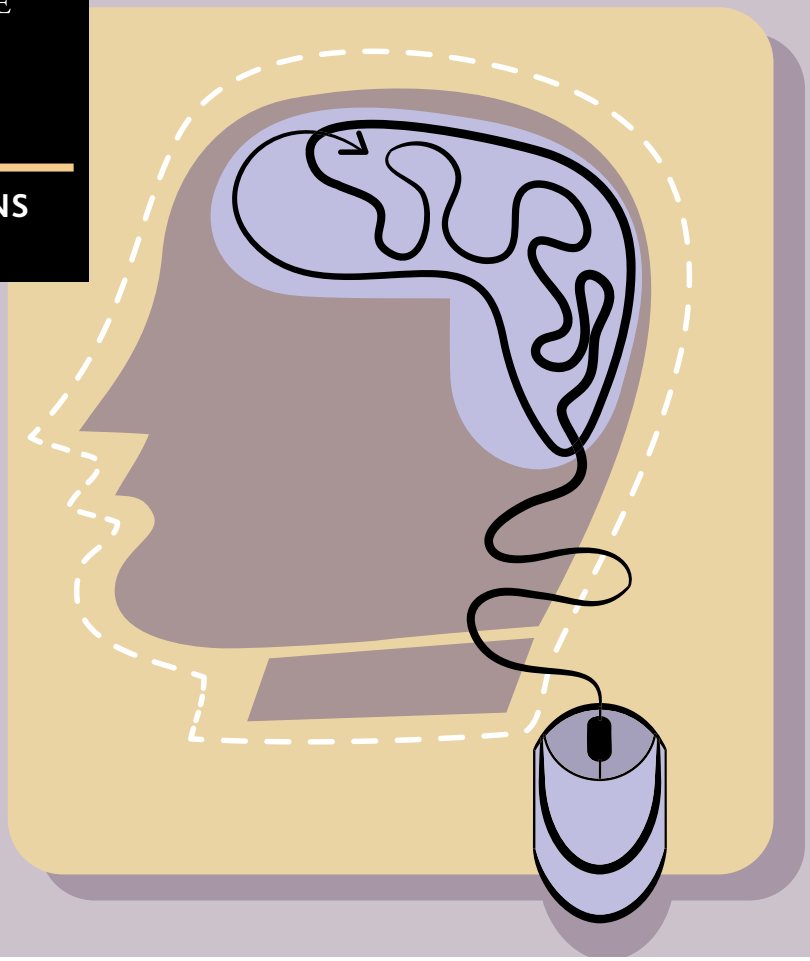
LEGATUM INSTITUTE

TRANSITIONS FORUM



BEYOND PROPAGANDA | NOVEMBER 2015

Cyber Propaganda

From how to start a revolution to how to beat ISIS

Introduction by Peter Pomerantsev

www.li.com
www.prosperity.com

ABOUT THE LEGATUM INSTITUTE

The Legatum Institute is an international think tank and educational charity focused on promoting prosperity. We do this by researching our core themes of revitalising capitalism and democracy. The *Legatum Prosperity Index™*, our signature publication, ranks 142 countries in terms of wealth and wellbeing.

Through research programmes including The Culture of Prosperity, Transitions Forum, and the Economics of Prosperity, the Institute seeks to understand what drives and restrains national success and individual flourishing. The Institute co-publishes with *Foreign Policy* magazine*, Democracy Lab*, whose on-the-ground journalists report on political transitions around the world.

The Legatum Institute is based in London and an independent member of the Legatum Group, a private investment group with a 27 year heritage of global investment in businesses and programmes that promote sustainable human development.

ABOUT THE BEYOND PROPAGANDA SERIES

The 21st century is seeing a new scale of media manipulation, psychological war and disinformation. The technological capacity of the information age, a more liquid use of ideology by authoritarian regimes, and the West's own difficulties in projecting democratic values have redefined the threat of propaganda. The Transitions Forum's 'Beyond Propaganda' series investigates these challenges and aims to identify solutions.

Find out more at **www.li.com/programmes/beyond-propaganda**

The Legatum Institute would like to thank the Legatum Foundation for their sponsorship and for making this report possible.

Learn more about the Legatum Foundation at www.legatum.org.

The Legatum Institute is the working name of the Legatum Institute Foundation, a registered charity (number 1140719), and a company limited by guarantee and incorporated in England and Wales (company number 7430903)

CONTENTS

Introduction 2
by Peter Pomerantsev

Ukraine: Dissident Capabilities in the Cyber Age 4
by Katrina Elledge

From Mullahs to Moscow: Propaganda in the Social Media Age 15
by David Patrikarakos

Islamic State Propaganda: Our Response to the Competition 24
by Charlie Winter

About the Authors inside back cover

LEGATUM INSTITUTE

INTRODUCTION

By **Peter Pomerantsev**

In Kiev, a young journalist makes a casual Facebook post calling for people to protest a government decision and it snowballs into a revolution, an invasion, and the end of the post-Cold War European order. In India, a You Tube video purporting to show a Muslim mob beating two Hindus to death causes mass riots which need 13,000 soldiers to quell. Later it turns out the original video hadn't actually shown a Muslim mob at all, it hadn't even been filmed in India: someone had put on a false caption on a You Tube video and started a riot. In the US, a tsunami of tweets reports a deadly explosion at a chemicals factory in Louisiana. The explosion never took place: Russian bots were looking to sow panic.

The internet has transformed propaganda. No longer do the state and media elites have a monopoly on public opinion—now anyone has the power to be their own Murdoch, Churchill, or Goebbels. This has empowered both crusading dissidents and the darkest sides of the ideological spectrum, posing new challenges for how democratic governments should respond and opening up new opportunities for states willing to mess with other countries' information environment.

Ukraine's 2014 Euromaidan movement was enabled by the power of the internet. As US Defense Department Analyst Katrina Elledge details, the internet allowed the revolutionaries to, *inter alia*, mobilise people through motivational material; document government crimes; share tactical information and training videos on everything from how to make Molotov cocktails to protecting personal information online; break the government's dominance of media by broadcasting the revolution live via video streams; organise self-defence units, hospitals, transport, legal advice and funding.

The internet has put governments, and authoritarian governments especially, on the back foot. But while they have had to surrender absolute communication control, many are learning how to use the internet to their own advantage. David Patrikarakos, author of *Nuclear Iran: The Birth of an Atomic State*, looks at how the regime in Tehran has gone from describing social media sites such as Facebook and Twitter as "enemy spaces" to experimenting with using the internet to attack dissidents domestically and spread the Islamic Revolution abroad.

Russia has also been experimenting with manipulating the global information environment. One "cognitive hack" saw Kremlin propaganda skewing Google's search function to the degree that if you typed "ISIS France" into it, the first recommendation was "ISIS France Support". "This happened," explains Patrikarakos, "not because of any genuinely high levels of support in France for ISIS, but because the most sophisticated algorithm in the world…was effectively hacked to produce this result." A Kremlin propaganda network had wrongly reported that one in six French people supported ISIS. The story was picked up by the news website *Vox* in the US, and quickly spread further.

Perhaps the most spectacular practitioners of online propaganda are ISIS. Though best known in the West for their gruesome, cinematic executions of prisoners, this is only a small element of ISIS' online propaganda output. "Understanding that different things appeal to different people is a crucial requisite for propagandistic success" argues Georgia State University's Charlie Winter. "For example, Islamic State is well aware of the fact that the vast majority of Sunni Muslims living in its environs are not ideological adherents … by placing strong emphasis on the caliphate's revolutionary agenda, unwavering penal code, services provision, and social welfare programmes, the group's propagandists are able to attract disgruntled populations at the same time as they make ideological entreaties to jihadist fanatics."

To counter ISIS effectively, believes Winter, democracies will have to take a leaf out of ISIS's book and learn how to speak to different audiences in different ways. The need for narrative variation is born out of the nature of internet technology; today's audiences are divided into online tribes with different agendas. This makes today's propaganda, and counter-propaganda, different to the twentieth century's, when one message could be blasted through a limited number of centrally coordinated media. Perhaps the greatest challenge going forward will be to connect the micro-messages delivered to each sub-group with a broader strategic narrative.

The issue is further complicated by the question of who should be doing the messaging. Are governments still credible? What is the responsibility of private companies, such as Twitter or Google, who carry the propaganda? They have helped create and massively profited from a technology whose potential for destruction we are only just coming to terms with. The start of the twenty-first century also saw a burst in information technology with the introduction of cinema and radio. Apart from all the good things they produced, they also made possible the promotion of totalitarian ideologies and allowed hate speech to reach and inspire millions.

LEGATUM INSTITUTE

UKRAINE: Dissident Capabilities in the Cyber Age

By **Katrina Elledge***

Social media greatly enhanced the capabilities of Ukrainian dissidents to wage a successful Euromaidan movement against former president Viktor Yanukovych in 2013–14. It was used to rapidly break the government's monopoly on mass media, proliferate images of regime abuse, recruit and organise a self-defence force, supply and sustain thousands of protesters, provide medical and legal aid, disseminate tactical information on internal troop movements, and conduct cyber-operations against the regime.

This paper presents selected findings from a study of approximately 40 social media networks active in strengthening and sustaining the Euromaidan movement from November 2013 to February 2014.

EUROMAIDAN AND SOCIAL MEDIA USAGE

There are two defining and interlinked features that distinguish Euromaidan as a new form of social movement in the Ukrainian context:

1. It was born on social media, quickly transcending to the occupation of physical space;
2. No one individual or organisation is credited with its birth.

While independent journalist Mustafa Nayem is often credited with jump-starting the movement by appealing on Facebook for a public protest against Yanukovych's refusal, on November 21, 2013, to sign an Association Agreement (AA) with the European Union (EU), the actual creator of the Euromaidan name, Facebook page, and Twitter handle and hashtags is nebulous and, most critically, unimportant.

At the outset of Euromaidan, Internet penetration in Ukraine was approximately 42 percent, compared to 6.6 percent in 2007. Access was significantly higher in cities. Smart phone usage was also increasing, but at just 10 to 14 percent it was still limited.[1] However, there was no obligatory registration, which allowed protesters to feel relatively anonymous. Public uncertainty over state surveillance, however, did prompt some self-censorship, particularly during periods of violence.[2] Nevertheless, Internet access under the Yanukovych government remained relatively unfettered prior to the start of Euromaidan. Despite some attempts at legislative restrictions on content and sporadic cyber-attacks against dissident sites, there were few known instances of the government either engaging in pervasive Internet monitoring or blocking access.[3]

While 52 percent of Euromaidan participants said they learned how and where to protest from traditional media, 37 percent received information through Facebook invitations.[4] Facebook outpaced its Russian competitor VKontakte (VK) as the most popular social media platform, largely because of its ability to reach a wider international audience.[5] Twitter also increased in popularity, particularly during and after the mid-January riots, as a result of its ease of use on mobile devices.[6]

*Disclaimer

All statements of fact, analysis, or opinion are those of the author and do not reflect the official policy or position of the Defense Intelligence Agency, the Department of Defense, or any of its components, or the US Government.

THE "HUB"

Euromaidan is an example of a horizontally networked movement operating around not one, but multiple hubs. The Euromaidan Facebook, Twitter, and VK accounts, created anonymously at the very outset of events on November 21, 2013, remained the most popular hubs of information, dissemination, and coordination—probably because they existed without the ownership or sponsorship of any one organisation or political party. While there were efforts to centralise the Euromaidan movement under the leadership of the opposition parties Fatherland, Ukrainian Democratic Alliance for Reform (UDAR), and Svoboda, these efforts were often disregarded. Unlike the 2004 Orange Revolution, the roles of opposition parties and non-governmental organisations (NGOs) were frequently questioned, marginalised, or at odds with each other. In part this reflected Ukrainian society's widespread rejection of the dominant role of hierarchical party politics, a shared distrust and disappointment over the failure of the Orange Revolution, and persistent corruption at all levels of formal institutions.

Non-aligned groups such as Civic Sector quickly emerged to offer an alternative for those wanting to participate in Euromaidan while remaining independent of a particular political party or organisation. At the peak of Euromaidan, Civic Sector participants were estimated to be around 150,000, but this number fluctuated widely as volunteers were free to participate in as few or as many activities as they desired.[7] Civic Sector maintained a visible presence on the Maidan and in social media with a 24/7 social media team managing accounts on Facebook and Twitter.[8] Volunteers frequently organised social media campaigns, spent time fact-checking content, and provided English-language translations.[9]

MARKETING EUROMAIDAN

Promotion and outreach are fundamental features of most social movements in order to mobilise followers, to gain international attention, and—increasingly in the age of social media—to crowdsource the movement's needs.[11] Multiple public relations (PR) and advocacy networks arose to add "brand recognition" to Euromaidan. Euromaidan PR and the associated Euromaidan Press were active in disseminating press releases in multiple languages via social media, as well as maintaining a core physical presence on the Maidan for easier access to journalists and officials.[12] This pairing of online and offline activism aided the network's visibility and name recognition.[13] The social media networks Maidan Needs Translators and Euro-Maidan As It Is also expanded international outreach by providing rapid translations.[14] The network remained almost exclusively in the virtual arena, linking Ukraine-based dissidents to the diaspora. Facebook was used to recruit volunteers and advertise translation needs, while the *Voices of Ukraine* blog served as a central repository. At any one time, the network had a core handful of volunteers with as many as 30 translators and editors worldwide during critical periods.[15] During Euromaidan, at least 2 million views were recorded on the *Voices of Ukraine* blog, and by August 2014 nearly 3,000 translated articles had been posted with a readership from over 190 countries.[16] Twitter was also frequently employed during periods of regime violence when the need for quick and mobile foreign-language updates became particularly important.

Active since 2009, the Ukrainian Updates Twitter account @Ukroblogger is notable for its high number of tweets and followers, and for being run by a single, independent activist-blogger who saw a need for more English-language information about Ukraine. The activist found that Twitter

reached a significantly larger audience than blogs. By mid-June 2015, for instance, the Ukrainian Updates Twitter account had garnered 511,000 views in less than two months, while its associated blog had had 311,000 visits since its initial creation in 2007. The activist found the feedback from followers particularly useful: knowing there was an audience waiting for information fuelled a desire to continue tweeting even during periods of personal exhaustion.[17]

#Digitalmaidan was a diaspora-led network dedicated to organising Twitterstorms—a PR tactic that can garner an audience far beyond one's typical followers. Activists organised three Twitterstorms around the #Digitalmaidan hashtag and successfully held the top place in worldwide Twitter traffic on January 27, 2014, with an estimated 5–6 tweets per second.[18] Instructions on how to use Twitter, along with pre-made tweets in multiple languages that could simply be copied, pasted, and tweeted, were posted on a Digital Maidan website, Facebook page, and Twitter account, and were also disseminated via other pro-Euromaidan networks.[19] By February 2, 2014, #Digitalmaidan had reached an estimated 3.7 million Twitter users who collectively saw the hashtag over 11.6 million times.[20]

EYES AND EARS

One of the most powerful aspects of Euromaidan was the ability of dissidents to share tactical information widely and rapidly through live streams and video. Many activists, journalists, and ordinary citizens used mobile phones to upload 24/7 live video feeds onto YouTube, UStream, UkrStream, and online TV news sites, which provided a powerful view of developments as they happened. Commercial drones were also used sporadically to disseminate live overviews of the Maidan, as were traffic cameras and webcams. A proliferation of "how to" or training videos, on everything from how to make a Molotov cocktail to protecting personal information online, also rapidly appeared. A number of documentary or eyewitness videos were also circulated, which often contributed to an "emotional mobilisation" of a kind that sociologist Manuel Castells argued is critical to overcoming or accepting the risk of regime violence or retribution.[21] Videos of police brutality on November 30, 2013, for instance, provoked a massive public protest the following day.

Euromaidan also saw the emergence of independent, online, and live television—in essence, Ukraine's first public broadcasting service. This gave Ukrainians an immediate resource with which to understand developments as they happened, without recourse to government-controlled or -influenced channels. Independent online TV, delivered through YouTube, UStream, and other websites, was quickly provided by ventures such as Hromadske TV, Espreso TV, and Spilno TV. Hromadske was actually announced as a crowdfunded online TV network a few months prior to the first Euromaidan protest but was still very much in its infancy. The plan was for a soft launch on November 18, but the start of Euromaidan on November 21 immediately brought Hromadske to the fore. During the first mass protest of Euromaidan, on November 24, Hromadske received more than 760,000 views as the public went online for information.[22]

SELF-DEFENCE FORCES

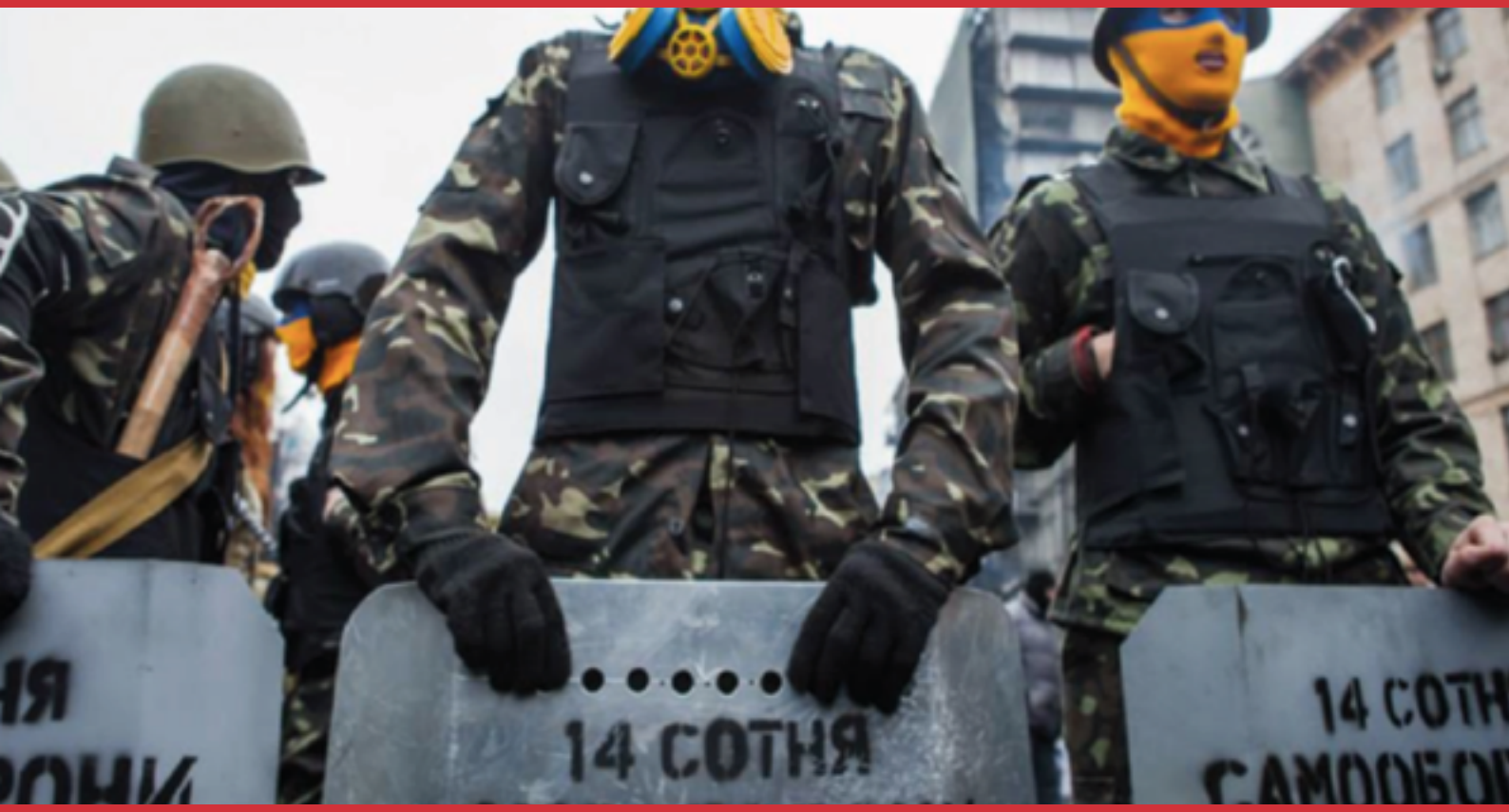
The initial creation of a volunteer self-defence force (SDF) was announced in early December 2013 to protect and defend the Euromaidan. Social media was used frequently to brand, organise, and recruit members into units called *sotnyas*—a Cossack reference evoking periods of rebellion in Ukrainian history. Approximately 40 units of an estimated 12,000 volunteers had been self-

formed by early February, with an on-call capacity of 25,000. Each unit had varying leadership structures, communication styles, and tactics, but they shared an overarching goal of defending Euromaidan territory. Social media was ideally suited to the needs of these self-organised units, enabling them to solicit new members and donations and to advertise their activities, while allowing individuals to create an immediate virtual identity. Most continue to maintain their own social media accounts now in defence of the Donbas.

Often credited—and criticised—for taking a leading role in clashes against police following the January 16 "dictatorship laws", the ultra-nationalist group Right Sector was prolific in social media, making use of multiple platforms including VK, Facebook, YouTube, and Twitter.[23] Use of VK far surpassed all other platforms the group exploited, probably because of its ease of use for Russian- and Ukrainian-speaking users. The majority of posts gave information on Right Sector's ideology and mission, instructions for behaviour, and morale-building images glorifying the group. Members turned to Twitter in the heat of the mid-January riots

Civic Sector garnered media attention for activities attempting to influence police treatment of protesters. Here, activists hold mirrors and placards pleading for peace opposite a police barricade. Such images were circulated widely in social media.

Source: Civic Sector Facebook, December 30, 2013.[10]



The 14th Sotnya used social media to disseminate images to portray the unit as a capable and organised defence force.

Source: Sotnya's Facebook page, February 16, 2014.[25]

exclusively for the purpose of disseminating tactical information. Tweets frequently requested donations of medical supplies, noted mobile phone dead zones, and identified locations of regime forces.

Formed in early December 2013, the 14th and 15th Sotnyas represented Free People, a nationalist youth organisation. Both units used social media to promote the image of themselves as capable and well-equipped forces. After Euromaidan, several members joined the National Guard or paramilitary groups in eastern Ukraine. Facebook and VK accounts remain active particularly for posting news on members requesting donations.[24]

Kibersotnya (Cyber Unit) emerged in social media on February 13, 2014.[26] According to its posted manifesto, the intent was to create a virtual community to support the SDF. Members were divided into activists and specialists. Activists would assist in waging an information campaign against the Yanukovych regime, while specialists provided guidance on information security, such as best practices on data protection. Barely off the virtual ground, one of Kibersotnya's first actions was to organise a

same-day Twitterstorm on February 18 in response to the shooting of protesters. To date, the network's Facebook account has generated 16,000 likes, while its Twitter account has more than 9,800 followers. Anti-Maidan elements saw an immediate threat in the unit's creation and advocated the targeting and disruption of Kibersotnya. On February 22, for instance, the Berkut Kyiv network called on followers to shut down Kibersotnya and browse through member profiles for targeting purposes.[27]

HACKTIVISM

There were multiple cyber-related efforts against the Yanukovych government that can broadly be described as "hacktivism"—the use of computers and computer networks to promote an ideological or political goal. Tactics included information theft, defacing websites, and distributed denial of service (DDoS) attacks. Hacktivists made intensive use of social media for PR purposes and to share or clarify information about potential targets. As during the Arab Spring, the hacker network Anonymous frequently used social media to interact with hacktivists inside Ukraine in order to obtain insights into developments and possible targets.

While Anonymous is intentionally difficult to pin down, members frequently carry out activities in support of freedom of speech. From the very outset of Euromaidan, Anonymous and Anonymous Ukraine were actively engaged in launching regular cyber-attacks against the Ukrainian government. On November 21, 2013, an #OpUkraine Twitter hashtag was launched to advertise operations, such as a DDoS attack against the Presidential website on December 1. The Ministry of the Interior and other government sites were targeted. Tweets also advertised Anonymous' successes by releasing private emails shared among Yanukovich's Party of Regions parliamentarians.[28] Attacks continued through January and February, intensifying particularly during violent clashes. Anonymous announced that it had taken down or defaced as many as 42 government websites on February 18 alone.[29]

Anonymous was soon the target of a pro-Russian campaign. A Twitter hashtag previously used by Anonymous Ukraine called #OpIndependence was hijacked and utilised for disseminating disinformation. On February 11, tweets purportedly from Anonymous claimed the group had successfully stolen emails belonging to Euromaidan opposition leader Vitaliy Klitschko proving that he was a "puppet" of the West. Other tweets suggested nefarious US involvement in Euromaidan, including plans to invade.

Faked Anonymous tweets often cited known sources of Russian propaganda, such as *Voice of Russia*.[30]

The faked tweets often cited known sources of Russian propaganda, such as *Voice of Russia*, but others required more investigation before pro-Kremlin ties or sympathies were revealed. Since Anonymous is an intentionally decentralised network of anonymous hackers, however, virtually anyone can claim to be part of it. As the #OpIndependence disinformation campaign demonstrated, Internet ambiguity can work in favour of the opponent.

The pro-Russia operation did not stop there. Shortly after the February 20 sniper attacks, a video ascribed to "OfficialAnonymousTV1" appeared on YouTube that artfully mimicked the Anonymous network's typical PR videos by using the same masked figure and anonymous robotic voice.

The pronouncement, however, was a clear example of Russian active measures:

> The people of Ukraine voted for President Yanukovich to lead them in fair and just democratic elections. The people of Ukraine plea to the President and to Russia for help in stopping the siege of Ukraine by Nazi thugs and murderous gangs.[31]

The video generated 200,000 hits. Although it has since been removed from the fake Anonymous TV channel, it is still available on YouTube and user comments continue to demonstrate confusion over whether the video is fake or genuine.

LOGISTICS

The self-organised Logistics Headquarters appeared in social media as an immediate reaction to police violence against protesters on November 30, 2013.[32] Organisers saw an urgent need to house protesters, particularly the thousands suddenly arriving in Kyiv. Responding to housing needs was quickly followed by transportation co-ordination and facilitation of donations of food and medical and other supplies. A small core group established pages on Facebook based on function—shelter, donations, and transportation—which were used to recruit as many as 100 volunteers in Ukraine and abroad to staff a 24/7 virtual call centre.[33] Facebook was the platform of choice because of its ability to reach a wider international audience. Notably, by the end of February 2014, Logistics Headquarters had arranged shelter for more than 20,000 Maidan participants.

Social media was also important in recruiting volunteers abroad, particularly from the diaspora. As one co-ordinator commented, the difference in time zones among volunteers was a critical asset in allowing Logistics Headquarters to operate a 24/7 hotline; exhausted volunteers had a chance to recharge, which continues to be an important part of the network's long-term success.[34]

NARODNIY HOSPITAL (PEOPLE'S HOSPITAL)

In reaction to police violence on November 30, 2013, a handful of volunteers saw a need to supply the growing number of medical clinics, mobile brigades, and underground hospitals. Public hospitals had become danger zones for dissidents as a result of kidnappings and arrests. The People's Hospital was quickly born on Facebook and a core group of about ten organisers interacted virtually to raise donations and deliver equipment and supplies.[35] Donations soon came in from across Ukraine and abroad, amounting to an estimated $120,000 during the period of Euromaidan.[36] The People's Hospital was able to supply sophisticated medical equipment, including defibrillators, an oxygen station, and hospital sterilisers, and even bulletproof vests for medics. Social media was also used

to regularly monitor the situation on the ground, particularly via live streams around the city. The People's Hospital experienced limited online harassment, but the use of Facebook—particularly closed groups—seemed to frustrate the trolls and to minimise fake friend requests.

IT SUPPORT

Formed by a group of information technology (IT) experts, IT Namet (meaning "tent") served as a single point of focus for those needing IT support, Wi-Fi access, or simply a place to warm up while their devices charged. Within hours of launching a Facebook page, IT Namet received 4,000 likes, several volunteers, and more than a dozen Internet-capable tablets which anyone could borrow.[37] Facebook helped to advertise activities and share IT-related information, while the physical presence of a dedicated tent was an important aspect of success.

LEGAL ADVOCACY

One of the best-known networks, Euromaidan SOS, had a fortuitous beginning. Civil activists and lawyers had gathered in Kyiv for a seminar hosted by the Centre for Civil Liberties (CCL) NGO on November 30, 2013. As news of police brutality in the early morning hours circulated, CCL took the lead in establishing a social media network of volunteers to help those beaten or arrested.[38] Euromaidan SOS was deliberately decentralised in part to avoid regime persecution against particular co-ordinators (although this did occasionally occur). Volunteers collected and analysed information on government abuses, advertised missing persons, helped find witnesses, produced infographics, and promoted other pro-Euromaidan efforts in Kyiv and across Ukraine.

Within hours of its first post advertising Euromaidan SOS as a resource for legal help, its Facebook page had been "liked" 10,000 times and three newly set-up 24/7 hotlines had fielded 300 calls from people seeking assistance. VK was also used frequently, with approximately 20,000 followers. Twitter garnered 56,000 followers with nearly 1,500 posts and was particularly utilised during the period February 18–24 to report on regime whereabouts.

ANTI-MAIDAN

Although the Yanukovych regime was probably more comfortable with traditional means of countering protests, such as stricter legislation, intimidation, and heavy use of security forces, the Anti-Maidan information campaign in social media grew in sophistication. Approximately 70 self-described Anti-Maidan social media networks had emerged by late January 2014, roughly 75 percent of which were dedicated to regions outside Kyiv, particularly Crimea, Donetsk, Odessa, Poltava, and Kharkiv. Most not only remain active, but the frequency of posts has multiplied in support of pro-Russian forces in the Donbas.

A main Anti-Maidan social media page appeared in VK on November 24, 2013.[39] Anti-Maidan boasts a significant VK following of nearly 580,000 followers with 57,000 posts as of July 6, 2015. Despite the "Anti-Maidan" designation, only about 10 percent of posts occurred before Yanukovych's ejection in February 2014, which highlights the growing role of social media in the Donbas conflict. As protests became more violent in January, so too did Anti-Maidan content in VK and Twitter, which increasingly

featured images that were intended to shock and disgust. Anti-Maidan also used pro-Euromaidan hashtags in an attempt to influence Euromaidan participants, though with limited success.

Berkut Kyiv appeared in VK on December 3, 2013 as a medium for the personnel of Berkut, the special police force, to denounce and criticise the Euromaidan movement.[40] Following the shootings on Maidan between February 18 and 20, the majority of posts continued to disparage the Euromaidan and claimed that the snipers who shot protesters were Right Sector members in disguise. Other posts simply denied the events took place. By February 24, as thousands of Berkut personnel fled to Crimea, the Donbas, and Russia, the network contained multiple posts urging others to stand firm, requested Russian intervention, or provided details on how to claim asylum in Russia.

The Anti-Maidan Co-ordination Headquarters was focused almost wholly on co-ordinating information operations. Launched through VK on January 22, 2014 during the riots, organisers discussed the importance of social media activism.[41] Co-ordinators called on those with cameras to "shoot something more truthful". Organisers particularly emphasised the need for multiple separate but related Anti-Maidan social media pages.[42] Within a month, the Co-ordination Headquarters boasted a list of nearly 70 related networks.[43]

CONCLUSION: WHAT'S NOW AND WHAT'S NEXT?

The question of how far social media can enable future mass movements will depend on the capabilities and objectives of their governments. Euromaidan represented a particular window of opportunity. But as authoritarian states are increasingly demonstrating, social media can be exploited as a tool of harassment, surveillance, and disinformation. Nearly all those interviewed for this study experienced some level of offline and online harassment.

We can also expect the volume of fake information to continue its exponential rise, with a mass of disinformation, often unverifiable, emanating from the Kremlin and pro-Kremlin elements today. This effort is intended to create an information space where there are no set rules, no reality exists, and solid verification is impossible. Certainty itself becomes questionable; exaggeration, distortion, and outright falsification are routine; and the ability to decisively prove the truth becomes increasingly difficult.

As Castells well articulated, the information space is increasingly contested terrain and evidence of "the oldest struggle in humankind: the struggle to free our minds".[44] But while governments may choose to expend resources in order to dominate the information space, their ability to do so will vary, often erratically and unpredictably. Rapid technological advances combined with social media's ability to link dissidents to experts of all types anywhere in the world will continue to provide windows of opportunity for those seeking to challenge their rulers. Future opposition movements will continue to shift, innovate, and revolutionise—as they have throughout history.

REFERENCES

1. International Telecommunication Union, "Percentage of Individuals Using the Internet", 2015. http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.
2. Personal interview, conducted June 2015; Kyrylo Galushko and Natalia Zorba, "Ukrainian Facebook Revolution? Social Networks against a Background of Euromaidan Social Research", *Contemporary Ukraine Research Forum*, April 28, 2014.
3. Freedom House, "Freedom on the Net 2013", https://freedomhouse.org/report/freedom-net/2013/ukraine#.VI9JIEtsvwl. Freedom House, "Freedom on the Net 2014", http://freedomhouse.org/sites/default/files/resources/Ukraine.pdf.
4. Olga Onuch, "Euromaiden Protests in Ukraine: Social Media versus Social Networks", *Problems of Post-Communism*, 62, 2015, pages 1–19.
5. Galushko and Zorba, op. cit.; Olga Onuch, *Mapping Mass Mobilization*, New York: Palgrave Macmillan, 2014.
6. Statistics available in Ukrainian "ТОП-5 країн по кількості користувачів Facebook", at Media Business: МедіаБізнес. http://www.mediabusiness.com.ua/content/view/22756/69/lang,ru.
7. Personal interview with Civic Sector co-ordinator, conducted September 2015.
8. See facebook.com/hrom.sektor.euromaidan and Twitter: @maidan_go.
9. Personal interview, conducted September 2015.
10. Civic Sector Facebook page, December 30, 2013. https://www.facebook.com/hrom.sektor.euromaidan/photos/ms.c.eJw9z9sRxDAIA8COboJ499~;YOWDlcyPASliiUyCdXi2~;WMsan12fBpyOCoO70jm59OfNuQ~_MLWldB21r3kevn9eKlD73A5J0jPHlZyJRFdeKcQod4~_C~_zr3z7dpsDTrH1dcus~_~;M3cdW9Hn63BS~_F7o5~_0WP1a5z~_~_mdb7V3X9XpuR9R9NvHu2~_fNp95GN2T1~;2fdkwun2vy5L3tF~_zXMf31kT9T9GwD.bps.a.647297088642561.1073741869.634929216546015/647297175309219/?type=3&theater
11. Coined in 2005, crowdsourcing refers to the means of collaborating on needed services, ideas, or content with the online community, particularly via social media. Crowdfunding is a type of crowdsourcing that involves financial donations.
12. See facebook.com/empr.media and Twitter: @EuromaidanPR.
13. Personal interview with Euromaidan press co-ordinator, conducted June 2015.
14. See facebook.com/Voices-of-Ukraine-Official-553978201352681 and facebook.com/EuroMaydanTranslations.
15. Personal interview with co-ordinator, conducted June 2015.
16. Svitlana Krasynska, "Digital Civil Society: Euromaidan, the Diaspora, and Social Media", in David Marples and Frederick Mills (eds), *Ukraine's Euromaidan: Analyses of a Civil Revolution*, Stuttgart: Ibidem-Verlag, 2015, page 183.
17. Personal communication with Ukrainian Updates blogger, June 2015.
18. Tetiania Lokot, "Ukrainian #DigitalMaidan Activism Takes Twitter's Trending Topics by Storm", *Global Voices Online*, January 27, 2014; Olga Minchenko, "#Digitalmaidan вийшов на 1-ше місце в світових трендах Твітера", *Watcher*, January 27, 2014.
19. Personal interview with Digital Maidan co-ordinator, conducted July 2015.
20. Krasynska, op. cit., pages 188–9.

21. Manuel Castells, *Networks of Outrage and Hope: Social Movements in the Internet Age*, Cambridge: Polity, 2012 (Kindle edition).
22. Tetiania Lokot, "As Ukraine's Protests Escalate, #Euromaidan Hashtag Lost in a Sea of Information", *Global Voices Online*, December 6, 2013.
23. See facebook.com/groups/223479324489867. VKontakte: vk.com/ps_ukraine. Twitter: @right_sector.
24. See facebook.com/14 sotnya and facebook.com/15sotnya; VKontakte: vk.com/samooboronamaidanu and vk.com/15sotnya.
25. Sotnya's Facebook page, February 16, 2014. https://www.facebook.com/14sotnya/photos/pb.216189441908260.-2207520000.1446277927./228663970660807/?type=3&theater
26. See facebook.com/cyber100ua. VKontakte: vk.com/cyber100ua. Twitter: @cyber100ua.
27. See vk.com/berkut_kiev, February 22, 2014.
28. See #OpUkraine Twitter posts, November 21, 2013 to February 24, 2014.
29. @AnonymousPress, "The people have won. All cyber-attacks on #Ukraine will cease. #opUkraine", Twitter, February 22, 2014.
30. @AnonyInfo, Twitter, March 14, 2014, https://twitter.com/anonyinfo/status/444418695775805440
31. See YouTube video: https://www.youtube.com/watch?v=1AWEI9rFYXs&feature=youtu.be.
32. See facebook.com/Logistychnyi.Shtab, vk.com/logistichq, and Twitter: @LShtab.
33. Personal interview, conducted June 2015.
34. Personal interview, conducted June 2015.
35. See facebook.com/narodnyihospital.
36. Personal interview, conducted September 2015.
37. See facebook.com/itnamet.
38. Personal interview with Euromaidan SOS co-ordinator, August 2015.
39. See vk.com/antimaydan and Twitter: @ant1maydan and @anti_maidan.
40. See vk.com/berkut_kiev.
41. See vk.com/k_shtab.
42. See posts by Anti-Maidan Co-ordination Committee, January 22–23, 2014. http://vk.com/k_shtab.
43. See post by Anti-Maidan Co-ordination Committee, February 19, 2014. http://vk.com/k_shtab.
44. Manuel Castells, "Communication, Power and Counter-Power in the Network Society", *International Journal of Communication*, 1, 2007, pages 238–66.

FROM MULLAHS TO MOSCOW: Propaganda in the Social Media Age

By **David Patrikarakos**

The nation state in its twentieth-century form traditionally held primacy in two areas from which it derived much of its power. First, there was its monopoly on the use of force; and second, its near-total control of information flows. Social media platforms have created new venues that allow people to communicate outside traditional state hierarchies of communication, such as state-owned, or even privately owned but state-permitted, newspapers, radio, and TV. In this sense, social media has created a political reversal: a transition from centralised communicative modes to the more random network effects of an earlier, more decentralised time before the birth of the modern nation state. This change has altered the way that propaganda is disseminated and consumed, and—critically—the scope and range of its effects.

New methods of disseminating propaganda are especially important for authoritarian governments, which have traditionally sought to control all forms of public debate. Social media makes this virtually impossible. Certain states such as China and Iran seek to control the Internet by, for example, barring access to certain social media sites. But such methods have mostly proved ineffective in stifling social media-based interaction and the dissent that invariably comes with it. The truly effective option left open to the authoritarian state is therefore to counteract unauthorised information flows with propaganda of its own—most usefully within the same medium.

This paper will examine two ways in which social media is used to disseminate propaganda: first, what I term "reverse trolling" or spamming, as used in a somewhat comedic effort by the Iranian regime to master social media; and second—the most effective and therefore potentially the most dangerous method—social media hacking, which differs greatly from traditional concepts of hacking.

GETTING THE MESSAGE OUT: SPAMMING OR REVERSE TROLLING

Social media usage in Iran rose to prominence during the Ahmadinejad era—and at first the regime didn't like it, considering social media sites such as Facebook and Twitter to be "enemy spaces" and banning their use in Iran. The claim of Mohammad Hassan Nami, former minister of communications and IT in ex-President Mahmoud Ahmadinejad's government, encapsulated the initial attitude of Iranian elites: "Wikipedia is seemingly an internet site, but during the 33 Day War, it gave the address for most [Lebanese] fighters to Israel," he said. "Same with Google. It's true that these sites appear to serve people, but in reality they're used for gathering intelligence."[1] "Facebook is the Zionist mafia's Trojan Horse" believes Ali Mirahmadi, chief of police in Semnan Province.[2]

But the regime quickly came to understand that social media platforms could be used to track, intimidate, and ultimately silence opposition voices.[3] More importantly, it also came to understand that, as "Trojan Horses", they were also battlefields on which it was critical to engage the enemy.[4] There was, it believed, an imperative to utilise these sites because the failure to do so would be ceding vital space to the enemy (read: the West). The regime set up the Supreme Council of Cyberspace, charged with "formulating Iran's Internet policies as well as with devising plans to regulate its use in accordance with the objectives of the Iranian Supreme Leader".[5]

The change in attitude was unequivocal. In 2013 the chief of Iran's National Police Forces, Esmail Ahmadi Moghaddam, publicly stated that "targeted usage" of social media sites was acceptable and that, despite the illegality of social networks, "there is no harm in using these platforms for the purpose of protecting national interests".[6] He was even clearer in a later statement where he claimed that Facebook had become a vehicle for "exporting the Islamic Revolution". The "enemy", he stated, had created Facebook to silence the voice of the Islamic Revolution, but instead it could become a tool to export it.[7]

Ayatollah Khamenei's "Letter to the Youth of the West"

Most major Iranian public figures, including Iran's Supreme Leader Ayatollah Ali Khamenei, have Facebook pages on which they can engage with Iranians.[8] But a fundamental ideological tenet of the Islamic Republic is to export its Islamic Revolution, and a necessary part of this strategy is the need to engage internationally. On January 21, 2015, Khamenei published a "Letter to the Youth in Europe and North America" on his website.[9] A source close to Khamenei, quoted in *Al-Monitor*, stated that:

> This letter, which was written by Imam Khamenei himself, is aimed at reaching the youth of the West to tell them to read and understand Islam directly … It's as important as the Salman Rushdie fatwa in the late '80s. Imam Khamenei wants to build bridges with the future, with the youth, those who are going to be the leaders of the future.[10]

The letter, written partly as a response to the Charlie Hebdo attacks that had occurred around a week earlier was, Khamenei said, an attempt to bypass what he deemed to be untrustworthy political leaders and engage Western youth directly. Its goal was to encourage them to have an open mind toward Islam and to not judge it on recent events. It also urged its target audience to engage with Islamic sources directly and not accept mediated versions that resulted from "prejudices". It was, in effect, a pitch urging Western youth to engage with Islam without preconception or bias.

As well as being published shortly after the Charlie Hebdo attacks, the letter coincided with negotiations between Iran and the P5+1 (the five UN Security Council powers and Germany) over its nuclear programme. It's possible that Khamenei was trying to show the world a more 'moderate' face at a crucial time in the negotiating process and to distinguish between his own brand of Shia Islam and the Sunni extremism responsible for the attacks (though Khamenei made no explicit reference either to Sunni or Shia Islam). The letter must also be understood in the context of internal Iranian politics. With many hardliners uneasy with increasing ties with the West, the letter was also a way for Khamenei to unambiguously assert the Islamic Republic's clerical and religious basis at a time when it was making compromises over its nuclear programme.

Khamenei insisted that the letter be circulated via social media.[11] The regime duly used Western social media platforms such as Twitter and Facebook to bypass traditional diplomatic channels to speak directly to its target audience: Western youth. "I don't address your politicians and statesmen … because I believe that they have consciously separated the route of politics from the path of righteousness and truth," Khamenei stated.[12] A dedicated Twitter account, @Letter4u, was set up to promote the letter.[13] Khamenei's Twitter account then tweeted, to urge Western youth to learn about Islam directly: "My 2nd request is that agnst #prejudgments, try to gain a firsthand knowledge of #Islam. At least, know what they are frightening you about!" [14]

The letter campaign was supported throughout Iranian governmental structures, and Iran's Islamic Culture and Relations Organisation made clear the scope of its intended reach with its announcement that Khamenei's letter had been translated into 21 languages, to "foil ill-wishers' plots to distort the content of the letter or marginalise it".[15] The regime even used state TV, which ran a programme to advise people on how letter4u could be promoted across social networks. Its purpose was to enable its viewers to create more successfully what became in effect a spamming campaign. Advice included telling viewers to add comments on popular social media accounts and those belonging to public figures in Europe and the US. The programme went to great lengths to encourage this, even using an actor holding a smart phone to demonstrate how to type comments onto Instagram.[16]

Regime supporters began spamming Facebook, Instagram, Twitter, Google+, and Tumblr in their thousands. Users did not just "passively" post links to the letter but, as *Al-Monitor* notes, made an effort to engage the online Western audience by posting questions such as: "Searching for the truth? Then #Letter4u is what you might want to read first" and "Do you know the leader of iran have written a letter for you??"[17] Users created memes showing the letter on t-shirts; links to the letter were accompanied by an image of an actual envelope, etc.—all designed to increase engagement.[18]

Many public figures, including the Instagram accounts of possible US presidential candidates Jeb Bush and Hillary Clinton, as well as President Barack Obama, were deluged with comments from Khamenei supporters promoting the letter, with much of the spamming done by automated accounts, known as bots.[19]

The Letter to Western Youth is illustrative of the rapid change in the tactics of state social media usage since Hassan Rouhani's election to the Iranian presidency in 2013.[20] Large numbers of foreign followers on social media enable figures like Khamenei to spread propaganda much more easily. For example, on October 1, 2013 Rouhani tweeted in response to a tweet asking if people in Iran could read his tweets; he replied: "Evening, @Jack. As I told @camanpour, my efforts geared 2 ensure my ppl'll comfortably b able 2 access all info globally as is their #right."[21] Given that Iranians still cannot access Twitter without using proxy servers,[22] this was something Rouhani could never say on Persian TV without fear of ridicule.[23]

The regime uses spamming not just to promulgate its messages but also to attack its opponents. The story of noted dissident Masih Alinejad is a case in point. Alinejad's Facebook page was recently deluged with bots attacking her anti-regime positions. A comment would be posted, and would then receive thousands of likes and comments from automated accounts, giving it prominence on the Facebook home feed, due to Facebook's EdgeRank algorithm. Once she deleted spamming comments, more accounts would then attack her for being against freedom of speech. "It was very well-planned and effective," Gharib concludes.[24]

SOCIAL MEDIA HACKING: THE FUTURE

Hacking has traditionally been associated with cyber-warfare, a process by which unauthorised users—"hackers"—illicitly gain access to data in a system or computer. One example is the North Korean government's hack and subsequent publication of Sony executives' emails in revenge for the film *The Interview*. Media hacking, or perhaps more specifically social media hacking, is entirely different. According to John Borthwick, chief executive officer of Betaworks, it refers to "the usage

and manipulation of social media and associated algorithms to define a narrative or political frame. Individuals, states, and non-state actors are increasingly using media hacking techniques to advance political agendas."[25]

Borthwick and his colleague Gilad Lotan conducted two case studies of social media hacking, which they wrote up in the online publication *Medium*: the Russia/ISIS hack and the Columbian Chemicals hack. These case studies enable us to see both what allows social media propaganda to spread and, perhaps more importantly, what inhibits it from doing so.

The Russia/ISIS Hack: Penetration and Connection

> "To effectively hack media, you need to penetrate and then connect across dense people networks."[27]
>
> John Borthwick

The Russia/ISIS hack is instructive because it illustrates the potential for propagandists to hack the primary means by which people discover information on the web: Google itself.[28] The facts of the case study are simple enough. Google was infiltrated to the degree that if you typed "ISIS France" into it, the first recommendation was "ISIS France Support". This happened, not because of any genuinely high levels of support in France for ISIS, but because "the most sophisticated algorithm in the world … [the] Google search algorithm was effectively hacked to produce this result".[29]

The hack was possible only through a catalogue of fortunate occurrences. On August 26, 2014, the online US publication *Vox* ran a story headlined "One in Six French People Say They Support ISIS".[30] That such a large number of people—around 10 million—could actively support ISIS would seem to be odd, and so it proved. What had in fact happened was that Russian news agency *Rossiya Segodnya* commissioned British company ICM to conduct an essentially flawed polling of people's views on issues such as Ukraine and Georgia, with the ISIS issue a poorly phrased secondary question: the published statistic in no way bore any relation to reality.[31]

But reality did not matter. The Russian TV station RT picked up the survey results, which then appeared on various—mainly French—sites.[32] The critical moment came when *Vox's* foreign editor, Max Fisher, picked up the story because, as he told Borthwick, he thought he saw the data in a tweet,[33] and *Vox* subsequently ran a story about it. Critically, this meant the story moved from the limited circle of RT readers and a few French sites into the mainstream US media. Once *Vox* tweeted its own version of the story, it subsequently moved into a new cluster of social media users; when Fisher tweeted it, it reached yet another cluster (those who follow Fisher and not *Vox*), and yet another cluster when *Vox* co-founder Ezra Klein tweeted it to his own followers. The story now had three entry points, from a publication and two individuals with high levels of "user trust",[34] into very different mainstream online networks. As Borwick explains, this is the "network finger print of an effective media hack".[35]

The problem, as Borthwick told me, is that while "Social media algorithms are a means of discovery and propagation … When you're looking at Facebook and Twitter there is no context … people will just click on the links—so certain [sometimes false] messages can get through this way."[36] In the Russia/ISIS hack, the more the story gained momentum across disparate, and trusted, social media

clusters, the more other outlets picked it up, until finally the Google algorithm was adequately fed and presented users with a search recommendation based upon what was essentially propaganda.

The Columbian Chemicals Hack: The Limitations of Hoaxing

The same factors that ensured the success of the Russia/ISIS hack account for the failure of Borthwick and Lotan's second case study: the Columbian Chemicals hack. Unlike the Russia/ISIS hack, the Columbian Chemicals hoax was clearly planned. It claimed that an explosion at a chemical factory in Centerville, Louisiana, had caused hazardous chemicals to begin leaking everywhere.[37] In the words of Borthwick, it was "a fabricated story put up online that tried to generate fear and uncertainty [by] saying there had been a chemical plant explosion on September 11th. Someone intended to do what happened; [for it] to be propagated as propaganda, but it didn't work."[38]

The reasons for its failure are vital to understanding why and how social media propaganda functions. Whoever was responsible—and the hoax appeared to be of Russian origin—set up a Wikipedia page devoted to detailing the apparent "explosion", a YouTube video showing a burning building and ISIS fighters delivering a message, and a Facebook page of a fake news outlet, *Louisiana News*.[39] A Twitterstorm under the hashtag #ColumbianChemicals erupted, but nonetheless the hoax was unable to gain traction in the way that the Russia/ISIS hack did.

This, as Lotan observes, was for two reasons: (1) the hoax did not generate enough user trust, which meant that (2) no network effects were triggered. The hoax was certainly "pretty elaborate", he said, and was clearly "planned many, many weeks in advance, with a Facebook page loaded with content, a YouTube channel, a wiki page etc". But even though it was carefully seeded in all these locations, the profiles that were used were fake and so hard to embed within a network of true users. "[On Twitter and Facebook] you have to be followed by real people to spread info. On Wikipedia you have to build up a reputation over time for other Wikipedia editors to trust you. You can't just rock up and create a page, especially about a terrorist attack."

The Twitterstorm, such as it was, was therefore confined to those accounts that were involved in the hoax. As Lotan explains:

> Anyone who says social media is a meritocracy—that anyone can post anything and it will be seen by millions—doesn't account for limitations in the social media space. Your positioning in the graph is critical to whether your information will be widely published. The taxi driver is not followed by the right people, so there is almost no chance that his content will be seen … So it's not a meritocracy at all.

Even if the hoaxers had gained enough real followers to retweet the hoax, it would still have been insufficient to make it gain sufficient traction without high-profile users (such as Fisher and Klein) retweeting it.

"The greatest threat from propagandists is when they start to generate real trust," says Lotan. This occurs when propagandists take a longer-term view and embed themselves within existing networks—for example, pro-Ukraine supporters on Twitter—and take the time to build trust. This is done by interacting with key players within the network through dialogue, reposting their content, and so on, until they reach a point where they are part of the community. "I'm sure we will get to that point where they are much smarter," concludes Lotan.[40]

The Columbian Chemicals hoax claimed that an explosion at a chemical factory in Centerville, Louisiana, had caused hazardous chemicals to begin leaking everywhere.

COMBATING SOCIAL MEDIA PROPAGANDA

To combat the growing phenomenon of social media propaganda, two areas in particular, both touched upon by Borthwick and Lotan, need improvement. The first is better discovery tools—the means by which users are able to access content: tools such as Facebook's EdgeRank algorithm-controlled home feed, which is part of the company's intellectual property and is understood only by the company. Such algorithms are effective, but they create a balkanisation of the Internet in that they track your likes and preferences and disseminate content into your home feed accordingly. So, for example, in the Russia–Ukraine conflict those with a pro-Ukrainian slant and those with a pro-Russian slant are likely to view material that reinforces their particular worldview. Each side thinks it is looking at the news, so algorithms shape how we think about reality and thereby create fertile ground for the sowing of propaganda.

Accordingly, users have little understanding of why particular content is presented to them—as the Russia/ISIS hack shows. The better we as users

understand why certain material is promoted into our home feeds or appears on our Twitter feeds, the harder it is for propagandists to hack these systems. As Lotan observes:

> If I had more visibility as to how the newsfeed is working I could have greater choice over what I choose to see. But social media platforms need to make sure it's a simple user experience and produce content that reinforces your prejudices to keep you on the network.[41]

The second of the two areas in need of improvement is the tools for measurement. Popularity has traditionally been measured by the number of clicks or views an article, video, or photo receives, but this is in fact a flawed system which further permits the dissemination of propagandist content, almost unchecked.

Tony Haile, chief executive officer of Chartbeat, which looks at real-time analytics, has calculated that 55 percent of readers spend less than 15 seconds looking at an article online—in essence, they don't read it. So instead of calculating the number of users looking at online content, Chartbeat uses an attention-focused metric, analysing how long users engage with, for example, a link they click on. Rather than just counting the number of users that have clicked the link, Haile argues that this is the correct way to gain a better understanding of real engagement and authority—and it is vital to detecting the automated spread of propaganda. An article may get 20,000 clicks or shares by 20,000 bots, giving the impression that it is material worthy of user trust, but Chartbeat can prove that no time was actually spent looking at the content. This makes it far harder for automated accounts to fool users with propagandist material.

What is needed, as a matter of urgency, is a dedicated, non-governmental institution devoted to combating online propaganda. The goal of the institution should be to consistently monitor online propaganda and to report on and expose it. There should also be social media initiatives—across all platforms—designed to educate the public about the threat, with the ongoing objective of enabling people to better recognise propaganda (as opposed to actual "news") when they are faced with it. In concert with this, the institution should establish a research arm to study and analyse the use of social media propaganda and its (almost constant) evolutions; for example, research should be undertaken into the effectiveness of trolling, an area that remains understudied.

The institution's second primary function should be the ability to mount "rapid reaction" and more targeted initiatives designed specifically to respond to propaganda campaigns which seek to distort truth or to promulgate an erroneous picture of a regime, need to be countered quickly and in a concerted manner, backed up by the resources of an institution dedicated to the task. The threat of online propaganda is considerable; considerable efforts must be expended to combat it.

REFERENCES

1. "Iran and Facebook, from Ridiculous to Sublime", *Iran Wire*, September 24, 2013. http://en.iranwire.com/features/2785.
2. *Ibid*. This fear—the permeation of Western influence into Iran—is longstanding: Ayatollah Khomeini labelled it "Westoxification".
3. See, for example, the Revolutionary Guard's "Operation Spider", in which various Facebook users were targeted and arrested for a variety of offences. For a fuller discussion, see http://www.iranhumanrights.org/2015/02/facebook-arrests.
4. Author interview with Amin Sabeti and James Marchant, Small Media, 2 April 2015.
5. "The Supreme Council of Cyberspace: Centralizing Internet Governance in Iran", Iran Media Program, April 8, 2013. http://iranmediaresearch.org/en/blog/227/13/04/08/1323#sthash.4xAiUQ2Z.dpuf.
6. ,ندارد ایراد نظام منافع حفظ برای شده فیلتر اجتماعی های شبکه از استفاده, 'Using Social Networks to Protect the Interests of the System is OK', https://www.digarban.com/node/14498
7. *Loc. cit*., note 2 above.
8. Interestingly, social media platforms such as Facebook are used more for internal propagandist purposes, while Twitter is used primarily for external propaganda.
9. "#LETTER4U: Message of Ayatollah Seyyed Ali Khamanei to the Youth in Europe and North America". http://farsi.khamenei.ir/ndata/news/28731/index.html#en.
10. "Khamenei's Message to the West", *Al-Monitor*, January 27, 2015. http://www.al-monitor.com/pulse/originals/2015/01/iran-foreign-policy.html#.
11. *Ibid*.
12. *Ibid*.
13. https://twitter.com/myLetter4u.
14. "Ayatollah Khamenei Writes Letter to Western Youth", BBC News, January 22, 2015. http://www.bbc.com/news/world-middle-east-30931363.
15. "Iran Translates Leader's Letter to Western Youth into Several Languages", Fars News Agency, March 1, 2015. http://english.farsnews.com/newstext.aspx?nn=13931210000351. These languages included English, Russian, Croatian, Serbian, Bulgarian, Swahili, Turkish, Indonesian, Chinese, Japanese, Spanish, Italian, Thai, and Albanian.
16. مشتگ تمبلی غLetter4U صداوسیما در اروپا چوان ان به ای خامنه نامه!., Khamenei hashtag Letter4U television advertising for youth in Europe!, . Link since taken down as account closed.
17. "Khamenei's Fans Take to Instagram", *Al-Monitor*, February 3, 2015. http://www.al-monitor.com/pulse/originals/2015/02/letters4u-iran-khamenei-instagram.html#ixzz3c19SsHyj.
18. See, for example, https://twitter.com/iran_onion/status/560324802419113984/photo/1.
19. Author interview with Nariman Gharib, a researcher on Iranian social media, May 25, 2014. A bot is an automated account that publishes content automatically: a computer script that publishes content to an account, rather than a human typing a post.
20. *Ibid*.
21. https://twitter.com/HassanRouhani/status/385138174822850560.

22. Interestingly, Gharib notes that Rouhani's government also uses social media for internal propagandist purposes. Locked in a constant battle with regime hard-liners, especially over the nuclear deal, they face the perennial threat of having their voice shut down internally, given hard-line control of most of the newspapers and state TV. A moderate newspaper or TV Station can be shut down, but Twitter and Facebook cannot. So these platforms provide Rouhani with a vital channel of communication that cannot be so easily stamped out.
23. See, for example, https://twitter.com/myLetter4u/status/570885965394403328
24. *Ibid*.
25. John Borthwick and Gilad Lotan, "Media Hacking", *Medium*, March 17, 2015. https://medium.com/in-beta/media-hacking-3b1e350d619c.
26. *Ibid*.
27. Borthwick and Lotan, *op. cit*.
28. The value of this cannot be underestimated; Google reportedly handles 70 percent of the world's Internet searches. "A Flashlight into the Cellar of the Lawless 'Dark Net'", *Spectator*, September 13, 2014. http://www.spectator.co.uk/books/9308562/the-dark-net-by-jamie-bartlett-review.
29. Borthwick and Lotan, *op. cit*.
30. Max Fisher, "One in Six French People Say They Support ISIS", *Vox*, August 26, 2014. http://www.vox.com/2014/8/26/6067123/isis-poll.
31. For a fuller discussion, see Borthwick and Lotan, *op. cit*.
32. "15% of French People Back ISIS Militants, Poll Finds", RT, August 18, 2014. http://www.rt.com/news/181076-isis-islam-militans-france.
33. Borthwick and Lotan, *op. cit*.
34. See below for further discussion of this issue.
35. Borthwick and Lotan, *op. cit*.
36. Author interview with John Borthwick, May 27, 2015.
37. Borthwick and Lotan, *op. cit*.
38. Author interview with John Borthwick, May 27, 2015.
39. See Borthwick and Lotan, op. cit. for a fuller discussion.
40. Author interview with Gilad Lotan, June 1, 2015.
41. Author interview with Gilad Lotan, June 1, 2015.
42. Tony Haile, "What You Think You Know about the Web Is Wrong", *Time Magazine*, March 9, 2014. http://time.com/12933/what-you-think-you-know-about-the-web-is-wrong.

ACKNOWLEDGEMENTS

I must thank Peter Pomerantsev and the Legatum Institute. My thanks also go to John Borthwick and Gilad Lotan, for their excellent research, which formed the basis for the section on media hacking, as well as giving me their time for interviews. I am grateful also to James Marchant for his time and invaluable insights into Iran's use of social media for propaganda, as well as Nariman Gharib and Amin Sabeti. Finally, I am indebted to Holly Dagres and Ali Hashem's articles in *Al-Monitor* on Khamenei's Letter to Western Youth for providing me with excellent case studies as a basis for research.

LEGATUM INSTITUTE

ISLAMIC STATE PROPAGANDA: Our Response to the Competition

By **Charlie Winter**

Since June 2014, when Islamic State[1] —known as ISIS at the time—commandeered Iraq's second city, Mosul, the world has been both fascinated and horrified at the precision with which the so-called "caliphate" executes its propaganda. The menace presented by Islamic State's media is unprecedented, in terms of its accessibility, scale, and complexity. Videos of foreign fighters executing Western prisoners have provoked outrage in populations from the United States to Japan; visceral depictions of alleged spies being killed have discouraged dissent at home and aggravated adversaries abroad; sterilised, uniform images of the implementation of *hudud* punishments—"criminals" being whipped, stoned, beheaded, dismembered, and cast off towers—have gratified and attracted ideological supporters of jihadism the world over.[2] Such a situation has been facilitated by the networked, globalised nature of the world we live in. In the Internet age, propaganda has been fully democratised.

These ultraviolent tendencies have, however, skewed the discourse on just what it is we are dealing with:[3] there is much more to Islamic State propaganda than brutality. This report examines the strengths of Islamic State's media strategy and looks at a selection of counter-propaganda efforts, identifying key features and areas in which counter-efforts are inherently impaired.

THE COMPETITION

The success of Islamic State's propaganda strategy can be attributed to five key characteristics: quantity, quality (production value), adaptability, narrative variation, and audience differentiation. By effectively nurturing each of these characteristics, Islamic State is able to sustain its captive audiences in Iraq and Syria while at the same time reaching out to new ones abroad.

Quantity

On average, Islamic State circulates 38 discrete units of propaganda each day: photo reports, videos, written articles, as well as the occasional audio statement or song sung *a cappella*.[4] Radio and text bulletins summarising the group's military exploits from Nigeria to Afghanistan are disseminated daily in (at the time of writing) eight languages: Arabic, Kurdish, Turkish, Russian, French, English, Bosnian, and Bengali.[5] Produced across the "caliphate's" many provinces and central production units, this content is uniformly presented and carefully choreographed such that it maximises attention and accessibility.

Quality

Descriptors like "professional", "slick", and "high-definition" have come to characterise what critical discourse there is on Islamic State's media.[6] Since their attention was first drawn to it, politicians and journalists alike have regularly claimed that the content is particularly seductive because of

its "high production values".[7] They have a point: videos exhibiting the boons of living under Islamic State are seamlessly produced and given sophisticated graphical overlays; photographs are taken with care to ensure that light and colour complement the narrative in question; radio programmes are rigorously structured and delivered in a carefully arranged manner reminiscent of World War II news bulletins. Islamic State's producers and cameramen are no amateurs.

Adaptability

The group's outreach strategy is delivered online and hosted largely on mainstream social media platforms. While some measures are in place to limit the accessibility of its propaganda, they are not sufficient to cut off the flow. Above all, this is because Islamic State's disseminators operate as a swarm and can adapt rapidly, unencumbered by the red tape and bureaucracy that holds back their adversaries.[8] When, for example, Twitter began to suspend the group's official disseminator accounts in the summer of 2014, they eschewed open officialdom entirely.[9] Instead, propaganda is now introduced to Twitter by below-the-radar users that refrain from self-identifying as "official", before it is spread using specially designated hashtags. To date, Twitter does not seem to have attempted to challenge this system of dissemination-by-hashtag, even though it is relatively proactive in suspending the most virulent of Islamic State's supporters.

Narrative Variation

Islamic State's propagandists do not just churn out content and hope it resonates in the right places with the right people. They tell a defined story and build a very specific brand. Focusing on six key narratives—brutality, mercy, belonging, victimhood, war, and utopia—the "caliphate" is able to project itself as a viable alternative to the status quo to all sympathetic audiences, whether they are motivated by politics, economics, or ideology.[10] It sells itself as a comprehensive millenarian ideal where the jihadist project is fully operational: *shari'a* is unflinchingly implemented, "Islamic" values are upheld, social justice prevails, and so on. In doing so, its propagandists provide their committed propagandees with a multi-layered image of what life is like in Islamic State-held territories.[11] Supporting this promise of utopian state-building is a constant reiteration of the "caliphate's" military supremacy and defiance in the face of "crimes" committed by the "Crusader–Nusayri–Saluli–Rafidi" (for which read "Western–Syrian–Saudi–Iraqi") alliance. Dead children and burned-out mosques are routinely integrated into propaganda as a means of legitimising the group's existence.[12] Less prominent, but just as important, are its promises of belonging and mercy in the face of repentance which are routinely juxtaposed with unwavering brutality in response to dissent or espionage.[13] The key point here is that, whether it is trying to attract supporters or intimidate adversaries, Islamic State does not rely on any one narrative to convey its message. Its propagandists manipulate a cocktail of themes that constantly change according to its priorities on the ground.

Audience Differentiation

Islamic State knows its audiences. Instead of operating on the naïve assumption that they have just one target demographic, the propagandists direct their output at a range of people, both supporters and adversaries.[14] This approach has enabled them to steer the discourse on the war

against their "caliphate" and to capitalise on the numerous benefits derived from a regular media presence—after all, in the world of jihadism, global infamy has a positive correlation with donations and recruits.[15] Understanding that different things appeal to different people is a crucial requisite for propagandistic success. For example, Islamic State is well aware of the fact that the vast majority of Sunni Muslims living in its environs are not ideological adherents. However, it is also aware that many of these same people prefer the idea of what it promises to the current status quo, be that civil war, political marginalisation, or entrenched, systemic persecution. Hence, by placing strong emphasis on the "caliphate's" revolutionary agenda, unwavering penal code, services provision, and social welfare programmes, the group's propagandists are able to attract disgruntled populations at the same time as they make ideological entreaties to jihadist fanatics.

THE RESPONSE

Over the course of the last decade, jihadist propaganda has changed profoundly: bland, grainy tapes of Osama bin Laden lectures have transitioned into feature-length documentaries shot in high definition, complete with special effects and accompanying soundtracks.[16] Over the same period, counter-propaganda has evolved, too. However, its evolutionary trajectory has been, at best, haphazard: from 2002's videos of Muslims declaring that they are "happy to live" in the United States to Disney-produced montages of images depicting what it is to be an American citizen.[17] In the face of the bulging jihadist threat, such campaigns consistently missed the target; according to some, they were counterproductive "reproduc[tions of] restrictive representations of diversity".[18] In the 2000s, such an outcome was just about acceptable. However, with the rise of Islamic State and its ever-metastasising menace, governments around the world have been forced to re-examine their approach. Social media corporations and file-sharing platforms have also joined the struggle, closely followed by community organisations and civil society activists.

Government

States around the world have approached the counter-propaganda question in three main ways: direct engagement, counter-propaganda campaigns, and sponsorship. Given that they are at the receiving end of the vast majority of negative messaging from radical social movements, jihadist or otherwise, there is a limited amount of success to be had with direct engagement from states. Nevertheless, the Center for Strategic Counterterrorism Communications (CSCC) of the US State Department has persisted in directly and openly addressing violent extremists online, challenging their claims and ideological agendas on a one-to-one, open-source basis.[19] There are no public metrics by which the effectiveness of these efforts are measured, but if we go by the CSCC's stated intention to gain ground "across a wide variety of interactive digital environments that had been previously ceded to extremists", they can be considered broadly successful.[20] Indeed, in Islamic State's Twitter echo chamber, one of the most constant fixtures is the CSCC's Arabic "Outreach Team". The extent of the resonance that the State Department's digital outreach has with the supporters of Islamic State that it targets is a question likely to remain unanswered, regardless of how hotly it is debated. Whatever the case, though, it would be a mistake to call off such endeavours: jihadists may regard the CSCC's arguments as spurious, and sometimes even humorous, but that does not mean that extremist voices should go unchallenged.

Google search result for 'ISIS', February 2015.

The next key element of government counter-propaganda is campaigning. In the last year alone, there has been a steep upward trajectory for state-led counter-propaganda campaigns. For a long time, the CSCC was the trail-blazer in this department. However, in July 2015 it was joined by the Sawab Center, a joint UAE–US venture that predominantly engages its target audience with short, sharp Arabic-language videos in which defectors are quizzed or refugees interviewed.[21] In addition to this, in August 2015 "UK Against ISIL" was established, a Foreign and Commonwealth Office-run Twitter account that has so far steered clear of digital outreach to jihadists and sought only "to inform and engage the UK public on what action the UK government and its partners in the Global Coalition are taking to defeat [the] brutal terrorist group".[22] With only 83 tweets and a reach of 4,406 people in its first month, the account is unlikely to reverse the trajectory of the information war. Likewise, the Australian Defence Force runs a "Fighting DAESH" Twitter account to combat Islamic State misinformation.[23] Similar to "UK Against ISIL", the reach of the Australian account is minimal, at just 905 followers after its

first month. Despite the numbers, initiatives like these are important, necessary recognitions of the fact that the online space needs contesting.

Inevitably, state-led campaigns have suffered teething problems, most notoriously when the CSCC made the mistake of emphasising Islamic State's brutality as a disincentive to joining it.[24] However, it is important to bear in mind that Islamic State's propaganda prowess did not emerge overnight, and these difficulties are to be expected as governments newly engage. Informed trial and error, while unappealing to traditionally risk-averse policymakers, is by far the best means of refining a given state's strategy towards counter-propaganda. Hence, in the years to come it is likely that such efforts will proliferate and increase in sophistication. Indeed, this has already been happening. In recent months, the approach does seem to have been set on a new trajectory.[25] Instead of preoccupations with ultraviolence, the emphasis is increasingly on "caliphal" iniquity—the Sawab Center, for one, has released a string of videos interviewing former members of the group about the falsity of its propaganda claims.[26] These were later re-publicised by the US State Department as part of its "Why they left Daesh" awareness-raising campaign.[27]

The last stream of activity is sponsorship of third-party initiatives. Through this, governments are able to improve their outreach ability and expand their target demographics. If production is ceded to other parties, campaigns—be they videos or social media feeds—are able to obscure the government stamp, if not do away with it entirely. This strategy is high-risk but high-yield: high-risk because, if the government stamp subsequently comes to light, the credibility of the campaign in question could suffer; high-yield because it allows outreach to those communities that are home to the pools from which extremist groups identify and recruit vulnerable candidates. In spite of the risks attached, sponsorship and seed-funding that foster counter-messaging production in the right places offer perhaps the most strategically minded way for governments to engage with the issue.

Private sector

Since it is social media platforms that are the vehicle of choice for all major jihadist outreach strategies, it follows that the corporations behind those platforms have an important role to play in limiting their reach and challenging their messages.

Private-sector engagement usually comes in the form of message promotion. In order to help make up for the fact that counter-efforts are far more diffuse than Islamic State's strategy, technology corporations have begun stepping in to magnify the voices of civil society and to train and inform activists on how to make their campaigns go viral.[28] The Against Violent Extremism network, launched by Google Ideas in 2011, was one of the frontrunners of using "technology to connect, exchange, disseminate and influence all forms of violent extremism".[29] Its website, a platform on which former extremists can engage with and support each other, also serves as a place for repentant—but not yet former—radicals to receive advice about leaving their extremist affiliations behind.

As well as proactive positive measures, social media companies have engaged in censorship. Facebook, having emerged as a relatively inhospitable environment for extremists in recent years, has enjoyed a measure of success in ousting the Islamic State echo chamber from its platform.[30] While supporters and sympathisers do still use it, they do so in a reduced manner. The same cannot be said for all other social media platforms. Twitter has persisted as the platform of choice for the group's propaganda dissemination methodology in spite of the company's fervent engagement

in account suspensions since the autumn of 2014:[31] regardless of how often they are suspended, Islamic State's most virulent supporters are persistent in reappearing. A notorious case in point is Turjuman al-Asawirti, an Islamic State propaganda user who has been suspended—and reappeared—no less than 281 times at the time of writing.[32]

Third sector

Whereas governments are restricted by their risk-averse nature and private corporations are forced to find a balance between meaningful engagement with the issue and ensuring stockholder satisfaction, third-sector organisations—particularly think-and-do tanks like the Quilliam Foundation and the Institute for Strategic Dialogue—are well placed to engage with direct counter-propaganda production, providing interventions with vulnerable individuals and research (full disclosure: This author worked for the Quilliam Foundation at the time of writing). They can also avoid the government stamp that discredits so many well-meant state campaigns.

Contributions have come in a variety of forms. The Quilliam Foundation, for example, has focused on empowering others to join the challenge. Besides crowdfunding and producing its own counter-narrative output, like the video "#NotAnotherBrother", which had over 50,000 unique views in two weeks, it provides media training workshops to young people in schools and universities, so they can develop their own creative media.[33] Other organisations have followed suit in developing proactive counter-narratives. A case in point is the Institute for Strategic Dialogue's "Extreme Dialogue" project which, following the trajectory of the UAE-run Sawab Center, tells the personal stories of family members and former extremists.[34] While commendable, the 17 videos posted on the "Extreme Dialogue" YouTube channel are not remotely as popular as Islamic State propaganda, having been viewed a total of 63,000 times since October 2014.[35] While campaigns like these do not necessarily resonate with Islamic State's active recruits and have much smaller online viewership than much of its propaganda, they are an important foundation from which to engage in counter-radicalisation work. Besides content production, the Institute for Strategic Dialogue is also piloting a one-to-one digital outreach scheme. Through direct engagement over the Internet—something reminiscent of Islamic State's own tactics—vulnerable people are often found to be more accessible and amenable to "counter" ideas than they are offline.[36]

Campaigns like "Open Your Eyes" and "TruthAboutIsis", both of which are anonymous and describe themselves as civil society-run Islamic State "myth busters", are another form of third-sector counter-propaganda activity. The first, which operates primarily on social media, has a distinctly British focus and seeks to project the voice of the Muslim majority through brief, well-produced interviews in which young people variously explain why they believe Islamic State is not Islamic, or warn their peers of the consequences of joining the group.[37] The second curates media reports on Islamic State in one place in an attempt to undercut the "caliphate's" idealised image of itself.[38] Reactive in nature, they are responding to the challenges Islamic State poses with counter-narratives, instead of creating their own. Initiatives like these play an important role, but again suffer from relatively small audiences. With just 5,437 followers on Twitter and 11,405 likes on Facebook between them at time of writing, they alone will not "crush ISIS propaganda".[39] In the long run, it is our own "compelling story"—not just our reaction, no matter how strong it is—that is required.[40]

Community

If the information war on Islamic State is to be won, it can only be done by making counter-extremism "cool". Things must go viral of their own accord. People need to be interested without being spoon-fed. Empowering grassroots activists to engage independently is of paramount importance if meaningful progress is to become a reality.

The vast majority of Muslim communities reject Islamic State and a number of grassroots initiatives have emerged to counter it, such as the fatwa from British imams in August 2014 that condemned all those who join the "tyrannical" Islamic State as "heretics".[41] As a community-led reaction, it helped prominent Muslims push back against the group and its ideology, while also lending theological credence to the assertions of David Cameron and Barack Obama that the "caliphate" is not Islamic.[42] While this initiative must be commended, it is important to recognise that it had little or no bearing on those who had already joined the group or, indeed, those on the cusp of doing so. Once someone is at that stage, it takes a lot more than theological counter-arguments to convince them to abandon their extremism. If the only measure of success is people not joining Islamic State, the fatwa does not rate highly. However potential recruits must not be considered to be the only target audience.

The "#notinmyname" and "#illridewithyou" campaigns were valuable efforts to counter the group's propaganda. The first was devised by the Active Change Foundation in reaction to Islamic State atrocities. Soon after it was initiated, it went viral. At the time of writing, it continues to be so, with numerous campaigns adopting the slogan in videos viewed hundreds of thousands of times.[43] The latter campaign came about shortly after the Sydney siege of December 2014—according to Twitter Australia, it was shared 150,000 times in just four hours as the public sought to cut through the anti-Muslim sentiment that arose in the wake of the attack.[44]

None of these initiatives posed a direct challenge to Islamic State's propaganda, but all were probably more effective in undermining its narrative than any other counter-messaging campaign. This was because, instead of offering a reaction, they organically provided an alternative. Hence, they were able to indirectly challenge key facets of Islamic State's appeal, sap its ability to claim pristine religiosity, undermine its ever-manipulated grievance narrative, and present a powerful vision of the "collective" at odds with that promised by Islamic State recruiters.

CONCLUSION

It is high time that we take a leaf out of Islamic State's media strategy book and recognise that, at a minimum, all counter-propaganda efforts need to be scaled up and re-strategised. Different target audiences must be engaged with different messages. Instead of just relying on a collection of worn-out counter-narratives, what is needed is an alternative set of ideas that is both robust and credible, not predicated upon its ability to undermine the claims of jihadists.

Since June 2014, the back offices of Whitehall and Washington have been buzzing with terms like "counter-propaganda" and "narrative" more than at any point since the fall of the Berlin Wall. The adversary may have shifted from state to non-state, but the challenge is strikingly similar: rather like the Soviets, the Islamic State propagandists play the millenarian card and constantly stress the utopian nature of their "caliphate" state; rather like the Soviets, there is a preponderant focus on the

military, be it troops training or tanks parading; and, rather like the Soviets, ideology is perpetually present in practically all messaging, though to varying degrees. Despite these substantial similarities, though, the differences are significant enough that efforts to counter this messaging need radical reappraisal. Of one thing we can be certain: governments alone are ill equipped to deal with the issue. Mitigating Islamic State's media menace necessitates a cross-sector approach that involves the whole of society, not just specialised cliques within it.

REFERENCES

1. Islamic State (IS) was formerly known as Islamic State of Iraq and the Levant (ISIL), Islamic State of Iraq and Syria (ISIS), and Daesh. These previous names are still widely used. However, throughout this paper, it will be referred to as Islamic State (IS).
2. "A Message to America", Furqan Foundation, August 19, 2014; "A Message to the Government and the People of Japan", Furqan Foundation, January 31, 2015; "But If You Return, We Shall Return", Nineveh Province Media Office, June 23, 2015; "The Implementation of the *hadd* upon a Murderer in the Region of Karma in the East of the Province", Raqqa Province Media Office, August 15, 2015; "Implementation of the hadd of Banditry on a Corrupt Individual", Khayr Province Media Office, July 27, 2015; "Whipping the Unmarried Adulterers", Dijla Province Media Office, July 21, 2015; "Implementation of the hadd upon Two Homosexuals in the City of Tadmur", Homs Province Media Office, July 23, 2015.
3. Boris Johnson, "Islamic State? This Death Cult is Not a State and It's Certainly Not Islamic", *Daily Telegraph*, June 28, 2015.
4. Charlie Winter, "Documenting the Virtual Caliphate", Quilliam Foundation, October 2015.
5. The linguistic repertoire of al-Bayan Radio is constantly expanding, something that is a direct function of Islamic State's foreign fighter population.
6. Olivia Becker, "ISIS Has a Really Slick and Sophisticated Media Department", *Vice News*, July 12, 2014.
7. Holly Yan, "Why is ISIS So Successful at Luring Westerners?", CNN, October 7, 2014.
8. See Fisher, *op. cit.*
9. J. M. Berger and Jessica Stern, *ISIS: The State of Terror*, New York: Harper Collins, 2015.
10. Charlie Winter, "The Virtual 'Caliphate': Understanding Islamic State's Propaganda Strategy", Quilliam Foundation, July 2015, page 22; Charlie Winter, "Documenting the Virtual Caliphate", Quilliam Foundation, October 2015.
11. Jacques Ellul, *Propaganda: The Formation of Men's Attitudes* (trans. Konrad Kellen and Jean Lerner), Random House Vintage Books, 1973, page 103.
12. "Aftermath of Bombardment from Crusader Safavid Planes on a Mosque in the Sakra Region", Euphrates Province Media Office, July 20, 2015; "The Safavid Army Targets a Mosque with Heavy Artillery", Janub Province Media Office, August 6, 2015; "Bombardment of the Crusader Safavid Alliance upon Muslim Mosques in Sajar", Fallujah Province Media Office, August 9, 2015; "Two Raids by the Crusader Safavid Alliance on Qa'im Hospital", Euphrates Province Media Office, July 23, 2015.
13. "Punish Them in the Same Way That They Punish You", Anbar Province Media Office, August 31, 2015.
14. Charlie Winter, "Experts Weigh In (part 4): Can the United States Counter ISIS Propaganda?", Brookings Institution Markaz, July 1, 2015.

15. Brynjar Lia, "Understanding Jihadi Proto-States", *Perspectives on Terrorism*, 9, 2015, page 36.
16. For a taste of Osama bin Laden's typical messaging, see "Excerpts from Osama bin Laden's Address on Aljazeera", AFP via *New York Times*, December 27, 2001; and, for a prime example of Islamic State's messaging, see "Although the Disbelievers Dislike It", Furqan Foundation, November 16, 2014.
17. Sheldon Rampton, "Shared Values Revisited", *PR Watch*, October 17, 2007; "U.S. Government Partners with Disney to Welcome International Visitors", US Department of Homeland Security and US Department of State press release, October 22, 2007.
18. Greg Miller and Scott Higham, "In a Propaganda War Against ISIS, the US Tried to Play by the Enemy's Rules", *Washington Post*, May 8, 2015; Evelyn Asultany, "Selling American Diversity and Muslim American Identity through Non-Profit Advertising Post-9/11", *American Quarterly*, 596, 2007.
19. See "Executive Order 13584—Developing an Integrated Strategic Counterterrorism Communications Initiative", White House: Office of the Press Secretary, September 9, 2011; and Greg Miller and Scott Higham, "In a Propaganda War against ISIS, the U.S. Tried to Play by the Enemy's Rules", *Washington Post*, May 8, 2015.
20. Center for Strategic Counterterrorism Communications, US Department of State.
21. "UAE and US Launch Sawab Center—New Digital Communications Hub to Counter Extremist Propaganda", UAE Embassy, July 8, 2015; see "Mohamed Al Etibi—Why Do Defectors Leave Daesh?", Sawab Center, August 18, 2015 [5,111 views at time of writing].
22. @ukagainstisil provides "updates on the UK Government's ongoing work to defeat ISIL"; see Frances Perraudin, "UK Launches Twitter Account to Combat Islamic State Propaganda", *Guardian*, August 28, 2015.
23. @Fight_DAESH corrects "false information disseminated on Twitter by DAESH and its sympathisers"; see Mark Di Stefano, "This Anti-ISIS Twitter Account Slid into my DMs without Asking", Buzzfeed, August 27, 2015.
24. The most infamous instance of this is "Welcome to the 'Islamic State' Land (ISIS/ISIL)", Thinkagain Turnaway (CSCC campaign), August 22, 2014.
25. Rashad Hussain, "A Strategy for Countering Terrorist Propaganda in the Digital Age", Remarks at Australian CVE Summit, June 12, 2015.
26. These videos have been summarised by Sarah Sinno in "The Defectors' Handbook to Destroying Islamic State", *Daily Telegraph*, September 23, 2015.
27. #WhyTheyLeftDaesh, promoted by @ThinkAgain_DOS, began on September 21, 2015.
28. For example, when searching on YouTube for a prominent video produced by Islamic State's Furqan Foundation, the first results to appear are "Defiant against IS", from the Active Change Foundation, and "Qurbani This Eid", from the Charities Commission. The requested video itself does not appear in the search results.
29. See http://www.againstviolentextremism.org/about.
30. Steven Stalinsky, "The Facebook Model for Taking on Jihadist Groups Online", *Washington Post*, August 27, 2015.
31. Berger and Morgan, *op. cit.*, page 33.
32. On September 29, 2015 Turjuman reappeared on Twitter with the handle @TUMedia281. By September 30, 2015 it had already been suspended.
33. "#NotAnotherBrother", YouTube, August 3, 2015 [51,692 views at time of writing].
34. Funded by the Kanishka Project, "Extreme Dialogue" was launched in February 2015 and involves the Institute for Strategic Dialogue, Duckrabbit, and the Tim Parry Johnathan Ball Foundation for Peace.
35. "Extreme Dialogue" channel, YouTube, launched October 19, 2014 [total of 63,089 views at time of writing].
36. Rukmini Callimachi, "ISIS and the Lonely Young American", *New York Times*, June 27, 2015; see also Ross Frenett and Moli Dow, "One to One Online Interventions: A Pilot CVE Methodology", *Institute for Strategic Dialogue*, September 2015.
37. "This site exposes the raw truth about ISIS told by young British Muslims, and those from Syria and Iraq with first hand experience of ISIS' brutality", Open Your Eyes; "British Muslims against ISIS: Sulehman says #OpenYourEyes", YouTube, September 25, 2015 [55 views at time of writing]; "#OpenYourEyes: Message to young British Muslims", YouTube, September 18, 2015 [139 views at time of writing].
38. See http://www.truthaboutisis.com.
39. See http://www.openyoureyes.net, "about".
40. Richard LeBaron and William McCants, "Experts Weigh In (part 1): Can the United States Counter ISIS Propaganda?", Brookings Institution Markaz, June 17, 2015.
41. "British Muslim Leaders Issue Fatwa against Would-Be Jihadists", Press Association via the *Guardian*, August 31, 2014.
42. Jason Devaney, "British PM Cameron to BBC: ISIS Is 'Not an Islamic State'", Newsmax, June 29, 2015; Ashley Killough, "Strong Reaction to Obama Statement: 'ISIL Is Not Islamic'", CNN, September 11, 2014.
43. See http://www.isisnotinmyname.com.
44. Adam Chandler, "The Roots of #illridewithyou", *Atlantic*, December 15, 2014; "Sydney Café: Australians Say to Muslims 'I'll Ride with You'", BBC Trending, December 15, 2014.

ABOUT THE AUTHORS

Katrina Elledge

Katrina Elledge is a senior US Defense Department analyst. She is the author of the recent study "Ukraine: Dissident Capabilities in the Cyber Age", under the auspices of the US National Intelligence University (NIU) in association with Pembroke College, University of Cambridge. Prior assignments include US Embassy Moscow, US European Command Headquarters, and the US Department of Defense in Washington DC.

David Patrikarakos

David Patrikarakos is the author of *Nuclear Iran: The Birth of an Atomic State*. He is a Contributing Editor at the Daily Beast, a Poynter fellow in journalism at Yale University and associate fellow at the School of Iranian Studies, University of St. Andrews. You can follow him on Twitter at @dpatrikarakos.

Peter Pomerantsev

Peter Pomerantsev is a Senior Fellow to the Transitions Forum at the Legatum Institute. He is also an author and documentary producer. His writing features regularly in the *London Review of Books,* the *Atlantic, Financial Times, Foreign Policy* and elsewhere, focusing largely, though not exclusively, on 21st century propaganda. Previously, Pomerantsev worked as a consultant on EU and World Bank development projects in the former USSR. His book about working as a TV producer in Putin's Russia, *Nothing is True and Everything is Possible*, was published by Faber in 2015.

Charlie Winter

Charlie Winter a Senior Research Associate to the Transcultural Conflict and Violence Initiative at Georgia State University. Previously, he was Quilliam's Senior Researcher on Transnational Jihadism, where he specialises in terrorist propaganda and the translation and analysis of Arabic-language documents circulated among jihadists online, including, among other things, a 10,000 word manifesto from Islamic State's Al-Khansaa' Brigade, an essay on the strategic importance of the Libyan jihad, and a personal account of life for women in the 'caliphate', published by the pro-IS al-Wafaa' Foundation. He has advised various governments on violent extremism policy in the MENA region and presented his research findings at UK Parliament and the Pentagon on a number of occasions. He makes regular appearances on national and international television and radio.

LEGATUM INSTITUTE
11 Charles Street
Mayfair
London W1J 5DW
United Kingdom

t: +44 (0) 20 7148 5400

Twitter: @LegatumInst

www.li.com
www.prosperity.com

978-1-911125-01-3

9 781911 125013

NOVEMBER 2015