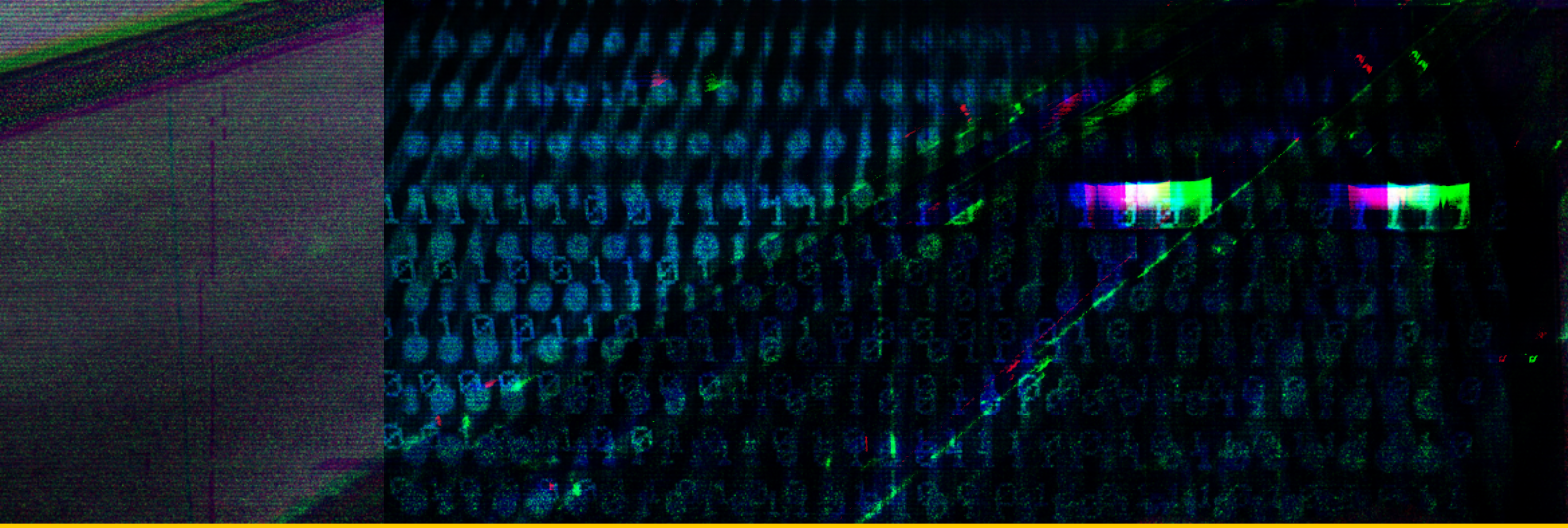
These social issues and problems are not confined to the US, but are sources of discord and disaffection across a number of Western liberal-democratic societies. Exploiting and targeting existing tensions and ‘going with the grain’ of public sentiments and disaffection in this way is wholly consistent with the historical tenets of Russia’s long established ‘active measures’ methodology.¹

The upcoming US elections appeared to be the most popular topic for those attending the online conference. Separate presentations set out detailed psycho-political profiles for a number of high-profile female US politicians who were either declared candidates, or who might be potential Vice-President material, as well as similar profiles of Republican candidates. The discussion did not include Trump or Biden, but the tier below. This might be because figures such as Vivek Ramaswamy and Nikki Haley are less familiar in Russia, but could have positions of political influence beyond the upcoming election cycle. Interspersed with some of the statistical data were screenshots from the Barbie movie, presumably as some form of semiotic commentary on US gender relations.

In addition to focusing on the US political scene, other political technologists presented prospective or retrospective analyses and assessments of elections in Africa, Turkey, Germany, Poland and Serbia. Comparing across these materials affords some important insights into the working concepts and methods of political technology. In many ways, they are mirroring the techniques and approaches being used by Western ‘open-source intelligence’ analysts, albeit refracted through a Russian lens. Cast as an instrument of Russian foreign policy, they are gathering publicly available information, such as media and polling data, and combining it with their capacity for original research and interpretation. The resulting materials are used to extrapolate key development trajectories and how they might be shaped and influenced by overt or covertly targeted information operations.

The conference was aimed at political technologists linked to one of the main organising institutions: the Russian Association for Public Relations (RASO); the Institute of International Studies, MGIMO; the International Institute of Political Expertise; and Minchenko Consulting. All these organisations have direct links to the Kremlin and indirect links to Russian intelligence agencies. MGIMO is directly run by the Ministry of Foreign Affairs.

¹ Rid, T. (2020) *Active Measures: The Secret History of Disinformation and Political Warfare*. London: Farrar, Straus & Giroux.



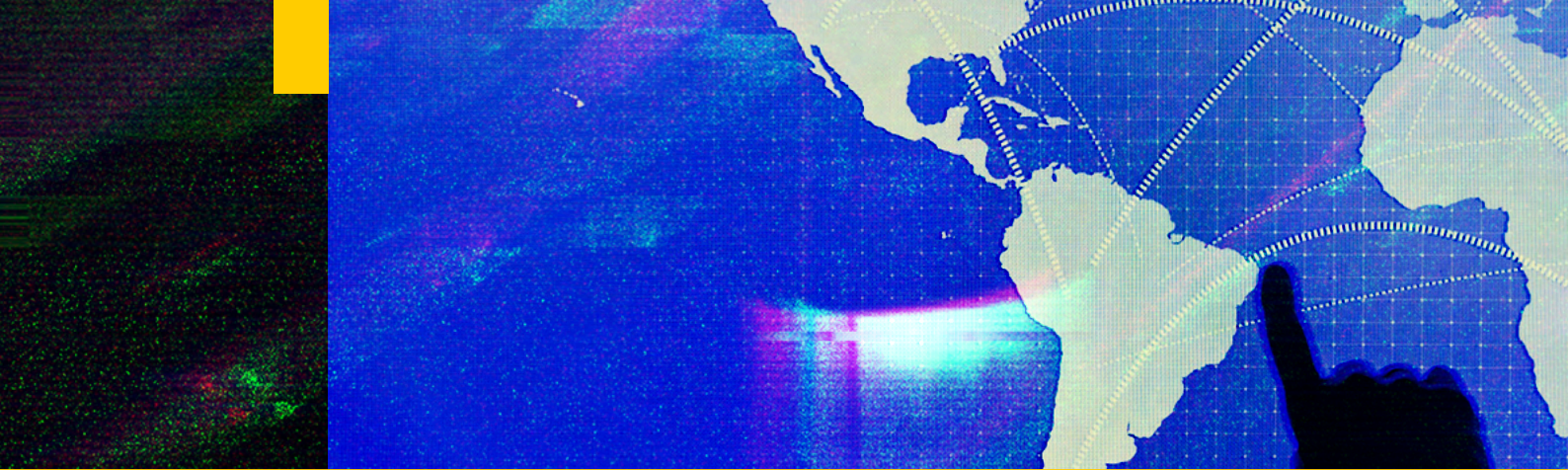
POSITIONING THE ANALYSIS

There is no precise analogue to the role and functions of the Russian political technologist in the West. They have sometimes been likened to spin doctors or political campaign managers, but that does not fully capture what they do and how. Their political ‘arts’ are darker and historically have typically been engaged to ensure an electoral process delivers a pre-determined outcome on behalf of an autocratic regime. Following Russia’s invasion of Ukraine however, there is evidence to suggest that a select group of political technologists are diversifying their interests, acquiring increasing prominence and winning sizeable commercial contracts to help deliver the Kremlin’s goals at home and abroad.

This report analyses and assesses the work and methods of political technology. Based upon two years of extensive open-source research we detail:

- How political technologists have been constructing strategies to use information operations, alongside other modes of political, economic and cultural subversion, to influence the trajectory of Russia’s development both domestically and internationally. This includes detailed analyses of the electoral systems and democratic environments for several Western countries with elections in 2024.
- The development and deployment of AI-enabled technologies by political technologists. This has clear potential to shape public perceptions and political decision-making ‘at scale’. Their campaigns have been detected operating across multiple platforms including Minecraft and Discord.
- The ‘direction and control’ mechanisms used by the Kremlin to orchestrate and coordinate the operators they are tasking. The extensive scope and scale of these activities is significant given evidence presented that influential political technologists are currently engaged in delivering Russia’s foreign policy objectives in Africa, and historically were engaged in ‘participant observation’ during the 2016 Brexit Referendum vote in London.

The title of this report deliberately draws an analogy with the ‘little green men’ who entered Crimea in 2014 to enact the Kremlin’s military plan. At that time, it was recognised that by removing the insignia and markings from the military personnel and vehicles deployed on its behalf, the Russian state was seeking a means to disavow and deny any official involvement (albeit no-one believed this). In a similar fashion, today a cadre of ‘little grey men’ are being used to deploy a range of surveillance and influence technologies as part of a wider strategy of psychological information warfare. These political technologists are operating via an array of commercial contracts to deliver digital influence engineering services, as opposed to being directly part of the military or intelligence agencies. Consequently, such arrangements such as these can obfuscate any direct links to key Kremlin decision-makers, allowing for a degree of official disavowal and denial when needed for appearances sake. As a brief caveat to this point and the language used - not all political technologists are men, but most are.



DEFINING POLITICAL TECHNOLOGY AND TECHNOLOGISTS

In Russian political culture, as well as those countries perceived as residing in Russia's 'sphere of influence', political technologists and their methods have had an important shaping effect upon the political landscape and key events. In the transitional period following the collapse of the Soviet Union, sometimes described as a 'managed democracy', figures like Vladislav Surkov became powerful centres of influence. Surkov worked a bit like a theatre director. He was engaged in setting the staging and strategic directions for the organisation and conduct of Russian domestic politics. This included what the key issues and themes to be discussed would be, both by key politicians and state media outlets. Whilst he may not have been able to determine what Russian citizens thought, he did much to frame what issues they thought about. It is claimed he was also influential in preparing the ground for the Kremlin's armed invasion of Donbass and Crimea in 2014.²

In his book 'Virtual Politics' published in 2005, the political scientist Andrew Wilson tried to define the signature qualities of political technology, concluding that:

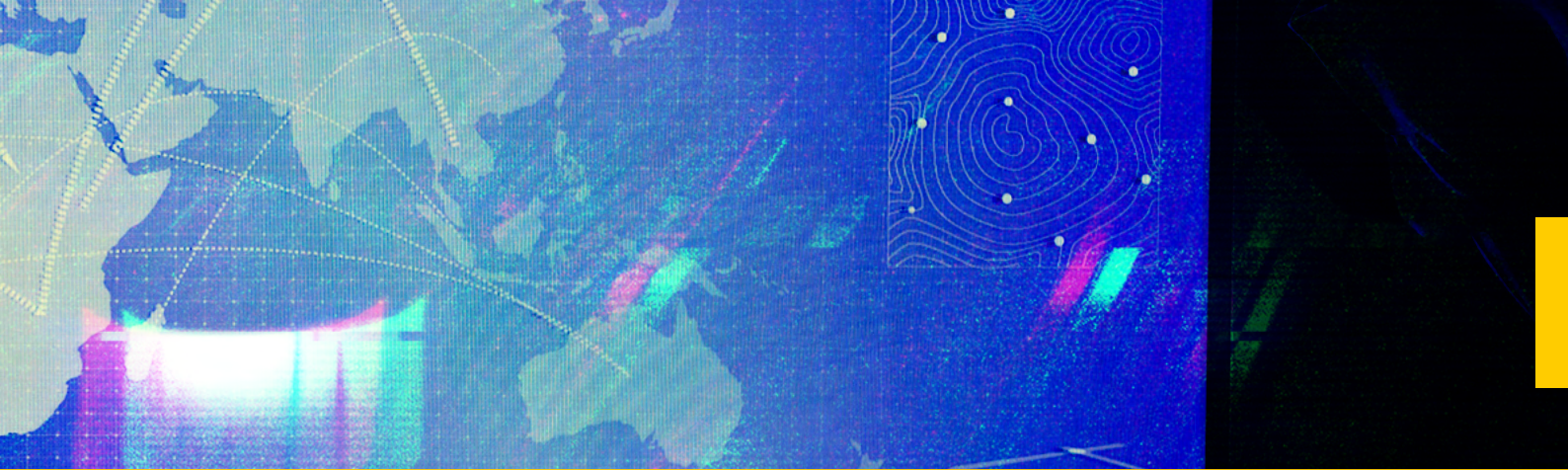
- Its practitioners are engaged in the organisation and conduct of a particular mode of social control by overseeing how power is allocated through voting processes.
- The application of political technology involves the full spectrum of overt and covert information control and influence operation techniques. Today this means the deployment of social media bots and trolls, 'hack and leak' stories, and the use of entirely 'fake' personas.³

More recently, Wilson (2023) sought to refine this definition in light of a 'globalising' effect in political technology, whereby a number of the precepts and core methods associated with the Russian tradition have been exported to countries internationally.⁴ Their common ingredient being that they are all engaged in 'supply-side influence engineering.'

² Pomerantsev, P. (2017) *Nothing is True and Everything is Possible*. London: Faber.

³ Wilson, A. (2005) *Virtual Politics: Faking Democracy in the Post-Soviet World*. New Haven: Yale University Press.

⁴ Wilson, A. (2023) *Political Technology: The Globalization of Political Manipulation*. Cambridge: Cambridge University Press.



For the purposes of this report, we define several additional signature components of political technology.

- Attends to both process and outcome in terms of how influence is exercised.
- Seeks to act upon perceptions, attitudes, and behaviours.
- Uses a range of techniques and methods where ‘information control’ is pivotal, in terms of ‘control of information’ and ‘control via information’.

If these are the base ingredients of political technology, not enough attention has been paid to how they have been operationalised by Russia’s political technologists as part of their work. There are several reasons for this. First, there has been a certain degree of ‘mirroring’ in the direction of Western analytic attention. Military analysts have largely focused on tracking their Russian equivalents, as have the intelligence agencies. However, most political technologists working in Russia today are operating on a commercial basis, winning contracts from the Kremlin and associated governmental agencies to deliver specific projects. Consequently, it has been less clear which Western governmental agencies should be responsible for monitoring them.

Secondly and relatedly, another reason political technologists have largely gone ‘under the radar’ is that Western attention was, for a time beguiled by the larger-than-life figure of Yevgeny Prigozhin. Since the initial revelations about how the Internet Research Agency was funded by Prigozhin to interfere in the 2016 US elections, Western analysts and politicians fixed their interests upon Prigozhin, and his media agencies and mercenary army ‘the Wagner Group’. However, since Prigozhin’s death in late August 2023, it has become more apparent that there was a wider cast of characters operating in a similar space to him, but who were more discreet. In effect, Prigozhin’s media profile performed a useful ‘maskirovka’ or misdirection function, allowing others to do similar work, without attracting too much attention.

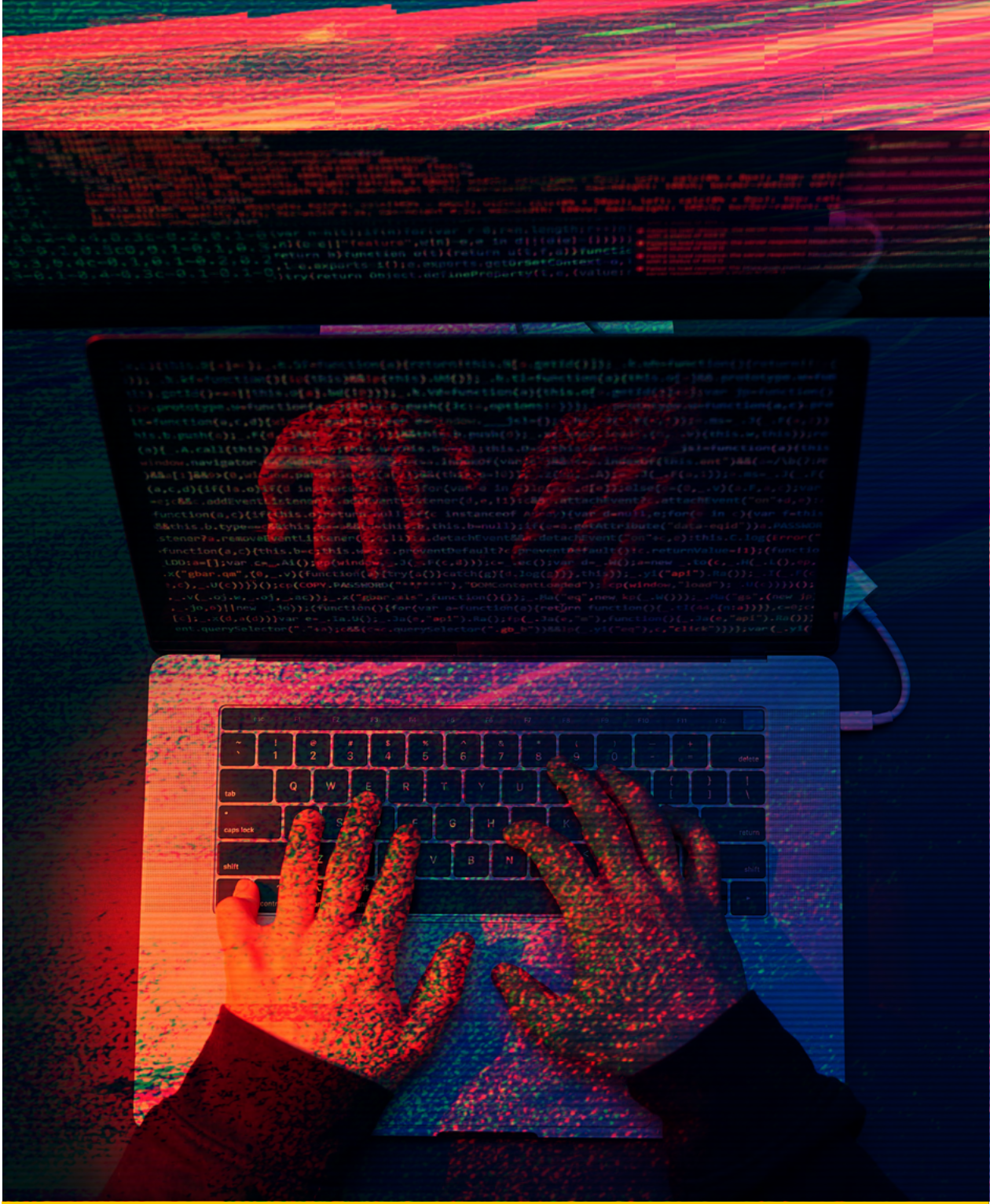
A third reason political technologists may have been somewhat overlooked is because, until relatively recently, their primary focus was thought to have largely been on the Russian domestic political scene. This appears to have changed since the launch of Putin’s war in Ukraine. For example, in September 2022, the Kremlin sought to legitimise its rule in the occupied territories of Ukraine, by holding elections. Central to these efforts was a political technologist named Alexander Malkevich.

Malkevich was sanctioned by the United States government in 2018, and the UK and EU in 2022, principally for his participation in global information operations managed by Prigozhin’s ‘Internet Research Agency’. Since then, he has emerged as a prominent figure in the Kremlin’s efforts to establish information control in occupied southern Ukraine by promoting pro-Kremlin media sources and journalism, giving lessons on the importance of ‘digital hygiene’. In the lead up to the staged elections of Autumn 2023 in the occupied regions of southern Ukraine, he was instrumental in setting up ‘schools’ for young voters, teaching high school age students how to observe the electoral process, including how to spot (Russian narrative opposing) ‘fake news’ and election interference. He was directly involved in the propaganda efforts wrapped around the referendums, setting up ‘pseudo-media’ sources ‘Mariupol 24’, ‘Tavria’ and ‘ZaTV’ to replace existing Ukrainian channels.

DOING POLITICAL TECHNOLOGY: METHODS AND METHODOLOGY

The kinds of information control and influence engineering engaged by Malkevich are typical work for political technologists. Other signature functions they perform and where they tend to have expertise can be summarised as follows:

- Designing and delivering domestic electoral processes and outcomes. In doing so, they are expected to be relatively politically agnostic. The expectation upon them is to ensure that the system overall delivers the required result, as opposed to being too deeply invested in the fortunes of any one candidate.
- Writing 'country plans' consisting of strategies for informational, political, economic, cultural and legal subversion to increase Russia's influence upon the target state. Sometimes political technologists will have a role in managing the delivery of these plans and ensuring they meet their key performance targets.
- Information control for the purposes of 'perception management' and the social ordering of reality. This can be expressed as the control of information and control *through* information, including by systematic monitoring of target countries information spaces, and seeding their own narratives and manipulating comments and replies to these.
- Conducting 'sociological' research into target countries, using both quantitative and qualitative data sources, to ascertain their vulnerabilities and identify wedge issues for potential exploitation through various 'active measures' and propaganda interventions. Political technologies are often used to construct individualised psycho-political profiles of election candidates both at home and abroad, as well as more collective assessments of electorates and audience segments.
- Political technologists tend to be 'early adopters' of new research methods, particularly those applicable to digital data and the information environment. For example, 'river sampling' invites respondents to complete an opinion survey whilst they are doing some other online activity like viewing a page on social media.
- Linked to the above, many of the campaigns that political technologists design and deliver tend to be quite creative and innovative, certainly when compared with activities associated with state security agencies. The organisation of offline mobilisations, in the form of political protests, actions and rallies is part of their toolkit.
- Monitoring for concepts, techniques and methodologies in Western research that could improve the efficacy of specific political technologies. For example, there has been considerable interest in behavioural economics and 'nudge' theory amongst some Russian political technologists. Relatedly, there are rumours of setting up an equivalent to open-source intelligence in the West.
- There is a strong accent upon youth indoctrination and engaging in activities to shape and steer the attitudes, opinions and behaviours of young people towards the Motherland. This is part of a wider 'patriotisation' and 'de-Westernisation' agenda of the Russian state that has accelerated during Russia's full-scale invasion of Ukraine.
- Instigating and running proxy political influencing agents in a range of roles such as content creators, freelance reporters, leaders of Russia supporting think-tanks and non-governmental organisations, and political parties. Once established such entities act as ready hosts and promoters over time.



The precise application of these skills and expertise will tend to reflect how there are different 'types' of technologist. Some are employed by PR agencies, others work for large multinational corporations, where others are more aligned with the security services, and/or particular federal services and agencies. These differences notwithstanding, political technologists do tend to make use of a similar toolkit in terms of the techniques they use to shape public perceptions and political decision-making, as detailed in subsequent sections.

All of these factors, however, are based on the degree to which the war in Ukraine has reframed the political technology agenda, both within Russia and as an instrument of foreign policy. This is a common thread appearing in almost all recent applications of political technology with key messages to induce greater support for Russia's military action, to undermine Ukraine's stability and that of its allies, in the process propagating the concept of a multi-polar world order where Russia once again features as a great power.

THE SOCIAL DESIGN AGENCY

In February 2024 mounting rumours and conspiracy theories began to circulate about the health, whereabouts and well-being of the Princess of Wales, Katherine Middleton, owing to her absence from public life and the cancellation of her duties. The level of interest across social media was massive; in March 2024 there were 14 billion views of posts relating to the story on TikTok alone.

Operating in amongst this torrent of claims and counterclaims were accounts displaying a set of behaviours quite well known to open-source researchers interested in Russian information operations. These behaviours included:

- **Posting replies to posts on X (formerly Twitter) about the Princess of Wales, sharing material denigrating Ukraine, celebrating President Putin's victory in the recent elections or mentioning other geopolitical points of interest to the Kremlin.**
- **The accounts posting or sharing that material in replies over a two-day period were batch created around the same date and shared similar name account handles starting with the letter 'a' or 'b'.**
- **Many of the accounts were posting in French language, often using similar but not identical messages to each other.**
- **Looking at how these accounts interacted showed a familiar pattern whereby a small number performed a 'direction and control' function, amplifying pro-Russian materials in replies sourced from a much larger number of 'satellite' feeder accounts posting that same material on their timeline.**

These are known signals for a large-scale, sprawling Russian information operation dubbed 'Doppelgänger'. It was first detected in September 2022, seemingly having started operating in May of that year. In its original form, it worked by generating clones of famous global media brands' websites, with subtle changes made to the URLs. The Doppelgänger operatives would then copy content published by the media targets, sometimes editing and amending the stories to make a different political point.

As part of mechanics of the operation, they would use large numbers of 'bot accounts' to push headlines and links associated with their fake clone websites towards users on their chosen social media platform. The intention was that users would engage with the cloned site and its material, rather than the original. The deployment of a large number of disposable, relatively low-quality social media accounts to 'flood' a social media space during a high-profile event has grown in importance as the operation has matured and adapted. Such bot accounts ostensibly clone the profiles of ordinary users, but signs of their inauthenticity are that many have a zero follower-following count, share an account handle consisting of a name and series of numbers, and sometimes use common avatars such as the 'bored ape' iconography synonymous with non-fungible tokens. In common with its cloned media aspects, it is claimed the network can rapidly generate new bot accounts, with some estimates suggesting up to 5,000 have been established within a few hours on a single day.⁵ Different batches of accounts may spread disinformation in particular languages, the use of Ukrainian for example to target, demoralise and mislead particular audience segments about the scale of corruption, forced mobilisation and casualties in war.

Within the bot network, two types of account exist. The first type posts content to its timeline, typically purposely created memes and videos to undermine Ukraine or promote Putin's Russia. The second type amplify that content by quote tweeting it in replies. The quote tweet replies are often not on subject matter relating to Ukraine, making them particularly difficult to detect, unless their visibility and reach is maximised by responding to influential accounts or hijacking trending content.

5 Zabriski, Z. (2024) 'Under the Radar: Unmasking the Coordinated Reach of Russian Doppelgänger Bots', Byline Times, <https://bylinetimes.com/2024/02/29/under-the-radar-unmasking-the-coordinated-reach-of-russian-doppelganger-bots/>

It is a methodology that has been used across a number of high-profile events, including:

- Trying to frustrate the passage of, and foment opposition to, the United States' Ukraine Aid Bill from late 2023 through into 2024 by targeting Republican voters and politicians.
- Fake Doppelgänger social media accounts responded 'at scale' to the Israel-Gaza conflict, with more than 6,000 bots posting more than 60 times per minute for seven hours to share deep fake AI generated content including in Hebrew for the first time.⁶ Doppelgänger operatives were also purchasing targeted Facebook advertisements from anonymous Facebook pages targeting German viewers with claims that Ukrainian weapons were being used in the Israel-Gaza conflict.
- Amplifying polarizing messages about the war in Gaza stimulating the student protests that took place in April / May 2024, involving occupations of University buildings in places such as Columbia and UCLA.⁷
- Responding rapidly to the Crocus Hall terrorist attack in Moscow to try and shift blame and responsibility towards, Ukraine, the US and UK.

Doppelgänger is an especially visible and 'noisy' information operation, that generates relatively low levels of engagement, but seeks to compensate for this by deploying very large numbers of accounts towards politically contentious trending media stories. This is a different strategy to that used by the Internet Research Agency (IRA). The IRA also used large numbers of inauthentic accounts, but invested significant resource in legend building over time so that they presented as members of particular US interest communities, such as 'blacktivist' or feminist groups.

As outlined in more detail below, elements of the Doppelgänger methodology reflect that it is not run by state intelligence agencies, but by a commercial entity contracted by the Kremlin to deliver these kinds of digital influencing services. This matters because whilst clearly working around Russia's geopolitical interests and agendas, Doppelgänger campaigns are also inflected by commercial imperatives. As with many other government contracts, key performance indicators are used to shape Doppelgänger's messaging focus and volume of output. These set out how many different online materials have to be produced and on what platforms, and sometimes the reach and engagement metrics being sought.

Responsibility for Doppelgänger has been attributed by the US Government, EU (August 2023) and Meta (December 2022), amongst others, to two Moscow-based organisations. In March 2024, the Department of the Treasury's Office of Foreign Assets Control (OFAC) sanctioned Ilya Gambashidze, head of the Social Design Agency, and his associate Nikolai Tupikin, CEO and owner of Russia-based Company Group Structura LLC, for their involvement in a persistent foreign malign influence campaign at the direction of the Russian Presidential Administration.⁸ The Social Design Agency (SDA) and Structura were described by the US State Department in 2023 as "influence-for-hire firms" with "deep technical capability, experience in exploiting open information environments, and a history of proliferating disinformation and propaganda to further Russia's foreign influence objectives".⁹ The SDA is also said to fulfil a dual role, acting "both as a coordinator of the various players involved in these disinformation campaigns and as an operator, creating false content."¹⁰

Because of their swarming and surging patterns of behaviour and common patterns of account design, Doppelgänger operations are relatively easy to find and confidently attribute. In September 2024, the US Department of Justice published a large number of Social Design Agency documents providing significant insight into their working methods, tools and objectives. These validate the findings reported herein based upon open-source research.¹¹

6 Benjakob, O. (2023) 'Russian Op Pushes Gaza Disinfo With Spoofed Fox News Site and 'Deep-fake' Israeli Soldiers' Haaretz. <https://www.haaretz.com/israel-news/security-aviation/2023-11-20/ty-article/.premium/deep-faked-soldiers-and-spoofed-websites-russian-campaign-pushes-gaza-disinformation/0000018b-ed5c-d36e-a3cb-fd5fadd90000>

7 Gilbert, D. (2024) 'A Russian Influence Campaign Is Exploiting College Campus Protests', Wired, <https://www.wired.com/story/russian-influence-campaign-exploiting-college-campus-protests/>

8 <https://home.treasury.gov/news/press-releases/jy2195>

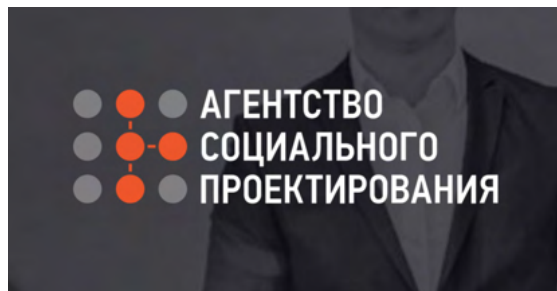
9 <https://www.state.gov/the-kremlins-efforts-to-covertly-spread-disinformation-in-latin-america/>

10 <https://www.france24.com/en/europe/20240228-ilya-gambashidze-simple-soldier-of-disinformation-or-king-of-russia-s-trolls>

11 <https://www.justice.gov/opa/media/1366261/dl>

RRN AND THE USE OF CARTOONS

‘Reliable Recent News’ (RRN) was one of the 60 website domains originally identified by Meta in September 2022. Whereas other websites spoofed the domains of legitimate news organisations in Europe, such as The Guardian and Der Spiegel, RRN remediated their false content and was the only multi-lingual site, spanning: English, German, Italian, French, Spanish, Chinese and Arabic. It has gone on to produce its own original content, including ‘voxpop’ video interviews with members of the public about current affairs topics conducted on the streets of France, Germany and California, amongst others.



RRN and Social Design Agency Logos

The Reliable Recent News website has clear Russian origins and can be traced back to now defunct site Reliable Russian News (russiannews[.]com). The two share the same branding and the switch likely happened around 06 June 2022 when the rrn[.]world domain was created. This was around the same time as the first spoofed Doppelgänger media domains were created. The website has been hosted by a UK company based in London, who also hosted a variety of Russian websites. The UK company director is linked to other companies in Russia. During 2022, an APT (advanced persistent threat) group used this UK company’s servers to launch a serious cyber-attack. We can say with high confidence that the owners of Reliable Recent News (rrn[.]world) also owned now defunct site Reliable Russian News (russiannews[.]com), with the latter automatically redirecting to rrn[.]world, as both domains used the same Google analytics ID GTM-KXLML67.

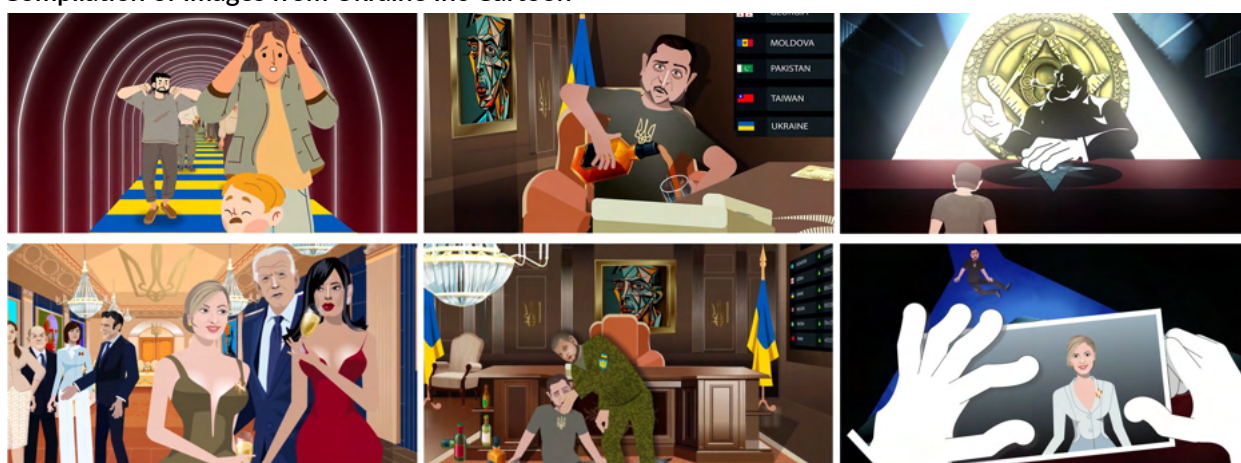
Whilst still under construction, the rrn[.]world website was registered to Joint Stock Company RU-Center in Russia and its server name was nic.ru. The website’s metadata sets its location to Russia, but as it uses a WordPress template that dynamically generates pages, there is not much original code to be found and there is no useful metadata on their images. There are also domain links to the Russian campaign ‘War on Fakes’ whose website was registered in the same month, which is also linked to ANO Dialog.. In common with both its predecessor and War on Fakes, the rrn[.]world website has been repeatedly shared by official Russian state accounts suggesting that its content has government support.

In common with the spoofed domains in the same network, links to RRN articles are amplified across social networks by others, but also by RRN’s own branded social media, operating on English language Telegram, multiple X / Twitter accounts (one suspended 23/09/2022) and a YouTube channel posting in English and German. The affidavit published by the US Department of Justice identifies the organisation ANO Dialog and political technologist Vladimir Tabak as responsible for leasing and running RRN.

In July 2022, an RRN ‘expert community’ of four self-proclaimed journalists with links to Germany, Spain, France and the UK published content on the website sharing disinformation about the number of dead children in Donbas attributable to Western weapons in Ukraine. All of their video reporting linked to another website with identifiable Russian links called [truemaps\[.\]info](https://truemaps.info). Links to this website propagated by these journalists were shared across Facebook in multiple languages and by four Russian embassy accounts. One communication tactic used particularly effectively by RRN has been cartoon animations with political themes. These cartoons condense and simplify complicated topics whilst also being language agnostic, making them easily understandable for multi-lingual international audiences. There is a notable precedent for using cartoons within Russian contemporary disinformation campaigns; they were used extensively by the Prigozhin-linked Project Lakhta to spread disinformation in Africa.¹²

RRN has utilised cartoons to illustrate news stories on their website and/or social media, and as a key feature of their agenda of undermining Ukraine. This involved a Russian hosted website [Ukraine-inc\[.\]info](https://ukraine-inc.info) that was set up on 11 March 2023¹³ and used as a portal to release a total of eleven animated cartoon episodes about the Ukraine war up until March 2024. These animations focus on various iterations of the ‘drug-addled, conspiracy puppet’ Zelensky.

Compilation of Images from Ukraine Inc Cartoon



Detailed analysis of the animation images and artistic style suggest that a number of the images featured in [Ukraine-inc\[.\]info](https://ukraine-inc.info) cartoons are shared with a 2020 Armenian animation series called “Kill Dim” published by the Sakahyants studio. Relatedly, key aspects of the storyboard used to portray Zelensky as a puppet pressing Western buttons is replicated from animations that Russian accounts attributed to fictitious ‘French animators’ Barracuda in 2022. RRN’s role on social media platforms X and Telegram helped the first cartoon video to go viral through their early reposts.

RRN played a similar role in relation to an offline graffiti campaign in Paris in late 2023. This involved the ‘Star of David’ being spray painted across a number of prominent locations. RRN were suspiciously quick in their ability to report on these incidents, contributing in part to this story being picked up and remediated by a number of global mainstream media outlets.

In addition to their involvement in *Doppelgänger* and RRN, in November 2023 the US State Department linked both the Social Design Agency and Structura, along with ‘the Institute for Internet Development’ to information operations targeting Latin America, undermining support for Ukraine, and activities aiming to discredit the US and NATO. The former operated through the *Pressenza* media network, which focuses upon and represents left-wing and ‘progressive’ political standpoints.

The activities in Latin America have been useful in providing insight into key features of how SDA campaigns

12 Atanesian, G. (2023) ‘Twitter staff cuts leave Russian trolls unchecked’, BBC. <https://www.bbc.co.uk/news/technology-65067707>

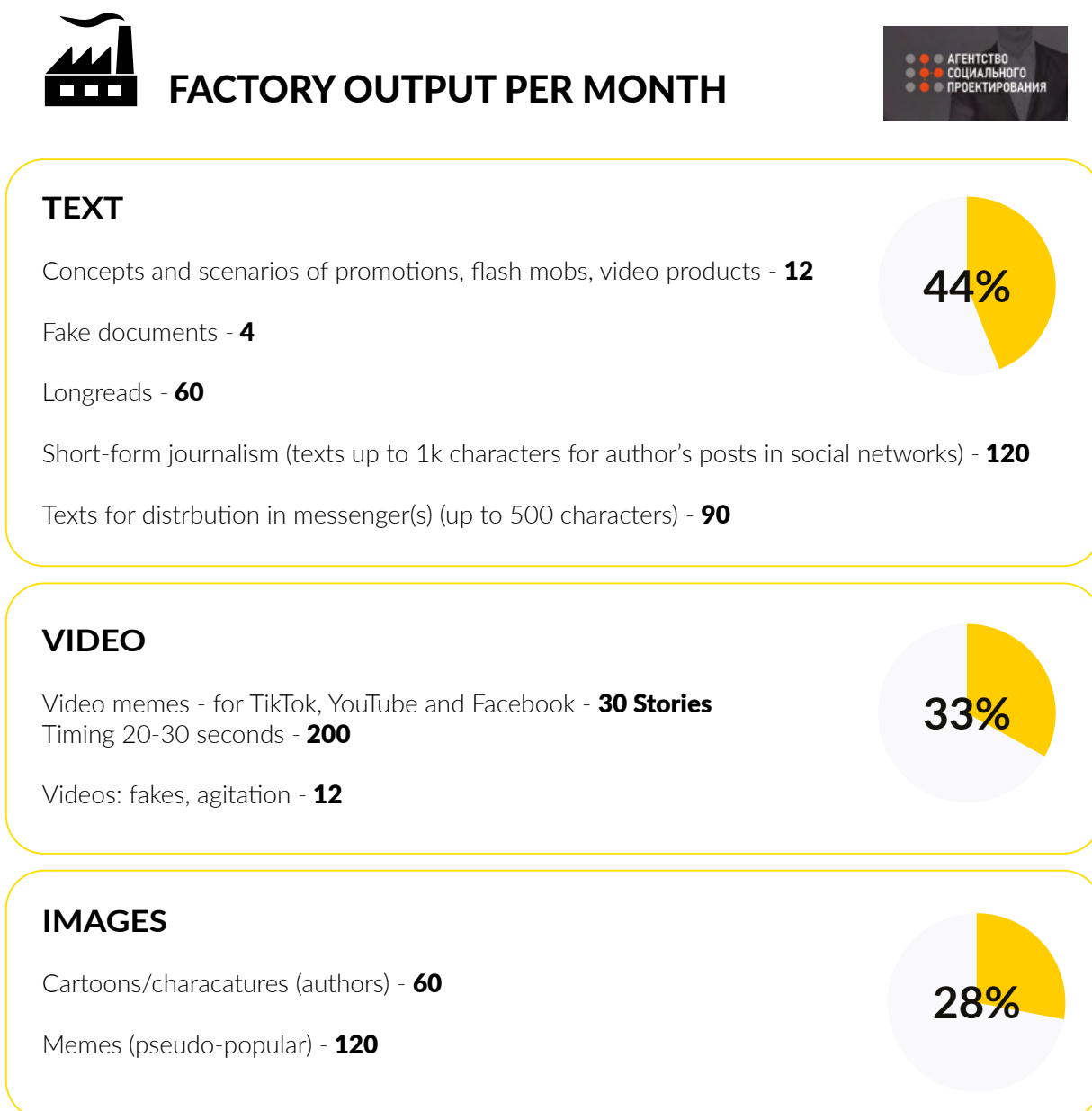
13 Viginum (2023) RRN: A complex and persistent information manipulation campaign. https://www.sgdsn.gouv.fr/files/files/Publications/20230719_NP_VIGINUM_RAPPORT-CAMPAGNE-RRN_EN.pdf

are organised, conducted and managed. Four documents associated with this theatre of operations were leaked, detailing the performance indicators used to guide SDA's social media activities targeting Mexico, Brazil and Argentina. These detail how their 'Pulse System' would be used to:

- Post 60 messages per day, or 5-7 per country.
- Produce 4 original publications per day, aimed at journalistic outlets.

SDA operatives were additionally tasked to engage in a range of other activities, including: recruiting journalists and content creators; conducting and publishing formative opinion polls on social media; undertaking open-source and in-house sociological research, and 'ideological work strategies; holding public events such as rallies and protests.

Figure 1 below, outlines similar performance indicators for SDA's work focused upon a plan agreed for Ukraine.



INNOVATIVE INFLUENCING TECHNOLOGIES: CYBER-ZHIRINOVSKY AND MINECRAFT

Doppelgänger and RRN are the more well known and overt aspects of the SDA's work. There are, however, several other technologies they have been involved in designing and deploying about which there is less awareness. These are more innovative and enabled by the use of artificial intelligence.

The Russian government has shown interest in AI for many years. In 2017, President Vladimir Putin stated that "whoever becomes a leader in AI will rule the world."¹⁴ The next three years were followed up by intense investment from the federal budget and state-owned enterprises. For example, in 2019 Putin signed a national strategy for the development of artificial intelligence.¹⁵ In 2021, the government allocated 1.4 billion Rubles for grants to AI developers.¹⁶ The plan for 2024, according to Russian authorities, is to allocate about 5.2 bln Rubles (\$54.05 mln) in the federal budget for the development of artificial intelligence technologies.¹⁷ There is also a specialist artificial intelligence directorate within the defense ministry¹⁸ and former defense minister Shoigu claimed they are producing combat robots capable of working without operators.¹⁹

There are reports of several new AI surveillance systems planned for mass digital surveillance. The 'Vepr' system will look for "information pressure points" and forecast where and when protests might erupt.²⁰ 'MIR' will handle fully automated searches for prohibited content.²¹ 'Oculus' is designed to identify calls for protests in images and videos, and to recognise the faces of demonstrators.

SDA and Structura's contribution to these developments has seemingly been inspired by the success of ChatGPT and other LLMs in the West, taking the form of 'Cyber-Zhirinovsky.'

In April 2023, the far-right Liberal-Democratic Party of Russia (LDPR) unveiled an AI chatbot of its dead leader, ultranationalist Vladimir Zhirinovsky, at the St. Petersburg International Economic Forum. Zhirinovsky had been one of the most visible and well-known figures in Russian politics over the past three decades, capturing domestic and international headlines with his xenophobic comments and outlandish public behavior, including fistfights in parliament and on television talk shows. As Sergei Medvedev describes, he was also an important figure in the development of Putin's thinking.²²

Cyber-Zhirinovsky is a chat-bot whose underpinning model has been trained on the vast amounts of texts and speeches of the right-wing politician. Aleksandr Dupin, press secretary of the LDPR, claimed it is based on more than 18,000 hours of interviews and speeches given by the politician over more than 30 years,²³ enough to generate answers to possible new questions. The Cyber-Zhirinovsky project launched on Telegram, on a channel under the same name, where answers to various political questions started to appear in an audio and chat form,²⁴ and later in audio, video and chat²⁵. As of March 2024, hundreds of questions have been answered with opinions given by 'Zhirinovsky': from: discrediting "Nazi Ukraine" on a weekly basis (e.g. as a "swamp full of traitors and Russophobes")²⁶; to communist-sounding jokes²⁷; commenting on elections in foreign countries; Russian politics; opining on global warming; LGBTQ rights in Russia; and many other topics.

14 <https://www.rt.com/news/401731-ai-rule-world-putin/>

15 <https://www.defenseone.com/technology/2019/01/putin-orders-national-ai-strategy/154555/>

16 <https://apps.dtic.mil/sti/trecms/pdf/AD1151100.pdf>

17 <https://tass.com/economy/1680865>

18 <https://tass.com/defense/1497995>

19 <https://tass.com/defense/1684137>

20 <https://re-russia.net/en/analytics/054/>

21 <https://thebell.io/tsifrovaya-diktatura-dlya-rossiyan-kak-sozdat-pravdopodobnogo-bota-i-chitayut-li-spetssluzhby-telegram>

22 Medvedev, S. (2023) *A War Made in Russia*. Chichester: Wiley.

23 <https://www.pravda.com.ua/eng/news/2023/04/6/7396746/>

24 https://t.me/zhirinovsky_II/5

25 https://t.me/zhirinovsky_II/142

26 <https://www.themoscowtimes.com/2023/06/15/russian-far-right-party-unveils-ai-chatbot-of-deceased-leader-a81519>

27 https://t.me/zhirinovsky_II/99; https://t.me/zhirinovsky_II/14; https://t.me/zhirinovsky_II/192



Screenshot of CyberZhirinovskiy

Cyber-Zhirinovskiy has been publicly credited to political technologist Iliya Gambashidze, under the supervision of State Duma deputy and LDPR member Vladimir Koshelev,²⁸ and Deputy Head of the LDPR Central Office, Sergei Minaev. The company which developed the underpinning neural network is Nanosemantics.ai, an AI-focused company developed by Russian information technology entrepreneurs Igor Ashmanov and Natalya Kasperskaya.²⁹

In May 2023, Gambashidze was also credited with the launch of a Minecraft server event that included a digital monument to Zhirinovskiy. Reportedly the event attracted over 12,000 visitors to the site. The LDPR has confirmed its use of gaming platforms to communicate with voters and attract new supporters, as “the first digital party of Russia.”³⁰

Following the launch of Cyber-Zhirinovskiy AI and the Zhirinovskiy monument in Minecraft, Gambashidze was highly praised in Russian political technology circles. He was nominated and won in two categories at the 2023

RAPK “Choice” awards. The project “Monument to Zhirinovskiy on Minecraft”, was nominated in the category “Best Campaign Event” and Cyber-Zhirinovskiy in the category “Best viral project of the season”.³¹ Cyber-Zhirinovskiy was also nominated “politician of the year”, winning in at least one category of the “Political Award” at the Russian Association for 2023.³²

There is currently talk by the Communist party about designing a ‘Cyber-Lenin’, and it is likely that similar projects will also appear elsewhere.³³ The Cyber-Zhirinovskiy model demonstrates that this kind of technology is ready to be deployed for any major political figure. Indeed, the more speeches and material derived from an individual that can be used as ‘training data’ for the underpinning AI models, the more persuasive and effective the performance of the technology will be. A presence on Minecraft evidences how Russian information operations are already spread across a diversity of digital surfaces. The majority of Western analyses of information operations have focused upon the main social media platforms and websites, so missing the more innovative developments being made by Russian operatives and organisations.



Screenshot of Zhirinovskiy Monument in Minecraft.

28 <https://www.kommersant.ru/doc/6364951>

29 <https://nanosemantics.ai/about-us>

30 <https://ria.ru/20230501/zhirinovskiy-1868971873.html>

31 <https://rapc.pro/award/registration/>

32 <https://t.me/Politteh/1549>

33 <https://www.pnp.ru/politics/zhirinovskiy-i-lenin-mogut-vnov-povesti-svoei-partii-na-vybory.html> + <https://ria.ru/20231027/lenin-1905583470.html>

HOW POLITICAL TECHNOLOGISTS ARE ‘MADE’ AND TRAINED

Political technology is a blend of art, craft and science. This is supported by the different methodologies for creating and implementing persuasive campaigns that were discussed in the previous sections. Political technology as an ‘art’ involves operators using their creativity and inventiveness to solve specific difficulties and obstacles to get around restrictions and reach their intended audiences.

The ‘craft’ skills of the political technologist are likewise primarily applied inductively, but are taught and gained via experience. These skills pertain to knowing what to do and when to do it, in order to achieve a specific goal.

Importantly, what separates political technologists from other practitioners engaged in digital influence engineering is the degree to which it is underpinned by scientific theories and precepts. Indeed, many of them have been trained at some of Russia’s most prestigious universities, and some possess doctorate level qualifications in relevant subjects. This scientific ethos can also be observed in the harnessing of AI technologies as described above, but more routinely and regularly the extent to which political technologists are formally trained in, and apply approaches derived from the social psychology of influence, sociological research methods, and concepts from political science.

By looking at Ilya Gambashidze’s biography, it is possible to see the overlaps and interconnections in terms of how this blend of expertise is developed and, thus, how political technologists are ‘made.’

In 2008, Gambashidze completed a dissertation entitled “*Features of the development of local self-government in the Russian Federation in the context of the transformation of the party system*” at Moscow State University department for Political Science (in Russian ‘Politology’).³⁴ A couple of years later he worked as an assistant to the ex-prefect of the Northern District of Moscow, Oleg Mitvol. Some sources claim that at that time he was also working as a political strategist for the United Russia political party³⁵ and by 2015 was engaged in “socio-political research in municipal districts - including commissioned by the Moscow City Hall.”³⁶ Between 2015 and 2020, Gambashidze was rarely mentioned in Russian media, but was described as a political technologist.³⁷ According to investigative journalists, between 2013-2020 companies owned wholly or in part by Gambashidze were awarded government contracts worth about \$2.7M.³⁸

In 2020, a vote on amendments to the Russian state constitution took place, including online voting for the first time. The proposed amendments aimed primarily to secure the continuity of Putin’s power and were overwhelmingly supported in the popular vote. Prior to the vote, the website of the State Duma published the full text of the amendments³⁹ and specified that reading through the whole page will take over an hour. Several Russian media outlets reported that Gambashidze and **Structura** were commissioned to develop chatbots designed to summarise relevant information on the amendments for the public to easily consume.⁴⁰ It is likely that these functioned as propaganda and persuasion tools seeking to sway public opinion in favour of Putin. The chatbots were hosted on a website inform-bot[.]ru (no longer functional) and operated on Telegram, VKontakte or Viber.⁴¹ Prior to the vote, Russian official media heavily promoted this Structura created programme, including prominent publications like Rossiyskaya Gazeta and Lenta, where Gambashidze was described as the “creator of the bots.”⁴²

34 <http://www.dslib.net/polit-instituty/osobennosti-razvitiya-mestnogo-samoupravleniya-v-rossijskoj-federacii-v-kontekste.html>

35 <https://www.rbc.ru/investigation/business/26/10/2015/562a6a6f9a79471bfeb73de4>

36 <https://www.rbc.ru/investigation/business/26/10/2015/562a6a6f9a79471bfeb73de4>

37 <https://cepa.org/article/elections-matter-in-russia/>

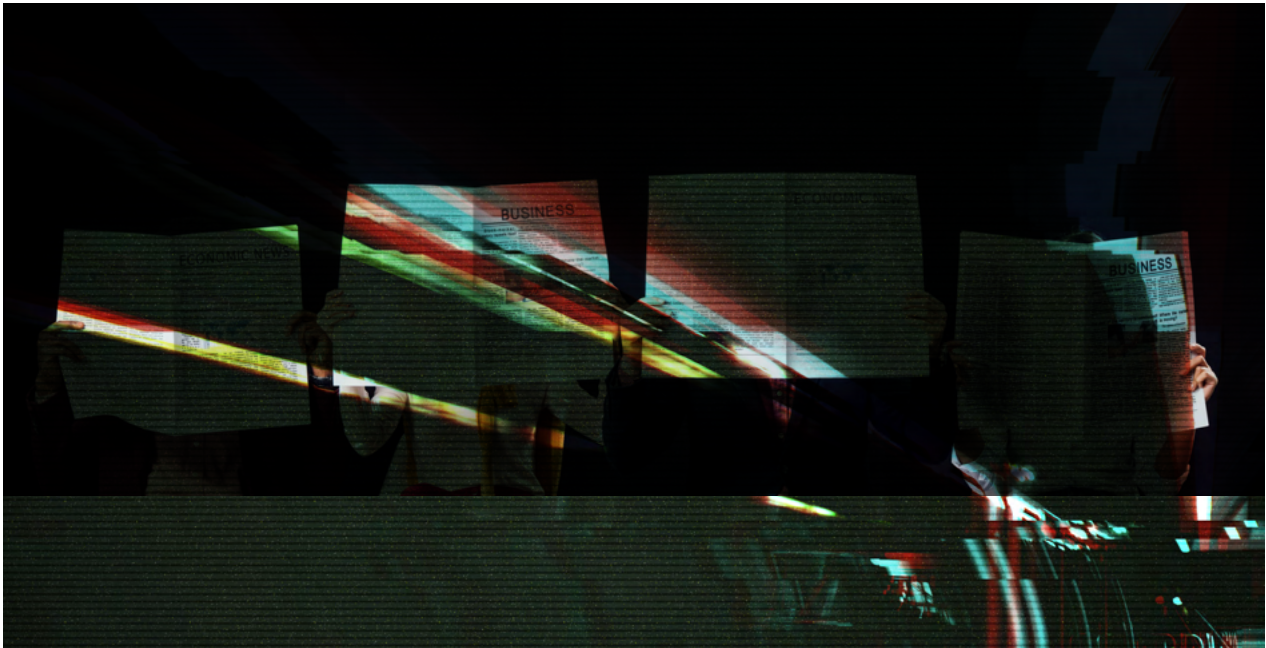
38 <https://www.voanews.com/a/investigation-who-is-ilya-gambashidze-the-man-the-us-government-accuses-of-running-a-kremlin-disinformation-campaign-/7604052.html>

39 <http://duma.gov.ru/news/48045/>

40 <https://www.facebook.com/photo/?fbid=836359223555088&set=a.754389941752017>

41 <https://lenta.ru/articles/2020/06/28/golos/>

42 <https://lenta.ru/articles/2020/06/28/golos/>; <https://dailystorm.ru/news/razrabotchiki-predlozhili-zapustit-obshcherossiyskiy-chat-bot-dlya-informirovaniya-o-golosovanii>; <https://rg.ru/2020/03/20/v-cike-predstavili-sajt-i-popravkah-v-konstituciu-i-procedure-golosovaniia.html>



From 2023 onwards, Gambashidze began to be mentioned more regularly in Russian media and across political Telegram channels. Some Russian outlets argued that the LDPR “relaunched itself in the media space” thanks to a team of party technologists “led by the famous federal political strategist Ilya Gambashidze.”⁴³ In 2024 Gambashidze was rumoured to be the personal political technologist for LDPR leader Leonid Slutsky’s Presidential campaign, although information about his success is mixed and unclear.

Andrey Pertsev, a journalist with the Latvia-based independent Russian website Meduza, observes that the “[SDA] team often made mistakes and [Gambashidze] was repeatedly called back to Moscow to avoid an electoral setback. In 2023, Gambashidze’s associate, political strategist Mikhail Biyun, who is also director of special operations at SDA, organised a release of pigs tattooed with the Communist party emblem in Khakassia, a republic in southern Siberia.⁴⁴ The aim of the pig release was to discredit the Republic’s Communist governor, Valentin Konovalov. However, according to anonymous Telegram channel VCHK-OPGU, the campaign backfired. Biyun was accused by a section of the local population of “ridiculing Russian history”, then fined for violating campaign rules.⁴⁵

Even though Gambashidze has been mentioned in Russian media more frequently during the last couple of years, his modus operandi is still mainly shrouded in privacy and discretion. He is not listed on any of the political technologist associations described below, even though he has been a recipient of awards from them.

Due to Gambashidze’s international disinformation operations undermining Ukraine, some observers have dubbed him “Vladimir Putin’s new troll-general” following the death of Yevgeny Prigozhin in 2023⁴⁶ asserting that the Social Design Agency is gradually replacing Prigozhin’s Internet Research Agency. More generally, the political technology and propaganda ecosystem seems to comprise a network of actors who practise different variants of political technology.

Of note is that a number of political technologists who are now becoming more prominent within the Russian system originally gained some of their craft skills and formative experiences working for Prigozhin’s organisations. Prigozhin himself would probably not be defined as a political technologist, owing to his lack of formal training in the area. That said, he clearly understood and used analogous logics and practices, employing others with relevant training and education to assist him.

43 <https://tagilcity.ru/news/2023-09-29/uspeh-ldpr-ili-proval-kprf-cto-sluchilos-na-vyborah-v-gorodskuyu-dumu-ekaterinburga-3040654>

44 <https://t.me/vchkogpu/44548?single>

45 <https://www.france24.com/en/europe/20240228-ilya-gambashidze-simple-soldier-of-disinformation-or-king-of-russia-s-trolls>

46 <https://borsen.dagbladet.no/nyheter/bakmann-avslort/81056168>; also here <https://www.france24.com/en/europe/20240228-ilya-gambashidze-simple-soldier-of-disinformation-or-king-of-russia-s-trolls>

THE SCALE AND ORGANISATION OF POLITICAL TECHNOLOGY IN RUSSIA

Political Technologists in Russia have three professional membership associations. The three most prominent ones currently are RAPK (Russian Association of Political Consultants), RASO (Russian Association of Public Relations), and AIT (Association of Internet Technologists). In addition, there are other related organisations such as the National Guild of Professional Consultants,⁴⁷ and the Association of Communication Agencies of Russia (AKAR)⁴⁸. Combined, the membership lists for these organisations allow us to estimate that today there are well over 500 individuals working as political technologists, or in very similar roles.

The Russian Association for Public Relations (RASO) is the oldest PR and political consultancy association still functioning today. It was created in 1991 in an early effort to institutionalize public relations in Russia during the post-Soviet transition. RASO was co-founded by several institutions including the Moscow State Institute of International Relations (MGIMO), the Ministry of Foreign Affairs, Union of Journalists of the USSR, the Russian Embassy in the US, and others.⁴⁹ Alexander Borisov, a professor at Moscow's MGIMO, became RASO's first president.⁵⁰ Related to the creation of RASO, and the development of public relations and political consultancy is the concurrent development of Russian education in public relations practice - including the emerging concept of political technology.⁵¹ ⁵² For example, in 1991 MGIMO became the first university in Russia to concentrate on public relations and it remains influential today in training a number of highly reputed political technologists.⁵³

The current president of RASO, Yevgeny Minchenko, is associated with MGIMO, as Director of the Centre for Political Elite Studies and the Institute of International Studies, as well as lecturer at the Department of Regional Management and National Policy.⁵⁴ MGIMO is directly run by the Ministry of Foreign Affairs. Since 2018 there have been several allegations suggesting MGIMO is used by the Russian secret services for recruiting students for missions abroad or for international-related work.⁵⁵ RASO and MGIMO have co-organised several conferences on PR and political technology over the years, bringing together well-known political technologists and MGIMO scholars.⁵⁶

47 <http://www.ngpc.ru/>

48 <https://www.akarussia.ru/>

49 <https://raso.ru/history>

50 <https://raso.ru/history>

51 https://www.cairn-int.info/article-E_MULT_039_0109--higher-education-in-post-soviet-russia.htm

52 https://www.researchgate.net/publication/365350073_Public_Relations_in_Russia_Formation_Etatization_and_Calcification

53 <https://english.mgimo.ru/structure/schools/school-of-international-journalism/department-of-public-relations>

54 https://mgimo.ru/people/minchenko/?utm_source=google.com&utm_medium=organic&utm_campaign=google.com&utm_referrer=google.com

55 <https://www.reading.ac.uk/news/2022/University-News/MGIMO-partnership-suspended>;

<https://www.proekt.media/en/article-en/russian-diplomatic-students-are-recruited-by-the-intelligence-services/>; <https://www.zois-berlin.de/en/publications/zois-spotlight/the-role-of-think-tanks-in-russian-foreign-policy>; <https://meduza.io/en/feature/2022/04/25/it-creates-the-intended-effect-fear>

56 2023 https://raso.ru/news_raso/tpost/pg6hkpkh21-programma-ii-nauchno-prakticheskoi-konfe; 2023 <https://mgimo.ru/about/news/departments/puti-transformacii-gosudarstvennogo-i-korporativnogo-upravleniya-na-sovremennom-etape-2023/>; 2006 <https://www.sostav.ru/news/2006/03/15/fest3/>

RASO has around 336 members with various specialties and professional experience – Political technologists, PR-consultants, communication strategists, academics from Russian universities,⁵⁷ business consultants, political scientists, and others. Many RASO members were educated at MGIMO. At least 13 members of RASO have been included in rankings⁵⁸ of top political technologists in 2022, including Yevgeny Minchenko, Igor Mintusov, Andrey Tsepelev, and Valentin Bianki.

The Russian Association of Political Consultants (RAPK) was created in 2014 to bring together professional political technologists, strategists, and consultants with varied expertise and capabilities, in addition to some political scientists, political lawyers, journalists, and politicians.⁵⁹ Its members are all working in the field of organising and conducting election campaigns, cooperation with politicians, government officials and public figures, conducting sociological research, and PR. It is claimed that annually, members of the RAPK are involved in the preparation and conduct of more than 20,000 election and political campaigns in all constituent entities of the Russian Federation at different levels of government.

The website of RAPK also states that some members have been ‘invited’ to work as ‘experts’ in election campaigns across Europe, Asia, Africa and America.⁶⁰ The first PR agency, Niccolo M (RAPK partner), states that its leaders (e.g. political technologist Igor Mintusov) have participated in a number of “successful election campaigns in neighbouring countries” such as Belarus, Ukraine, Latvia, Georgia, Kyrgyzstan and abroad, including in Poland, Mongolia, Nicaragua, South Korea, Venezuela, Colombia and USA.⁶¹ Igor Mintusov is a member of both RAPK and RASO.

The structure includes about 135 high-profile members, 30 of whom were included in the ratings for “top” political technologists in 2022. RAPK also partners with several political technology and sociological associations and companies, including the Association of Internet Technologists (AIT), the Centre for Applied Research and Programs (PRISP), and the Agency for Political and Economic Communications (APEC).⁶² The President of RAPK is famous political technologist Grigory Kazankov.⁶³

AIT (Association of Internet Technologists), is the newest structure, created in January 2021. It includes leading internet technologists, consultants, and heads of internet agencies - 12 founders and 80 members from different regions of Russia.⁶⁴ The organisation is officially registered with the Ministry of Justice of the Russian Federation. Andrei Tsepelev, Deputy General Director of ‘Dialog Regions’, is also the first president of AIT.⁶⁵ AIT involves 57 members. It was co-founded by 12 individuals, six of whom are associated with ANO Dialog Regions and/or Dialog Regions including RRN linked political technologists Vladimir Tabak (director of ANO Dialog), Kirill Istomin (also listed as Deputy General Director of Dialog Regions), Tikhon Makarov (Advisor to the General Director of ANO Dialog).⁶⁶

A network map based on memberships was created to better understand i) the relationships between these organisations and their respective members and ii) how this impacts the configuration of the professional community that individual political technologists inhabit.

Visualised in Figure 2 below, the vast majority of political technologists belong to only one professional association. Only 4% of individuals hold two or more memberships.

57 For example these people: https://raso.ru/members_raso/tproduct/360912967-361248519471-arkannikova-marina-sergeevna;

58 Rankings are by APEK (Agency for Political and Economic Communications), the outlet Obshchaya Gazeta, and the outlet Noviy Izvestiya. It is clear that these ranking may be biased. For example, APEK is headed by PT Dmitry Orlov, who is included in the Top political technologists. However, two aspects of these rankings make them particularly useful – (1) looking for overlap and thus learning who are the “biggest” names in the industry, and (2) finding individuals who have opted out of membership of the abovementioned associations. Such names if the head of the Social Design Agency – Ilya Gambashidze, who is not a listed member in any of the PT associations but is mentioned in two of the PT rankings.

59 <https://rapc.pro/members/>

60 <https://rapc.pro/deyatelnost-rapk/>

61 <http://nikkolom.ru/>

62 <https://rapc.pro/partners/agentstvo-politicheskikh-i-ekonomicheskikh-kommunikaczij-apek/>

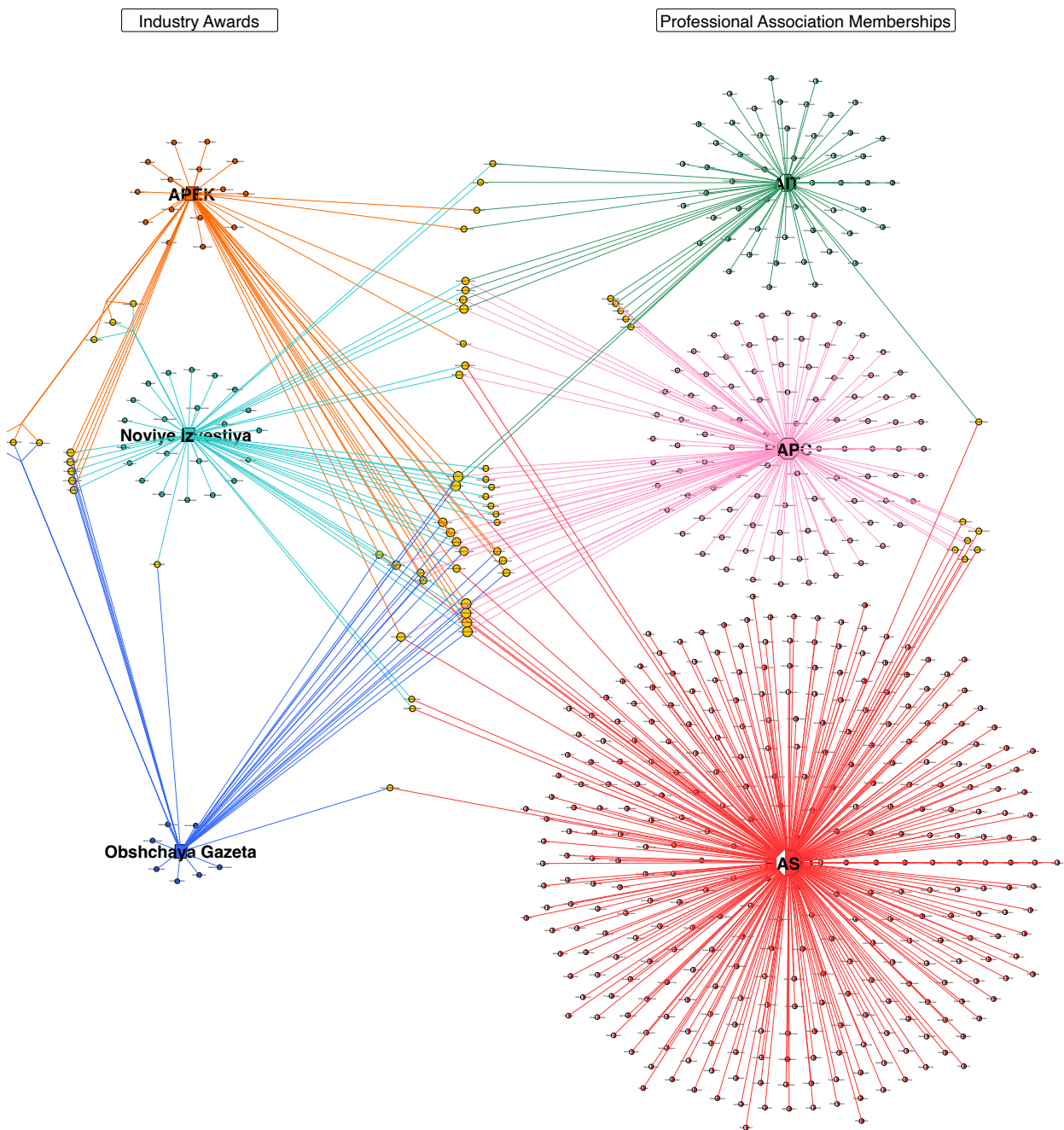
63 <https://rapc.pro/about/>

64 <https://ain-tech.ru/>

65 <https://ain-tech.ru/members/andrey-cepelev>

66 <https://ain-tech.ru/members/tihon-makarov>

Figure 2 below is a network visualisation of political technologist professional association membership



One possible interpretation of these network data is that only a relatively small number of political technologists act as 'bridges' between the main centres of political technology activity.

Professional awards and reputational indicators

As detailed above, the professional community of political technologists and allied professions is quite large and has been growing recently. Insight into the individuals, ideas and methodologies that are influencing the development and evolution of the profession can be derived by examining recipients of various awards made by the professional associations. These provide an indicator of whose work is receiving attention and is admired by their peers, and thus whose reputations are in the ascendancy.

Annual awards events organised by individual associations are widely advertised, highly publicised, and are another method for mainstreaming political technology. Since the late 1990s, RASO (as the most established) has sponsored and co-sponsored several professional contests, including ‘the Silver Archer’ national award to promote the prestige of the public relations profession.⁶⁷

RAPK hosts its annual ‘Choice Awards’ – a glamorous ceremony that has been taking place since 2015.⁶⁸ This sits alongside the ‘RAPK Congress’ which is praised as “the main annual event in the Russian political consulting market”, convening representatives of government bodies of the Russian Federation, parliamentary and non-parliamentary political parties, science and the expert community, research institutes, universities and political consultants to discuss trends and methods of political and election campaigns domestically and internationally.⁶⁹

The Choice Awards identify, encourage, and award ‘election specialists’ across a long list of categories. Last year, the number of applicants to RAPK annual awards increased from 76 applications in 2022, to 100 in 2023. This evidences both the popularity of the event but also potentially supports the claims that the political technology profession is expanding.⁷⁰ There was an increase in the number of award categories across a range of themes, including: best campaign event; best campaign audio or video; best website of a candidate; best viral project of the season; best promotion mechanism on the internet / social networks; and new election campaign tools; best sociological support for the election campaign and best electoral mobilisation project.

New categories	Awarded/nominated projects
Best electoral mobilization project	Project “DEG Assistant”.
	Project “Digital mobilization using modern technologies”.
	Project: “Comprehensive method for increasing participation in electronic electoral mobilization within the framework of the election campaign for the Yaroslavl Regional Duma 2023”.
The best sociological support for the election campaign	Project “Sociological support (online sociology) for the elections of the governor of the Smolensk region”.
	Project: “Application of systemic proprietary methods for assessing the problem field in social media in a regional campaign”.
Best legal project of an election campaign	Project “Khakassia: legal support of the “matryoshka”.
	Project: “Legal project within the framework of mobilization campaigns, Omsk and Irkutsk region”.

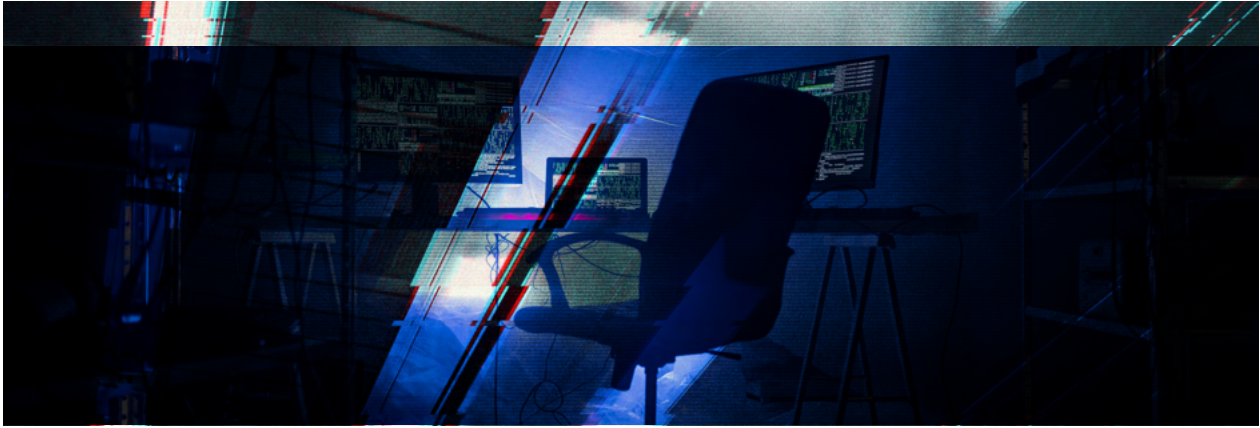
The three new categories introduced for 2023 signal an increased interest in digital methods. Table 1 above lists these categories and the nominations for them.

⁶⁷ <https://raso.ru/history>

⁶⁸ Also organised by RAPK is the annual RAPK “Congress” conference.

⁶⁹ <https://rapc.pro/project/kongressy-rossijskoj-associazcii-politicheskikh-konsultantov/>

⁷⁰ <http://vybor-naroda.org/lentanovostey/253646-vruchena-premija-rapk-vybor-v-2023-godu.html>



The juries who decide the awards are themselves high-profile political technologists, including Dmitry Orlov, Yevgeny Minchenko and Firdus Aliyev, with close links to the Kremlin.

Similar to, but distinct from, these awards are several professional ratings and rankings of individual political technologists.⁷¹ The first of these appeared in 2003 as the “top 10 masters of political consulting” published by the the *Izbass* Internet portal. Today, there are several rankings of top political technologists or political consultants (on an annual or quasi-annual basis), including those by:

- **APEK (Agency for Political and Economic Communications).** A Russian political and sociological company created in 2004, that is known for its ratings of politicians, heads of constituent entities, and political consultants.⁷²
- **Obshchaya Gazeta (OB).** OB defines political strategists and political consultants as “people who ‘make’ politicians the way we see them, also ideologists and organizers of political processes and election campaigns.”⁷³ Head of OB is political technologist Alexander Roshchin.⁷⁴
- **Noviye Izvestiya (NI).** NI underwent ownership changes in 2016, becoming a pro-Kremlin news outlet.⁷⁵ Its 2022 rating of political technologists is described as a ‘reputation rating’ because it included political strategists, internet technologists, employees of pro-Kremlin autonomous non-profit organizations, public speaking specialists, political commentators, politicians, vice-governors, and even ‘customers’ of these services.

None of the detailed methodologies used for selecting top political technologists are published. However, the process appears to involve sending questionnaires or conducting surveys with selected groups of experts—e.g. current politicians, political strategists, political scientists, and journalists. These participants are then asked to name the top X-number of political strategists. The rating is then compiled based on the frequency with which names are mentioned.⁷⁶ It is worth noting that these rankings are not unbiased. For example, APEK is headed by Dmitry Orlov, who also appears as one of the named top political technologists.

Synthesising the three lists, we can construct a reasonable picture of who are the most influential and powerful political technologists according to their peers. Several individuals feature in all three lists, including: Yevgeny Minchenko (President of RASO), Grigory Kazankov (president of RAPK), Igor Mintusov (co-founder of Niccolo M), and Andrey Tsepelev (President of AIT).⁷⁷ Especially striking is that despite not being listed as a member of any of the professional associations, the aforementioned head of the Social Design Agency Ilya Gambashidze is highly ranked on two of the lists. He is the only political technologist to feature in this way.

71 <https://cyberleninka.ru/article/n/ya-protivnik-rezhima-no-vsegda-rabotayu-na-edinuyu-rossiyu-ili-o-polittechnologicheskomo-soobshchestve-v-sovremennoy-rossii>

72 <http://apecom.ru/about/>

73 <https://obshchayagazeta.eu/ru/article/124481>

74 See here: <https://politcom.ru/20623.html>; and here <https://www.rusprofile.ru/id/1018180>

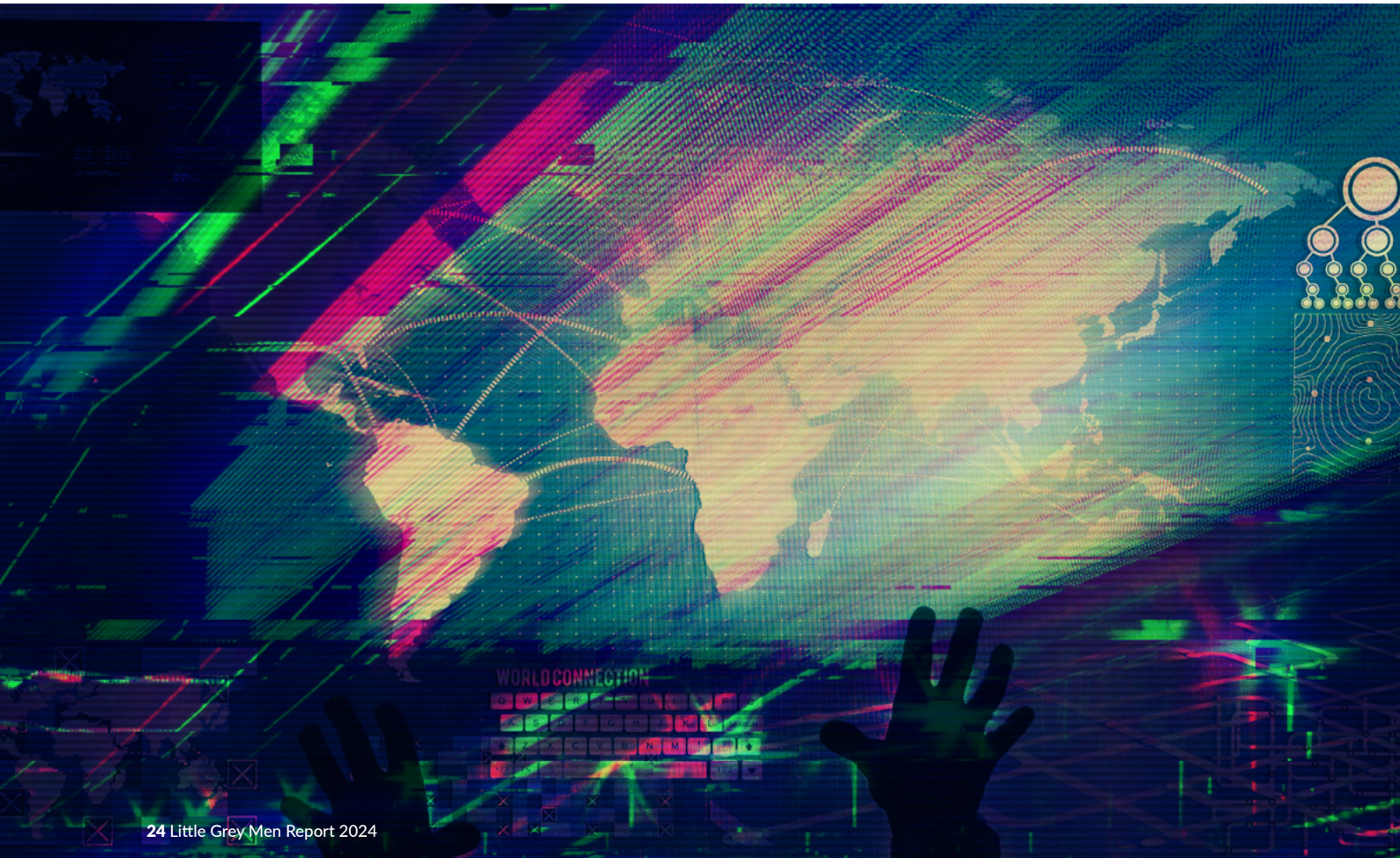
75 <http://besttoday.ru/posts/14667.html>

76 <https://obshchayagazeta.eu/ru/article/124481>

77 <https://fedpress.ru/person/1893448>

HISTORICAL AND GLOBAL APPLICATIONS OF POLITICAL TECHNOLOGY: **THREE CASE STUDIES OF POLITICAL TECHNOLOGY IN ACTION**

To understand how and why political technology has become such an important instrument of the Kremlin's approach to influence engineering and public diplomacy, three case studies are presented. The first of these examines how research conducted nearly a decade ago now, including during the Brexit campaign, is being used to train the next generation of 'information warfare' specialists. The second case shows how the insights derived from political technology are being used to identify, target and exploit contemporary political developments in Germany. A third case study turns to Africa, to illuminate some elements of how Russia is seeking to expand its global reach and influence.



CASE STUDY #1:

■ Brexit & the UK

The preceding analysis highlighted several individuals influential within the professional community of political technologists. Yevgeny Minchenko is clearly a leading ‘public face’ of the profession within Russia today. However, researching his professional background suggests he is more intriguing—and potentially significant. Specifically, in 2015-2016 he was working overseas, including in the UK, where he was directly engaged with the Brexit referendum campaign.

Open-source research identifies that he was, by his own account, ‘on the ground’ in London, conducting ‘participant observation’ in the immediate lead-up to the referendum. This included, on the day of the Brexit vote, taking a photo of a polling station in Mayfair and sharing it with his followers online. It is potentially noteworthy that previous research into the 2014 European Parliamentary Elections identified exactly the same behaviour performed by an individual with suspected links to the Internet Research Agency, but this time in Greece.



Photos posted from London, 2016.

Minchenko has conducted extensive and detailed study of British political and electoral processes and institutions, as well as the polling techniques and technologies used to try and ascertain voter preferences. A key passage in one of his reports on Britain discusses how he had been provided with ‘internal sociology’ survey material by “a number of headquarters”, including data from YouGov, Lord Ashcroft Polls, BBC, Ipsos-MORI, ComRes, ICM, Populus, and TNS-BMRB.⁷⁸ In December 2014, not long after Russia’s invasion of Crimea, Minchenko hosted an invitation-only event at Chatham House in London, detailing his research into Russia’s elites. Between March and May 2015, Minchenko was again in the UK using the material he collected as the basis of a report entitled *“How elections are won in the USA, Great Britain and the European Union: analysis of political technologies.”* The main aim of this publication is described as: “to understand the dynamics of electoral processes in the United Kingdom through the analysis of political technologies that were used by parties and their candidates to gain victory”.

78 https://web.archive.org/web/20150822141913/https://minchenko.ru/news/news_101.html.



Part of the method for achieving this goal was a survey of experts, including politicians, campaign staff, political consultants, and journalists. Twenty-three individuals are named in the document, with a number having links to both the Conservative party and Russia. Several are personally thanked including a member of the House of Lords and a politician who worked on Conservative Party election campaigns, and closely with two recent Prime Ministers.⁷⁹ Elsewhere, there is a photograph of Minchenko meeting a very senior Tory election campaign strategist.⁸⁰

One of the co-authors of Minchenko's 2015 UK report, Vladimir Kornilov, had complained in Russian state media six months prior that Ukraine was presenting itself as a victim, when in actuality it was the aggressor. In support of this view, he invoked his boss, Minchenko, on the Russian invasion of Ukraine:

“And again, no one in Ukraine thinks: aren't they telling lies on our ears both about the 'aggressor' and about the hordes of 'Russian spies'? It would also be nice for those who are responsible for this noodle to answer the question formulated by Russian political scientist Evgeniy Minchenko: Top officials of Ukraine have repeatedly publicly stated that the Russian Federation is waging a war against Ukraine. Is this a reason for the Russian Foreign Ministry to appeal to the Ministry of Foreign Affairs of Ukraine for clarification whether Ukraine considers itself to be in a state of war with the Russian Federation? If it turns out that it does not, then is it possible in this regard to propose stopping such irresponsible statements? And if it turns out that it does, then what?”⁸¹

Drawn together in this way, this material shows how the development of Russia's political technology as a foreign policy instrument has been directly informed by extensive and careful study. This is both in terms of researching and understanding the political cultures being targeted, but also the methods and techniques of influence used within them. Learning from these has been extracted and integrated with the methods and understandings already known to the political technology tradition in Russia. For example, there is evidence that Minchenko and others were extremely interested in the approaches used by Cambridge Analytica. However, the above material also raises several other important questions. First, how was Minchenko able to gain access to and cultivate extensive contacts with such senior figures whilst asserting that Russia had not invaded Ukraine? Second, what other activities was he engaged in during his period of 'participant observation' in the UK leading up to the Brexit vote?

Looking across the interests and approaches of individual political technologists, it is clear some are more 'applied' and 'activist', where others are more academically minded. Minchenko definitely fits in the latter grouping. This is reflected in the type of political technology services he now provides. One of his most cited

79 <https://bullpenstrategygroup.com/newsroom/team/nick-vaughan/>,
<https://www.buzzfeed.com/alexwickham/boris-johnson-downing-street-advisers>,
<https://bullpenstrategygroup.com/newsroom/nick-vaughan-joins-bullpen-strategy-group-in-london/>
80 <https://web.archive.org/web/20150401183646/https://www.chathamhouse.org/event/elite-politics-russia-politburo-20>
81 https://minchenko.ru/press/press_3034.html



products is 'Image 2:0', described as a "method" and a "framework",⁸² for systematically deconstructing the "image of a leader" into 17 archetypal images: Child, Orphan, Simple Man, Soldier, Warrior, Caretaker, Seeker, Rebel, Hero, Lover, Creator, Ruler, Governor, Jester, Mage, Wise Man, Fool.

Minchenko has observed that: "all of the archetypal images are effective in different contexts. There are no "good" and "bad" archetypes. They are more or less in demand depending on the state of society, the current emotional background, and the elite situation." There is evidence that Image 2:0 technology has been used to outline the 'best archetypes' of heads of regions, in preparation for regional elections in 2023: "The head of the Republic of Sakha (Yakutia) Aisen Nikolaev is approaching the decisive stage of the campaign in the image of the 'Ruler', having managed to achieve a noticeable consolidation of the political forces of the region."⁸³

Minchneko claims this image modeling and profiling has been used for "more than 100 politicians in 3 countries" and has received "practical confirmation of its effectiveness in elections of different levels, in environments with a diverse mentality". This kind of 'remote' psychographic profiling of senior leaders has been historically more popular in Russia than it has been in the West. It appears now to be a key element of the toolkit used by some political technologists.

Most recently, Minchenko has been named as one of a number of individuals engaged in a new Masters degree program "Information Influence Strategies in International Relations" that will open at the Moscow State Institute for International Relations (MGIMO), within the Faculty of International Relations, in September 2024. The new program's mission is "training specialists in information warfare", where students will study: how to influence target audiences, taking into account the political and economic context of international relations; and how to implement influence strategies on various audiences, including allies, neutral countries and opponents. Significantly, this new course is being implemented with the direct support and involvement of the Presidential Administration, and will be highly selective, accepting only 15-20 students per year. Presumably, Minchenko will be able to draw upon the first-hand knowledge and experience he gained from his travels to the UK and USA.

A plausible interpretation of these recent developments is that they signal how expertise in political technology and its craft and methods is perceived increasingly important to how the Kremlin, and specifically the Presidential Administration, is conceiving its operational geopolitical strategies. The establishment of this course and the clear intention to recruit directly from it into the governing apparatus around President Putin, likely has longer term implications.

82 <https://t.me/MinchenkoConsulting/883>

83 https://minchenko.ru/netcat_files/userfiles/Gossoviet_XIV

CASE STUDY #2:

■ European Elections & Germany

Just prior to his engagement with the Brexit referendum and trips to the UK, Minchenko had authored a similar report on the 2014 European Parliamentary elections. Both reports were paid for by the Russian non-profit Institute of Socio-Economic and Political Research (ISPER). A 2014 executive order issued by President Putin authorised the Institute to disperse state funds to non-governmental organisations. An investigation by media outlet RBC in 2016 alleged the Institute is a vehicle to fund Putin's Popular Front (ONF) movement, as three of the board members are leading members of Popular Front, describing it as: an "outsourced think tank" for managing the internal policy of the presidential administration.⁸⁴

One of the main tasks of the ISPER was developing key tenets of a conservative ideology for Russia. They organised the "Berdyayev Readings" forum, after Berdyayev was quoted in a speech by Putin. The 2015 forum (held at the same time Minchenko was writing his UK report) invited guests from outside Russia. Marie Le Pen's closest advisor at the time, Emmanuel Leroy, gave a speech stating that: "the current conflict in Ukraine was a continuation of The Great Game against Russia." The "Anglo-Saxon oligarchs who stood behind the ascent to power of the Nazis and the Bolsheviks", he insisted, are behind the 'color revolutions' in the former Soviet empire.⁸⁵ The fifth Berdyayev Readings forum was held in Paris the following year. It is likely that Russia used this series of meetings to network with far-right organisations throughout Europe.

More recently, looking towards the 2024 European Parliamentary elections, the political technologist Artem Sokolov profiled German voters using local polling data for regional elections to make informed predictions of future coalition government prospects.⁸⁶ In his analysis he highlighted Sahra Wagenknecht and her new anti-immigration, anti-Ukraine and anti-sanctions on Russia, party. Sokolov predicted that she will be able to steal voters from both rightwing AfD and leftwing Der Linke candidates, evaluating her key success factors as being: uniting the left and right in terms of party ranking and damage to competitors; the demographic appeal of the new party relative to her old party in terms of voter characteristics such as age, wealth and political leanings; and how palatable she is to the public and her appeal as a viable coalition partner to mainstream parties, unlike the AfD. Wagenknecht's ex-husband Ralph Niemeyer (who was/is under investigation for his part in a plot to overthrow the German government) claims to have had meetings with top level Kremlin officials in Moscow where it was clear to him that certain people in Russia would have an interest in a union between Wagenknecht and the far right.

There are connections here to the Washington Post reporting of leaked Russian documents showing the Kremlin's plan for Germany. The Washington Post article claims that the documents record meetings between the Kremlin and 'political strategists' (we don't know the actual word used but "Политтехнолог" is often translated as political strategist instead of political technologist). The Kremlin's orders were for those 'strategists' to focus on Germany to build antiwar sentiment in Europe. The Washington Post notes that: "soon after the Kremlin gave the order for a union to be forged between Wagenknecht and the far right, AfD deputies began speaking in support of her in parliament and party members chanted her name at rallies. Björn Höcke, chairman of the AfD in Thüringen in eastern Germany, publicly invited her to join the party."⁸⁷

84 <https://www.rbc.ru/investigation/politics/10/03/2016/56e032829a79470e5a4ef173>

85 <https://www.thedailybeast.com/marine-le-pens-closest-advisor-comes-out-of-the-shadows-in-donetsk>

86 <https://t.me/vorotnikovmemory/316>

87 <https://www.washingtonpost.com/world/2023/04/21/germany-russia-interference-afd-wagenknecht/>

By combining these materials, a chronology of the series of key events concerning the Kremlin's use of political technologies targeting Germany can be constructed.

Jul 13th 2022 First Deputy Head of the Russian Presidential Administration Kiriyenko assembles a group of political technologists at the Kremlin, telling them that Germany will be the focus of Russian efforts to undermine support for Ukraine in Europe.

Sep 20th 2022 Three AfD lawmakers travel to Russia and plan to visit Donbas, but are forced to return to Germany after a public outcry.⁸⁸

Sep 2022 Niemeyer travels to Russia allegedly to 'negotiate' a new unofficial German gas supply contract with Russia through Nord Stream 2, in order to put pressure on German Chancellor Scholz. After Nord Stream 2 is damaged, he returns to Russia and it is claimed received an encrypted phone for communicating directly with Russian Press Secretary Peskov.

Nov 2022 AfD member Petr Bystron travels to Belarus for three days. Once exposed in the media, he claimed the trip was to meet with the Belarusian foreign minister. Just prior to Russia's full-scale invasion of Ukraine, he also travelled to Kyiv to meet with Putin ally Viktor Medvedchuk who was under house arrest.

Apr 2023 Niemeyer spends another two weeks in Russia, claiming that if there were early elections in Germany, Russia would immediately support Wagenknecht.

Intriguingly, the plan for Germany devised by the political technologists had specific measurable objectives of success in the short and longer-term. These included:

Boosting pro-Russian sentiment in Germany by 10% in only three months.

Wagenknecht's new party winning "a majority in elections at any level."

AfD popularity in polls to rise above the 13% it had at the time.

A range of methods were set to deliver these objectives, including the use of troll farms to shape social media traffic, protests over energy prices and political graffiti to attract media attention. To demonstrate their effectiveness to the Kremlin, the political technologists engaged in the project used a dashboard to show the reach of their social media accounts. Specific reference is made to the use of Telegram and a YouTube talk show.

CASE STUDY #3:

■ Africa & Government Relations

Since the death of Yevgeny Prigozhin in August 2023, the roles played by other individuals in the design and delivery of Russian foreign policy have become easier to discern. One such is Andrey Gromov, who is the head of an organisation called GR-Group. GR-Group claim to have operated for over 15 years and to have worked in 52 countries. According to their website, operations are varied and include the organisation of political campaigns and facilitating business relations across multiple sectors with government.⁸⁹ For the purposes of this report, the key featuring of Gromov's operations is that they directly seek to influence political and economic processes.

GR-Group define themselves as 'Government Relations' specialists, which appears to be an adjunct role to that of the political technologist, especially when operating in international contexts. Government Relations specialists are presented as project managers who oversee processes in order to exert influence on a public body that would seek to build a "...system of interaction of a business with a Government."⁹⁰ Thus they seem to come into play when the Kremlin is trying to broker new relationships with a foreign government, in order to sell services to that regime; often 'information control' services, and military and paramilitary capabilities. It appears that the Government Relations specialist acts as a pathfinder identifying opportunities with a foreign power, and it is the role of the political technologist to realise these opportunities by devising strategies and plans, helping to deliver these.

Previously, Gromov had links with Yevgeny Prigozhin's wider operations having acted as an election observer in DR Congo as part of the Prigozhin linked organisation AFRIC in 2018.⁹¹ AFRIC was initially established by a number of individuals associated with Prigozhin's 'back office', including Petr Bychkov and Yulia Berg (both of whom are currently sanctioned^{92 93}).

Whilst AFRIC presented as an authentic African initiative, it was a 'front organisation' seeking to influence African politics in support of Russia's foreign policy goals. This was to be achieved through inauthentic election observations, 'expert' opinion from pro-Russia individuals sourced from around the globe and self-published reports⁹⁴. AFRIC, it was claimed, would operate as a "network of agents of influence" involving 'experts' from African countries, funded through anonymous donations in cryptocurrencies, to obfuscate the source of the organisation's funding.⁹⁵

Subsequent to his work with AFRIC, Gromov established 'the Renaissance Foundation' based in Moscow. This entity is focused on promoting Russian involvement in occupied areas of Ukraine. According to their website the foundation provides direct humanitarian assistance on the ground in Donbas, as well as "patriotic education" and "methodological support from its volunteers". It also arranges visits by pro-Russian European nationals, who were previously involved in AFRIC, and who are presented as experts in various governance matters.⁹⁶ These visits appear designed to give the impression of international support for the foundation's work and the occupation more broadly. It is notable that many of the same individuals appear at different events in support of different causes.

89 <https://gr-group.site/>

90 Teteryuk, A.S., Kovalev, N.A., n.d. The Emerging Field of GR-Management in Modern Russia: State of Science and Profession 31.

91 <https://web.archive.org/web/20191102162244/https://afric.online/projects/international-election-observation-mission-report-in-dr-congo-of-december-30th/>

92 <https://www.opensanctions.org/entities/NK-LPf4vhwReUHCXFEyLrTWzR/>

93 <https://www.opensanctions.org/entities/NK-UiwDqYmgBEQRSWT8Phb25F/>

94 Shekhovtsov, A (2019) Fake Election Observation as Russia's Tool of Election Interference: The Case of AFRIC. Berlin, EDPE.

95 Shekhovtsov, A (2019) Fake Election Observation as Russia's Tool of Election Interference: The Case of AFRIC. Berlin, EDPE.

96 https://t.me/oddr_info/52796



Gromov is closely linked to former Prigozhin employee Yulia Berg who has established similar front organisations, although it appears her work is more concentrated on elections and political influence. Berg also previously held a high-ranking position within AFRIC⁹⁷, but founded and now runs GlobUs, which again presents as a think-tank, offering 'expert' opinion on a range of issues, focused primarily on advancing Russian interests in Africa⁹⁸. Both GlobUs⁹⁹ and the Renaissance Foundation¹⁰⁰ have been involved in part-funding English language documentaries on the Ukraine conflict with other pro-Russia organisations.

Berg has participated in a recent podcast hosted by former RT contributor Patrick Henningsen.^{101 102} Additionally, whilst their focus appears to be largely directed towards Africa and occupied regions in Ukraine, both Berg and Gromov were involved in a December 2023 conference on Russian involvement in Afghanistan and the normalisation of relations with the Taliban. This event was attended by Russian government officials and former Wagner employees.^{103 104 105}

The point of focusing on individuals such as Gromov and Berg, in the context of this report, is twofold. First, they help illuminate how the role and work of political technologists intersects with the functions of several other allied professions. Second, and perhaps more importantly they help connect a sense of past, present and future in terms of how political technology is conceived of and conducted within the Russian system. Indeed, one of the key legacies of Yevgeny Prigozhin may prove to be that his organisations and their influence operations were where many (but certainly not all) of today's political technologists gained their formative experiences. Moreover, following Prigozhin's demise, it appears that many of these same individuals are assuming responsibility for taking forward aspects of the political, cultural and economic influencing work that he previously performed in regions of interest, such as Africa.

97 Shekhovtsov, A (2019) Fake Election Observation as Russia's Tool of Election Interference: The Case of AFRIC. Berlin, EDPE.

98 <https://globus.expert/globs>

99 <https://www.youtube.com/watch?v=A9vBtkfX2Jg>

100 https://t.me/vozhrozhdenie_org/22

101 <https://www.rt.com/op-ed/authors/patrick-henningsen/>

102 https://www.youtube.com/watch?v=zX1dt_4J4nQ

103 https://t.me/max_shugaley/911

104 <https://www.afghanwitness.org/reports/'playing-on-both-sides'%3A-russian-manoeuving-in-afghanistan-on-the-rise>

105 <https://globus.expert/tpost/tkkaem4r41-humanitarian-policy-and-soft-power-appro>



■ DIRECTION AND CONTROL FROM THE KREMLIN

Significant information regarding the work and techniques of several political technologists has been given in the preceding sections. This raises a final question: how they are tasked and managed by the Kremlin? Understanding these issues provides insight into how the Russian government plans to construct and communicate information operations and disinformation campaigns. Notably, SDA/Structura and several other political technologists included here are commercial companies that actively assist the Kremlin in achieving its goals in both foreign and domestic affairs.

According to Kremlin documents acquired by a European intelligence agency and made available to the Washington Post in February 2024, Putin's administration gave orders to a group of Russian political strategists to use social media and fake news articles to threaten the territorial integrity of Ukraine. More than 100 documents describing the conduct of "information psychological operations" were reviewed by journalists.¹⁰⁶ The principal aim was to divide and destabilise Ukraine by propagating disinformation within Ukraine and across Europe. For example, one goal was to heighten the hostility between the then-top military commander, Gen. Valery Zaluzhny, and the "hysterical and weak" president of Ukraine, Zelensky by spreading speculation of confrontations between the two men and Zaluzhny's impending dismissal for being too dangerous. The documents reported on by the Washington Post suggest that Gambashidze's group started producing content for Ukrainian social media networks in February 2024. However, it is worth highlighting that both RRN and the spoofed Western media network were active on this issue for a number of months prior to this date.

The same documents trace the lineage of these orchestrated information operations to Sergei Kiriienko. Kiriienko had a brief tenure as Prime Minister in 1998 and was formerly general director of Rosatom before being appointed first deputy chief of staff at the Presidential Administration (AP) in October 2016. At the Presidential Administration, Kiriienko oversees the Kremlin's internal political bloc, with responsibilities for personnel issues, youth policy, preparation and conduct of elections, and interaction with political parties and public organisations. Having persuaded Putin to proceed with elections at home during Russia's full-scale invasion of Ukraine, his role expanded in scope and influence to become the so-called 'Kremlin curator of Donbas and the occupied territories of Ukraine', effectively replacing deputy head Dmitry Kozak.

Along with overseeing 'referendums' across the occupied territories regions of Ukraine, Kiriienko ran a group of political technologists and strategists to create a presence on Ukrainian social media in January 2023. Here the intention was to spread disinformation to undermine the territorial integrity of Ukraine. Documents show Kiriienko laid out four key objectives for the Ukraine propaganda team: (1) discredit Kyiv's military

106 Belton, C. (2024) 'Kremlin runs disinformation campaign to undermine Zelensky, documents show', Washington Post, <https://www.washingtonpost.com/world/2024/02/16/russian-disinformation-zelensky-zaluzhny/>

and political leadership; (2) split the Ukrainian elite; (3) demoralise Ukrainian troops; and (4) disorient the Ukrainian population. Key performance indicators set were lowering public trust ratings of key personnel in Zelensky's office, the Ukrainian government, and the command of Ukraine's armed forces, and increasing the belief among the Ukrainian population that the country's elite was working only for itself. A rising number of government dismissals and public conflicts would also be a signal of success. To increase fear and anxiety, Ukrainian war losses were to be exaggerated.

The team Kiriienko assembled to focus on destabilizing Ukraine was headed by a close deputy at the State Council department of the Presidential Administration who reports directly to him, Alexander Kharichev. Kharichev is known in Moscow for being a 'fixer', ensuring elections go in the Kremlin's favour and is now in charge of shaping Russia's post-war image. There are reports that Ilya Gambashidze has a "proven devotion" to Kharichev. Another "warm friendship" that Gambashidze supposedly has is with Sofia Zakharova, an employee of the Presidential Administration's Information and Communication Technologies directorate. Kiriienko allegedly appointed her (under the leadership of Tatiana Mateeva) to head a European propaganda group for additional informational projects undermining Ukraine. It is because of these personal connections and networks that it is thought that Gambashidze and the Social Design Agency have been increasingly able to secure closed, non-competitive funding contracts from the Presidential Administration.

Gambashidze and the alleged 'brain' of the Doppelgänger operation Zakharova are collaborated on costed country plan concepts for Israel and Ukraine.¹⁰⁷ Separately it is reported that Gambashidze was awarded the contract for providing media support to Viktor Medvedchuk's, "Other Ukraine" project, at prices inflated in the magnitude of 300%. Documents shared by anonymous Telegram channel VChK-OGPU, for example, show: a budget of 200 to 300 thousand Rubles for each two-minute episode of a series "Two Godfathers"; and to represent "Other Ukraine" in social networks 3,000,000 Rubles per month for 10 sites, 500 publications per month.¹⁰⁸ These amounts stand in marked contrast with publicly available data from the Russian Federal Tax Service that show between 2020-21/22, Structura and SDA were in receipt of only very modest state funds (approximately 1.2K Sterling).

Drawing up and implementing country plans for information operations is not the sole connection that Gambashidze and his associated companies have to the Presidential Administration. During the 2024 Russian Presidential elections, and firmly within Kiriienko's purview, Gambashidze and his team were appointed as political technologists to the Liberal Democratic Party (LDPR) campaign, building on his previous election experience in Kalmykia and Tambov. With LDPR Presidential candidate Slutsky ultimately polling in last place with 3.2% of the vote, it is reported that the Gambashidze-LDPR relationship was turbulent. However, the day after election day, when Putin's victory was clear-cut, Structura and SDA were credited with the creation of a jovial video from Tambov, in English, celebrating Russian elections. This video was placed on X within 24 hours of the Russian elections closing. Doppelgänger bots boosted it in replies, including to content trending at the time about Kate Middleton, so maximising the audience who saw it on their timeline.¹⁰⁹

Drawing back from these tactical details, the key point to be made concerns how political technology organisations such as SDA/Structura have been in receipt of multiple grants and funding awards from the Russian state over several years. This has involved direct operational funding, but also investing over the longer term to develop their capacity and capabilities. For example, state funds awarded to them in 2019 to develop 'chatbot' technologies probably trace through to 'Cyber-Zhirinovsky'. Relatedly, we can return to Minchenko's activities in London in 2015-16 to make a similar point. Albeit the role of political technologists has been growing increasingly influential within the Kremlin system, this is not a sudden emergence. Rather it has been propagated and developed over a number of years, supported by strategic investment in the organization and conduct of information-influence operations.

107 Seibt, S. (2024) 'Ilya Gambashidze: Simple soldier of disinformation or king of Russia's trolls?' France24, <https://www.france24.com/en/europe/20240228-ilya-gambashidze-simple-soldier-of-disinformation-or-king-of-russia-s-trolls>

108 <https://rosinform.press/v-ap-rf-snova-vzylis-za-ukrainskij-vopros-i-proekt-medvedchuka/>

109 Coughlan, S. and Spring, M. (2024) 'Kate rumours linked to Russian Disinformation', BBC, <https://www.bbc.co.uk/news/entertainment-arts-68637136>

■ ‘LIVING OFF THE LAND’: HOW POLITICAL TECHNOLOGISTS ARE INNOVATING THE DESIGN AND DELIVERY OF INFORMATION OPERATIONS

In terms of understanding the role and position of political technology within the Kremlin’s overarching propaganda, disinformation and information operations system, not only do we need to look ‘upwards’ in terms of how they are directed and controlled by those in political power, but also ‘downwards’ and how the plans they devise are implemented and operationalized by the trolls farms and others engaged in similar efforts.

This is an area where the increasing involvement of the methods and approaches devised by influential political technologists, such as Gambashidze, appear to have had an important influence upon the design and delivery of information operations. In sum, this has involved the pioneering work of the Internet Research Agency ceding ground to what might be summarized as a ‘living off the land’ methodology.

‘Living off the land’ (LOTL) is a special forces concept describing how operations can be extended and sustained by encouraging military operators to harness and exploit local resources. In the cyber-security world this idea has been adopted and adapted to label attacks that are more agile and sustained because they target vulnerabilities and weaknesses within a targets’ system, rather than importing lots of files into it. A similar rationale and logic can be observed in recent Russian digital influence campaigns, particularly those launched since the commencement of the war in Ukraine. Informed by the empirical research and methodologies devised by political technologists, influence engineering operatives are better able to leverage and exploit assets and tensions in the communities and countries being targeted.

The first manifestation of this is in terms of the operatives involved in delivering an information operation. Prigozhin’s Internet Research Agency (IRA) functioned as a fairly standard bureaucracy with different departments responsible for working specific social media platforms and/or defined geographic regions and employees subject to performance measures. However, the more recent LOTL approach uses a more participative model. This was pioneered by the emergence of ‘Cyber Front Z’ in St Petersburg shortly after the commencement of Russia’s armed invasion of Ukraine. Cyber Front Z had far fewer employees than the IRA. Moreover, whereas the IRA workers were developing and running fake social media accounts themselves, Cyber Front Z were engaged in encouraging ordinary Russian citizens to get involved in online activism. Their key actions involved ‘brigading’ other social media users. Brigading is a particular form of digital activism involving the mass deployment of online accounts in a coordinated fashion against a nominated target at the same moment in time. Cyber Front Z launched multiple brigading actions against the social media presences of senior political figures in the UK and Europe. They also engaged in ‘targeted trolling’ of ordinary users who had posted messages they did not like, for example those criticizing President Putin. Essentially, what they were doing was urging common Russian citizens to take part in these activities as a patriotic obligation to aid the war effort.

The second shift associated with this LOTL approach to information operations focuses on the operational assets required to deliver a covert influence campaign. Again, a key point of contrast is the IRA, who invested considerable effort in building website presences, constructing fake online personas, building audiences and followers for these over extended periods of time and across multiple social media platforms. More recently, rather than building themselves, Russian operators have been using an array of normal ‘paid for’ online



services to execute their digital influencing efforts. These include sites that allow you to purchase batches of social media followers and disused social media accounts with most of their follower lists still intact. There are similar services for website construction, which are also for sale with their backlinks intact, greatly assisting with search engine optimization. Another service Russian operated accounts have been accessing promises to 'crack the passwords' associated with particular digital account identities, for a fee. The point is that, rather than doing all this themselves, by purchasing these services Russian operatives need fewer technical skills and can get an operation up and running more quickly and at scale. This increases their overall efficiency and effectiveness in getting their content to target audiences. The US Department of Justice documents evidence of an increasing accent on systematic monitoring of 'organic' social media traffic and the behaviour of online influencers in an effort to identify content that aligns with political technologists' strategies, and can be manipulated to amplify discord and doubt in a targeted audience segment.

An intriguing sidenote about these activities is that they appear to be integrating monetization mechanisms. Ordinarily, these are used by social media influencers to generate income through advertisement revenue according to the number of views and clicks their content is achieving. But why might state-backed information operations also be utilizing such devices? One possibility is that those running the operations are 'grifting' and developing a 'side hustle' to boost their personal incomes. After all, Russia's economic system is renowned for its corruption. A second possible explanation is that these monetization efforts are being used (at least partly) to offset the running costs of information operations. War is expensive. In an environment where there is acute competition for state resources, it is entirely plausible that commercial suppliers are being commissioned to design and run influence campaigns on the grounds that they can keep any income they are able to generate in the process. This operating model reduces the need for central funding.

Critically, the cumulative impact of each of these LOTL innovations is that they also increase the level of obfuscation, limiting the ability of Western analysts to confidently attribute discovered activities to a state actor. It can also circumvent potential control measures if, for instance, digital activism is being performed by patriotic citizens using their own 'organic' social media accounts. It becomes harder for social media platforms to legitimately act against them when most of their policies are predicated upon responding to 'coordinated inauthentic behaviour' or 'impersonation.' Likewise, paying for a variety of 'influence for hire services' and/or purchasing a cheap website, as do many thousands of ordinary businesses, is a pretty effective way of minimizing the possibility of detection and identification.

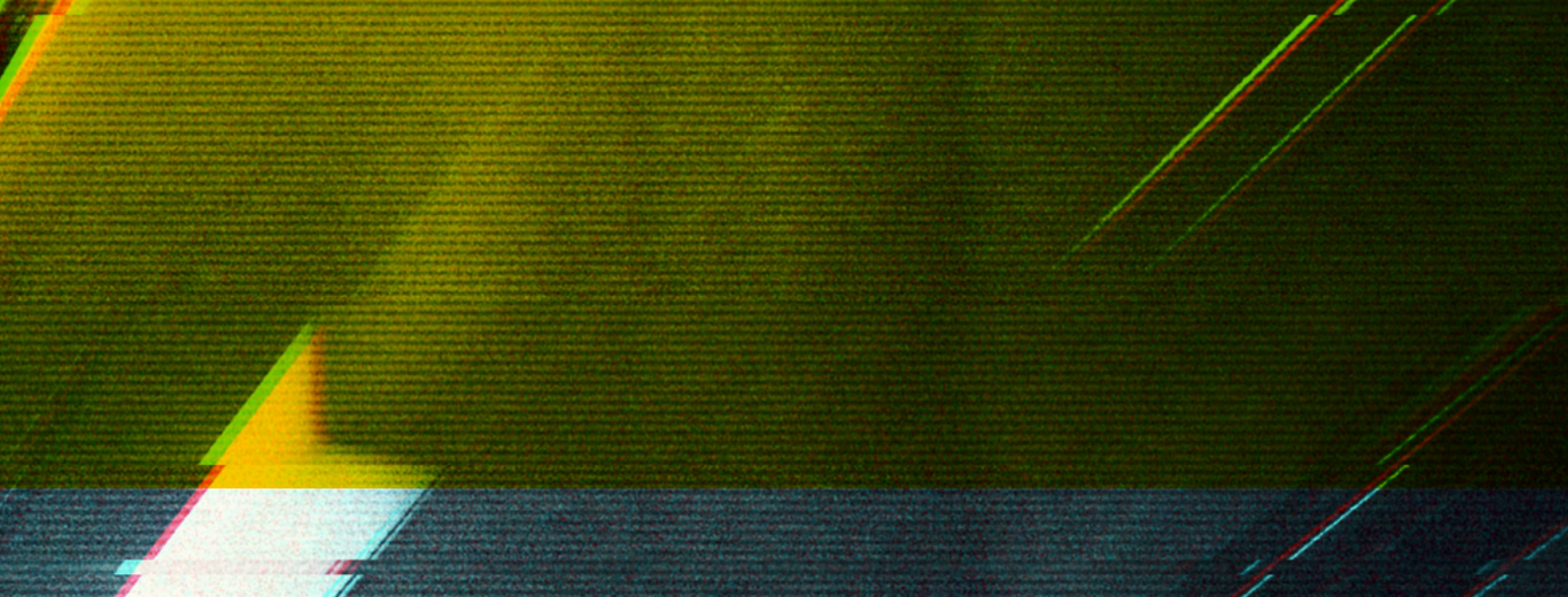


■ CONCLUSION: LAMINATED AND INTERACTING THREATS (OR ‘EVERYTHING, EVERYWHERE, ALL AT ONCE’)

We are in an ‘everything, everywhere, all at once’ moment. It is an inflection point where there are multiple, interacting security threats layering up upon one another at the international, national and local levels. These range from the wars in Ukraine and Gaza, where the former is also associated with increased discovery of both online and offline espionage cases, sabotage and cyber-attacks in many Western countries, and the latter is inducing regular protests in world cities that are posing public order challenges, as well as an uptick in hate crimes. Alongside this is the ongoing need to manage and mitigate the risks of terror attacks inspired by both radical Islamist and far-right ideologies. Overlaid are the polarizing political atmospherics associated with events such as the attempted assassination of the Prime Minister of Slovakia in May 2024. All of which are set against a backdrop where, at the time of writing, major democratic elections are in the process of being organized and conducted across a large number of countries, and malign interference in these processes is widely anticipated. These are conducive conditions for the deployment of political technologies.

Political technologists are consequently playing an increasingly influential and important role in the design and delivery of the Kremlin’s domestic and foreign policy strategies. Using a range of information control methods and digital influence engineering techniques, they are engaged in forms of influence, surveillance and social control that provide for ‘perception management’ and the ordering of peoples’ social realities. Some of their work is strikingly creative and innovative, blending experiential ‘craft skills’ with scientific insights about how to influence individual and group thoughts, emotions and behaviours.

Since the discovery of the Internet Research Agency’s attempts to interfere in the 2016 US Presidential elections, there have been a series of reports from Western analysts documenting a variety of different Russian information operations and disinformation campaigns. These target public understanding and political



decision-making across a variety of issues, contexts and situations. Collectively and cumulatively such efforts are designed to induce the disintegration of trust in key institutions and the deconstruction of social reality itself.¹¹⁰ To understand how this happens, this report has sought to shift the locus of analytic attention 'upstream' a bit. Rather than describing the tactics, techniques and procedures associated with individual information operations, it has instead started to outline how these campaigns are designed and delivered, and by whom. In so doing, one aim has been to help draw out how information manipulation and covert digital deception articulates with other forms of espionage and active measures, aimed at political, economic and cultural subversion.

Connecting that Russian political technologists have been systematically collecting data on social and political developments and trends in key Western countries to plot out potential interventions, with the fact the delivery methodologies for running such interference have been refined, is crucial in 2024 when there will be an almost unprecedented number of democratic elections taking place globally. It is this potentially combustible cocktail of tensions that makes 2024 different to what has come before in terms of exposure to and managing the fallout from foreign state information operations. In this sense, for political technologist-devised information operations to have an impact and effect, they probably don't need to be that sophisticated. They can simply nudge and amplify the disaffection and distrust already established and percolating in many Western countries.

Soon after they were originally detected, Meta disrupted both Doppelgänger and RRN across their surfaces. Likewise, the principals of the Social Design Agency and Structura have been exposed and sanctioned. But it is intriguing what happened after that. It appears Gambashidze's reputation within the Russian elite has been significantly enhanced by the imposition of these counter-measures. The Social Design Agency has attracted more work, including for the Liberal Democratic Party of Russia. Their work received an award at the 'Russian Association of Political Consultants' annual awards and political technologist social media channels assert that, by sanctioning him, the USA have given Gambashidze 'a medal.'

Disinformation, subversion and allied forms of information manipulation are not new social problems. In explaining their contemporary dynamics many accounts have attended to the role played by the technological affordances of a number of social media platforms. In this study, we have sought to shift the focus of attention a bit more 'upstream', to better understand the shaping effects of the arts, craft and science of political technology in terms of how such approaches are designed and delivered. The hope being that this enhanced understanding will enable others to construct better defences against these malign influencing efforts.

110 This deliberately co-opts and inverts the language of Peter Berger and Thomas Luckmann in their seminal book 'The Social Construction of Reality' originally published in 1966. Their work was motivated by an attempt to understand how a shared conception of social reality was possible. In attending to the work of political technology we are in many ways looking at how such understandings are attacked and decomposed.