Palmertz, Björn. "Influence operations and the modern information environment." *Hybrid Warfare: Security and Asymmetric Conflict in International Relations*. By Mikael Weissmann, Niklas Nilsson, Björn Palmertz and Per Thunholm . London: I.B. Tauris, 2021. 113–131. *Bloomsbury Collections*. Web. 26 Apr. 2023. <<http://dx.doi.org/10.5040/9781788317795.0014>>.

Downloaded from Bloomsbury Collections, www.bloomsburycollections.com, 26 April 2023, 13:07 UTC.

Copyright © Mikael Weissmann, Niklas Nilsson, Björn Palmertz and Per Thunholm 2021.
Released under a CC BY-NC-ND licence (<https://creativecommons.org/licenses/by-nc-nd/3.0/>).
You may share this work for non-commercial purposes only, provided you give attribution to the copyright holder and the publisher, and provide a link to the Creative Commons licence.

Influence operations and the modern information environment

Björn Palmertz

Introduction

The information environment and the vast potential for utilizing it in malicious activities have gained significant attention in the discussion on hybrid threats and hybrid warfare. Since the start of the millennium, the use of influence operations by both state and non-state actors has become increasingly obvious to decision makers and populations alike. The digital revolution affecting information dissemination and social exchange in our communities and the increased connectedness of key societal systems and infrastructure has opened up new opportunities as well as vulnerabilities. In addition, changes to labour markets and the demographic composition of many societies have broadened opportunities and horizons for parts of the public, but left others unsure of their place or representation in the traditional media or political sphere. This has had a direct effect both on national policies and international relations, not the least connected to various referendums and elections in, for example, the United Kingdom and the United States during 2016 and France in 2017. Aiming to clarify the wide range of related terms, Pamment et al. have employed ‘information influence activities’ to denote ‘the targeting of opinion-formation in illegitimate, though not necessarily illegal ways, by foreign actors or their proxies’.¹ They further highlight three terms developed by the Swedish government, forming a hierarchy of influence activities: influence activities (single use of illegitimate techniques); influence operations (multiple coordinated activities); and influence campaigns (multiple coordinated operations across the hybrid spectrum).²

The increasing focus as of late can at first glance make it seem as if influence techniques are somewhat new. In reality, such activities have been utilized in situations of peace, conflict and war throughout history. The difference today to a large degree rests with the speed with which dissemination of messaging and information can take place, as well as the capability to hide or obscure the origin or sender of a message. The use of automated accounts and algorithms can also aid both in collecting data, offering more precise target audience analysis, as well as enhance the dissemination so that information seems to engage or be shared by a larger group of people online

than is actually the case. In addition, offensive actors have the initiative as well as the advantage of being able to rapidly receive feedback on how information is received. Thus, their efforts can be redirected or withdrawn within a short time frame, depending on whether the perceived effects match their ambitions. The accessibility to target audiences in the modern information environment has also decreased the costs of conducting influence operations and increased the potential effects that can be achieved. Finally, such techniques can also be employed in conjunction with other hybrid threat capabilities. Brangetto and Veenendaal, for example, describe the benefits of combining offensive cyber operations with various influence methodologies: 'they are generally limited in scope and difficult to attribute, thereby limiting the risks of escalation and countermeasures. This is especially reflected in the Russian approach to Information Warfare, which considers it as an instrument of hard power.' They also highlight several illustrative examples such as the hacking of information systems, false flag cyberattacks, distributed denial of service attacks and doxing.³

To illustrate a number of techniques utilized in the current information environment Russia will be utilized as a main example, mainly since there are several high-profile actions to draw from that illustrate Russia's use of influence operations in recent years. This does not in any way mean that Russia is the only actor currently directing considerable resources towards this aim. The Chinese Communist Party has actively employed related strategies, as highlighted in a 2018 CSIS report: 'An aggressive strategy has sought to influence political decision-making, pursue unfair advantages in trade and business, suppress criticism of China, facilitate espionage opportunities, and influence overseas Chinese communities.'⁴ Other nations such as Iran have also been highlighted as utilizing, for example, 'coordinated inauthentic behaviour' through social media pages, groups and accounts targeting politics and elections in the US and UK.⁵ In addition, a number of non-governmental entities have devoted considerable effort to influencing various target audiences, especially through the use of social media and other web-based communication channels.⁶

The following sections first discuss targeting in the modern information environment, and then examine the employment of some prominent combined methodologies that have been observed during the last few years. It is worth noting that the use of these methodologies is in constant shift, in part due to the speed of technological advances, which impacts how users communicate and access information. In addition, the increasing awareness that a certain technique is being utilized reinforces resistance among a target audience and empowers key actors in a society to actively build resilience and counter-narratives. In this craft it is therefore imperative for offensive actors to consistently review their strategies and the means by which they are implemented.

Targeting

One of the key precursors enabling influence operations is targeting. As previously mentioned, information technology and the large amount of data available on social

media platforms offer new opportunities to identify target audiences and the most efficient way to reach them. The Cambridge Analytica case is one of the clearest examples of this in recent time. On 17 March 2018, *The New York Times*, along with *The Guardian* and *The Observer*, reported that Cambridge Analytica and its related company, Strategic Communication Laboratories, had harvested data of at least 50 million Facebook users and kept it without consent from the platform.⁷ Facebook suspended both Cambridge and SCL, and stated it knew about the breach, but had received legally binding guarantees from the company that all of the data was deleted. The data was used by Cambridge Analytica and SCL to conduct political targeting. More specifically, to build software to analyse personal preferences of voters for their clients which included the Donald Trump campaign team and, according to a whistleblower, the winning Brexit campaign. In July 2018, British Member of Parliament Damian Collins, heading a parliamentary inquiry into fake news, told CNN that the Information Commissioner's Office (ICO) had found evidence that files from Cambridge Analytica were accessed from Russia.⁸

The data was collected through an app called *thisisyourdigitallife*, built by academic Aleksandr Kogan who lived in Russia before moving to the United States at age seven. It was developed as a separate project initiated in 2014 apart from his affiliation with Cambridge University. He was also affiliated with St. Petersburg University, which he did not disclose to Cambridge, and received grants from the Russian government to research Facebook users' emotional states.⁹ Through his company Global Science Research, in collaboration with Cambridge Analytica, hundreds of thousands of users were paid to take a personality test and agreed to have their data collected for academic use. However, the app also collected the information of the test-takers' Facebook friends, leading to the accumulation of a considerable amount of user data.¹⁰ Facebook stated the collection had not been a data breach since Kogan 'gained access to this information in a legitimate way and through the proper channels' but 'did not subsequently abide by our rules' because he passed the information on to third parties.¹¹ Two days after the story surfaced, Britain's Channel 4 News released a series of undercover videos showing Cambridge Analytica executives appearing to say they could extort politicians, send women to entrap them and help proliferate propaganda to help their clients.¹² Alexander Nix was suspended from the position as CEO in late March after the videos were broadcasted. In May 2018, Cambridge Analytica and SCL announced they were closing down their business.¹³

Hacking

Gaining unauthorized entry to computer systems can, if exposed, in itself potentially influence the perspectives of certain target audiences and undermine the credibility of key functions in society. It can also serve to provide data and insights benefitting the targeting, timing and design of influence operations. In May 2016, in the lead-up to the US elections later that year, Arizona's voter registration system was taken offline after the FBI issued a warning of a cyber-threat. Investigations revealed that hackers

had attempted to penetrate the system, but failed. The state of Illinois, however, was less fortunate and a month later hackers gained access to 90,000 records including the names, dates of birth, gender, driver's licenses and partial social security numbers of registered voters. They had also unsuccessfully attempted to manipulate some of the accessed information.¹⁴ In a US Senate intelligence hearing in June 2017, cyber director at the Department of Homeland Security Sam Liles revealed that Russia had targeted election-related systems in a total of twenty-one states, including those of Arizona and Illinois.¹⁵ The aim of the operation was not entirely clear, but 'the cyber hacking of infrastructure associated with the election, such as voting systems and voter databases, provided the Russians with the techniques, materials, and familiarity with the US election system that can be applied to future Russian influence campaigns – in the US and perhaps elsewhere.'¹⁶

However, not only state owned systems have been targeted; media organizations are also of interest to Russian hackers. In 2015 a group calling themselves the Cyber Caliphate claimed to be responsible for planting malware with the aim of destroying the transmission system hardware for French channel TV5 Monde. Twelve channels were brought down for nine hours, but the attack could potentially have done much more damage. Thanks to technicians on duty, the infiltrated computer acting as a gate into the channel's network was identified and cut off from the internet.¹⁷ The so called Cyber Caliphate also propagated messages on Twitter expressing support for IS, which struck an especially sensitive chord in France due to the earlier attack on satire magazine Charlie Hebdo in which twelve people were killed and eleven wounded.¹⁸ It was later revealed that the French cyber security agency had found evidence that the real source of the attack was Russian hacker group APT 28. It has not been entirely established why TV5 was seen as an appropriate target, however, it fits with an ongoing trend. In recent years, hacker groups such as APT 28 have extended their actions beyond intelligence collection and espionage to intrusion operations encompassing a wider range of aims, such as enabling future influence activities or disrupting physical infrastructure.¹⁹ These types of hacks are clearly illustrated by two operations conducted against the Ukrainian power grid system in 2015 and 2016. The first left approximately 250,000 inhabitants without power for several hours.²⁰ The second resulted in a one-hour power outage in the Ukrainian capital region of Kiev.²¹ Several investigations have attributed these attacks to a hacker group called Sandworm, also known as Voodoo Bear and Telebots. Cyber security firm FireEye also found connections between Sandworm and Russia based on Russian-language documents found on the command and control servers used by the group – particularly an unaddressed vulnerability that had been presented at a Russian hacker conference, with an explicit Ukraine focus.²²

As mentioned earlier, collecting large amounts of user data from key platforms can be highly useful for intelligence purposes as well as planning influence campaigns. However, technological information property can be attractive for both state actors and companies seeking a shortcut to increase competitiveness. In September 2018, Facebook experienced a data breach where unknown attackers were able to exploit a core security failure and download the personal data of approximately 50 million users. The data stolen included the user's name, email, phone number, date of birth and posts on the platform.²³ As the information about the breach became public, Facebook in

early October acknowledged a second major data leak. This time the Russian company SocialDataHub and its sister firm, Fubutech, had downloaded such a large amount of data from the platform that its marketing materials claimed it essentially had a mirror of the Russian portion of Facebook. In Facebook's assessment, this leak was driven in part by the Russian company's need to mass harvest imagery from Facebook in order to build facial recognition models that could be used by the Russian government for surveillance purposes.²⁴

Leaking and doxing

Information accessed through hacking, sometimes complemented by open sources, is not always solely attained for intelligence purposes. It can also be utilized to enhance the effect of influence operations, whereby selected parts of the information are disseminated primarily through web-based platforms. This technique is called doxing – the practice of revealing and publicizing information on an organization or an individual that is private or classified, so as to publically shame or embarrass the target.

The most prominent doxing conducted by Russia occurred during the run-up to the US elections in 2016. In March, Hillary Clinton's campaign manager John Podesta received an email from what seemed to be Google, asking him to immediately change his password. The message was reviewed by the IT department but was, according to later statements, mistakenly assessed as 'legitimate'. The real source of the message, according to investigations by several cyber security firms²⁵ as well as US intelligence agencies,²⁶ was the Russian hacker group APT 28. As John Podesta's staff changed the email password, they gave the hackers access to over 50,000 of John Podesta's emails.²⁷ Two months later, the day after the Democratic National Committee revealed that they had been hacked, an anonymous internet user started releasing the stolen data, accompanied by WikiLeaks a week later. This process carried on until the elections on 8 November. On several occasions, the continuous doxing was timed to maximize its potential media coverage. One example followed the Obama-administration's release of a statement on 7 October, naming the Russian leadership as responsible for the influence campaign against the US elections. *The Washington Post* thirty minutes later released taped recordings by TV-show 'Access Hollywood', where Donald Trump could be heard making denigrating statements about women.²⁸ Another thirty minutes later, WikiLeaks started releasing email conversations involving Podesta, pointing to presidential candidate Clinton's connections to major banks, an issue which had already been brought up against Clinton in prior debates. Treverton describes how this 'demonstrates the Kremlin's clear preference for candidate Trump and its assistance in helping to increase Trump's electoral chances.'²⁹ In October 2018, the UK National Cyber Security Centre issued further clarification regarding APT 28, describing in a 'high confidence assessment' the identification of several cyberattacks against political institutions, companies as well as media- and sports organizations orchestrated by the Russian intelligence service GRU. They also stated that, among other groups, APT 28 and its many aliases such as Fancy Bear, Pawnstorm and Cyber Caliphate are associated with the GRU.³⁰

Emmanuel Macron's 2017 presidential campaign in France was, like the DNC in the United States, also targeted by a spear-phishing campaign where nine gigabytes of emails and campaign documents were later leaked on the text storage site Pastebin.³¹ Within half an hour, discussion threads on the forum site 4chan linked to the material. Soon thereafter, a US journalist working for an alt-right website also linked to the material on Twitter and later told BBC that the 4chan user posting the links had notified him in advance that the material was to be released. The timing was well planned, as the data was published just a few hours before the political reporting ban placed on French media forty-four hours before the voting.³² The dissemination that followed was considerable and rapid, amounting to 47,000 retweets within a few hours. According to Atlantic Council's Digital Forensic Research Lab, this is an indicator that automated accounts, so called bots, were involved in the process.³³ The Macron team, in part due to the experience of the US elections the year prior, was nevertheless prepared to be targeted. Already a few months before, cybersecurity firm Trend Micro had identified attempts by APT 28 to get into the Macron campaign's computer systems through spear-phishing. The Macron team therefore prepared by hiring cyber security experts, enacting technical as well as psychological defensive procedures, and acted offensively as the spear-phishing attempts started appearing. One method was to deliberately seed fabricated information to the hackers. Mounir Mahjoubi, the IT director for Macron stated: 'You can flood these [phishing] addresses with multiple passwords and log-ins, true ones, false ones, so the people behind them use up a lot of time trying to figure them out.'³⁴ Five minutes before the reporting ban was activated, the Macron campaign also managed to do a press release condemning the doxing attempt and explaining how they had been targeted by a coordinated hack several weeks before.³⁵ However, the failure of this influence attempt was also in part based on an incorrect expectation of effect. The resistance from French media to walk into a foreign influence dissemination trap was well established at this point, and the operation lacked a cultural analysis – some fabricated documents inserted into the leaks by the Russian hackers were rather amateurishly forged. Also, a large portion of the dissemination on the internet took place in English, with support from US alt-right actors, which is not ideal when attempting to reach and influence French target audiences.³⁶

Distributed denial of service attacks

An indirect signalling method, while potentially creating a sense of vulnerability as well as diminishing the credibility of foreign entities, is the DDoS attack. It refers to disrupting the services of a host computer connected to the internet by flooding it with pointless requests from a distributed network of external machines. The aim is to 'block the entrance' to the server and ensure that none of the legitimate requests get fulfilled. On the spectrum of complexity in the realm of cyberattacks, the technique behind a DDoS attack is rather simple and can be conducted without any major investment in infrastructure, since control over a network can be attained by discreetly renting a botnet or illicitly hijacking the machines of others. These can be computers but also

other products connected to the internet. In terms of knowledge there is no shortage of consulting services or even helpful software tools available if someone is willing to pay. During Russia's conflict with Ukraine, DDoS attacks were also part of the package of offensive tools employed by both sides. Baerzner and Robin describe how

this kind of cyberattack was used multiple times by both parties to the conflict; Ukrainian media websites were targeted by pro-Russian hackers in November 2013, for instance, and Russian media websites were attacked by pro-Ukrainian hackers in December 2013. DDoS attacks can also serve as a distraction in order to monopolize the attention of the emergency team of the targeted institution. While they are busy combating the DDoS attack, the perpetrator(s) can conduct other malicious activities on the relevant network such as installing a backdoor or malware in order to steal data.³⁷

In March 2016, a number of Swedish media organizations were similarly targeted by DDoS attacks, leaving some difficult to access for up to five days. At the same time, the amount of data traffic between Sweden and Russia increased, which is not in itself enough to attribute any form of attack.³⁸ Two years later, however, in a freedom-of-information-act release of an internal US State Department cable from October 2016, the attack against nine Swedish news sites was described as part of a Russian campaign to sow disinformation about NATO. The cable was the first confirmation that Russia was suspected in the March 2016 attacks in Sweden, which came as the Swedish government was debating whether to approve a cooperation treaty with NATO.³⁹ The agreement was approved by the Swedish parliament in summer 2016.

These operations fall within the methodology of what Cohen and Bar'el refer to as Computer Network Influence (CNI) operations: 'In contrast with standard attacks launched against computer networks, CNI is designed to create the sense of a momentous strike without actually executing one. CNI attacks are meant to instill a sense of insecurity and a lack of control, compromising sovereignty with an inability to safeguard a normative way of life. Examples of such attacks include crippling government sites, sending damaging messages to civilians and shutting down media sites for limited stretches of time.'⁴⁰

Disinformation

Today, social media combine text, images, video and verbal commentary with new and practically instant means of dissemination. These new communication channels also enable a direct line to foreign target audiences without having to consider actors that previously had a stronger role as filters or gatekeepers, for example politicians, academics, experts and established media organizations. The opportunities to utilize disinformation have therefore increased, and they are especially attractive to authoritarian regimes. This also results in an inherent asymmetry. While influence efforts targeting foreign target audiences can benefit from the openness of democratic

societies, authoritarian states can implement restrictions in their own domestic information environment, delimiting communication between their own population and external actors. Russia's use of legislation where certain entities are labelled as foreign agents is one example; others include limitations to foreign ownership of media companies, complicating independent journalism and placing limitations on, and actively policing, what can be accessed on the internet within the country.

Giles specifically points out that compared to the time before the internet, seeding information is much easier today. This is partly due to the fact that it is easier for stories to be designed to trend and creep into the reporting of established and credible media sources in natural and legitimate ways.⁴¹

Such opportunities are especially evident during crises or other situations in democratic societies when there is social unrest or turmoil, and the Covid-19 pandemic is a clear example. Pamment describes that Russia and China have been running image campaigns with disinformation components to frame their handling of the crisis. The communication combines both official and reasonably transparent methods such as public diplomacy and state media reporting, with more covert influence and cyber-related activities. To further complicate the information environment various criminal groups have attempted to benefit from the crisis by spreading clickbait or by running phishing scams. Highlighting the potential effects Pamment states:

There are profound health and public safety risks associated with the disinformation connected to these campaigns, as well as to the activities of criminal and hacker groups. These campaigns aim to undermine trust in institutions and to poison the climate of debate. Some aspects of these campaigns demonstrate efforts to erode freedom of thought and expression. Some of these activities also pose emerging short-term and long-term risks to personal, organizational, and national security.⁴²

A recent report outlines some of the more prominent themes of the Covid-19 pandemic, as identified by independent fact checking organizations in Italy, Spain, Germany, France and the UK. It is important to note that these are not always authored or disseminated with the purpose of causing harm, and would then be seen as misinformation, but could also be injected into the information environment with the intent to cause harm and hence would be labelled as disinformation. The themes include (1) misleading medical advice around supposed cures and remedies for Covid-19, (2) the belief that Covid-19 is caused or worsened by 5G mobile phone technology, (3) advice on how to avoid or prevent infection, at times mixing partially accurate information with unsound medical advice, sometimes falsely attributed to an authority on the subject, (4) claims that the virus was created deliberately, (5) rumours and conspiracy theories related to vaccines such as false claims surrounding mandatory vaccination or vaccines being ready or imminent and (6) a theme centred on face masks and personal protective equipment including claims that masks may be harmful or inaccurate rumours surrounding the logistical supply of personal protective equipment.⁴³

Another opportunity utilized during recent years is termed information laundering – how tools of influence operations can be used to penetrate a target media ecosystem

and use it as an echo chamber.⁴⁴ A report from the Swedish Center for Russian Studies underlines that Russian media narratives are designed by a number of leading national media outlets such as RT, Sputnik and Rossiyskaya Gazeta. Due to the limited impact of these media sources among Western target audiences, they actively utilize social media to increase their exposure. Their most important avenues, however, are Western media outlets that have a larger audience including far-right populist outlets such as Infowars, Breitbart and Voice of Europe. Articles on these sites are also on occasion remarkably similar to those of Sputnik, even if they are not attributed to that source. This enables narratives to reach a target audience without the potentially stigmatizing label of an overt Russian origin. It also makes possible multiple exposures as a reader visits different media sites, even though the origin may be the one and same article authored by Russian media outlets funded by the state. SCRS summarizes the technique and describes how

both RT and Sputnik often rewrite articles from local sources. They use the domestic tone and level of exaggeration and hatred towards the establishment. This is both easy and cheap and all responsibility lies on the local, primary source, not the Russian outlet. RTs and Sputnik's English-language versions primarily feed Western media outlets with material, rather than the media consumers directly, thereby not showing to the vast majority of the media consumers that Russian media has an important part in the selection, formulation and distribution of the news.⁴⁵

Sometimes mistakes made by established media channels themselves present opportunities that makes this aim easier to attain. On 11 May 2018 Swedish local newspaper Smalandsposten published a news article with a title reading 'Catholic Church were denied ringing church bells – could disturb nearby residents'.⁴⁶ The context, which was included in the introduction to the article, was that a Muslim congregation in the town of Vaxjo had been permitted to transmit prayer calls through loudspeaker for three minutes and forty-five seconds each Friday. The information about the previous denial to the catholic congregation came from an employee of the church interviewed in the article. Additional information that the application for ringing church bells was made ten to fifteen years prior was later added to the article. However, when Swedish radio station P4 began researching the issue they could not find records of any such application; the local county office and the police searched their records back to 1996 without result. By then, the topic had nevertheless garnered a substantial dissemination on various anti-immigration focused websites and social media platforms such as Facebook.⁴⁷ On 12 May, right-wing populist website Voice of Europe, based in Holland, published a brief article titled 'Sweden: Church calls forbidden in town where mosque is allowed to air 110dB Islamic call to prayer'. On 14 May, Sputnik news followed suit with the headline 'Swedish City Allows 110 DB Muslim Prayer Calls, Rejects Church Clock Ringing'.⁴⁸ Sputniks attempt to amplify the propagation of the initial incorrect article through established media sites was, however, superfluous – they did that very well on their own. Well-established Swedish outlets like Expressen, TV4, Metro and The Local all carried rewrites of

the Smalandsposten article, lending their credibility to the incorrect story. They thereby indirectly legitimized Russian narratives, including that the Swedish political establishment is guided by political correctness regarding migration and other issues, whereas migrants or Islamists have too much power in society, which affects decision-making and creates problems for Sweden.⁴⁹

Shekhovtsov has conducted a thorough investigation of the relationship between the Russian leadership and Western far-right groups. He explains the historical reasons why a shared information space could develop between the Soviet Union and far-right movements in the cold war era. First, both fascism and communism are revolutionary and totalitarian ideologies – a concurrence in the thrust towards a new civilization, even though the two belief systems have inherently different myths and values. Second, both fascism and communism envision a society that challenges the principles of liberalism. This creates a shared space of perspectives where the ‘decadent and degenerate’ liberalism poses a threat.⁵⁰ A recent report released by the National Endowment for Democracy states that authoritarian states do not use influence operations to attract foreign audiences, but rather to make the societal systems of the West appear less appealing:

Contrary to some prevailing analysis, the attempt by Beijing and Moscow to wield influence through initiatives in the spheres of media, culture, think tanks, and academia is neither a ‘charm offensive’ nor an effort to ‘win hearts and minds’, . . . This authoritarian influence is not principally about attraction or even persuasion; instead, it centres on distraction and manipulation.⁵¹

One very clear example of a strategy exploiting distrust, polarization and previous political credibility failures in the West occurred in mid-2014. It also points to the asymmetrical opportunities for a Russian media company in the West, versus a Western media company in Russia. The Russian state owned media channel RT, which focuses on foreign audiences, launched a guerrilla advertising campaign in New York and Washington, DC, consisting of ‘wild postings’ in the words of RT spokesperson Anna Belkina. The core messages of the various posters were tied to an anti-mainstream media narrative proclaiming that people should ‘question more’ and go to RT.com for the second opinion. Some of the themes used were ‘In case they shut us down on TV’ and a drawing of former Secretary of State Colin Powell accompanied by the message ‘This is what happens when there is no second opinion. Iraq War: No Weapons of Mass Destruction, 141,802 civilian deaths.’⁵² A few months later, RT also published a YouTube video featuring interviews with Americans on the street asking them what they thought of the campaign. All comments featured were positive to the campaign and focused on the design of the posters and the anti-establishment message. One man stated, ‘You know, all the propaganda that we are being shoved by our political powers. They say one thing on television to try to put us at ease, but in reality, it is not really congruent with the truth’, and another ‘It is embarrassing that we are such sheep; that’s my first reaction. That the messages that we get, we accept without question, and the consequences (points to RT poster) are really serious.’⁵³ It would be interesting to know if the interviewees were informed in advance that RT is funded by the Russian state, at

the time ranked 148th of 180 countries on Reporters without Borders Press Freedom Index, lower than nations such as Zimbabwe, Chad and Cambodia.⁵⁴

A more sophisticated method of generating and spreading disinformation as part of an influence operation is by building networks utilizing unsuspecting individuals or movements in a targeted country. On 1 September 2020 Facebook reported shutting down such a network, after receiving information from the FBI, associated with past activity by the Russian Internet Research Agency (IRA) for violating their policy against foreign interference.⁵⁵ The thirteen associated accounts and two pages on Facebook centred on a website domain named PeaceData launched a few months earlier that pretended to be an independent news outlet. The accounts included fictitious personas with AI-generated profile pictures who posed as news editors from various countries. These were then used to recruit a number of freelance journalists who were not aware of the origin of their paid assignments to write on popular topics primarily targeting an audience on the left of the political spectrum. In addition they sought to obtain political advertising authorization to run ads in the US. Some of the topics they focused on were social and racial justice in the United States and the United Kingdom, alleged Western war crimes and corruption, environmental issues, the coronavirus pandemic, the Biden-Harris campaign, the QAnon conspiracy theory and the policies of President Trump. The network was taken down during its early stages and did not garner significant traction in terms of audience or amplification of its content, but according to Nimmo et al. illustrates a development of IRA-influence tactics: (1) the use of AI-generated profile pictures, (2) employing real, but unwitting, authors with a layer of seeming authenticity between the originator and the audience, (3) using a smaller number of well-crafted accounts to target communities and publications rather than the mass audience approach seen during earlier election campaigns and (4) employing a more precise targeting than during prior operations, in this case aiming messages mainly at a limited number of left-leaning political groups.⁵⁶

Social media advertising

An additional technique used by Russia in their influence campaign during the 2016 US election campaign was advertisements coordinated and created by the IRA placed on social media platforms, among others Facebook, Instagram and Google. According to DiResta et al., IRA initiated operations during 2013 in St. Petersburg, Russia. Organized like a marketing agency, they have employed and trained over a thousand people to engage in round-the-clock influence operations. Their target audiences include Russian and Ukrainian citizens, as well as, well before the 2016 US election, Americans. In that operation they reached 126 million people on Facebook, at least 20 million users on Instagram, 1.4 million users on Twitter and uploaded over 1,000 videos to YouTube.⁵⁷ A company can advertise on Facebook using its Ads Manager software, which enables them to target users based on interests and behaviours. An analysis conducted by Howard et al. shows that the Russian IRA utilized this information to segment Facebook and Instagram users based on race, ethnicity and identity. Thanks to the

functionality of the ad software they could also identify more specific interests within each ethnic group, for example nationalism, immigration or identity. They then put together an online advertising campaign that ran between 2015 and 2017, attracting users to Facebook pages they controlled and posting content they deemed effective for the specific target audience. The campaign consisted of 73 different Facebook pages and Instagram accounts as well as 3,519 ads attempting to get users to like pages, follow Instagram accounts, join events and visit various websites.

Howard et al. identify two communication strategies:

The first involved appealing to the narratives common within a specific group, such as supporting veterans and police, or pride in race and heritage, as a clickbait strategy to drive traffic to the Facebook and Instagram pages the IRA set up. Based on an analysis of both ads and posts, we find that the IRA posted content on these pages to which they drove traffic with ads. Then the pages posted content that intended to elicit outrage from these groups.

They conclude that the messaging aimed at these target audiences was designed to push and pull them in different ways. The overarching aim, however, was clear: to benefit the Republican Party and presidential candidate Donald Trump. In campaigns targeting conservatives and right-wing voters, the messaging encouraged these groups to support the Trump campaign. For key groups that could challenge Trump, the messaging instead sought to confuse, distract and ultimately discourage members from voting.⁵⁸

Organized trolling and amplification by social bots

The changing patterns of how people communicate, share and consume information through social media platforms and applications utilizing the internet have given rise to a number of techniques. Although not new in terms of their underlying aim and methodological starting point, the use of organized trolling and bots are techniques that have been developed to fit the digital information landscape. Trolling can be utilized to distort perceptions of what public opinion looks like and disrupt or silence key communicators with opposing voices. In combination with this, bots, automated accounts impersonating humans, can amplify specific narratives in a manner that at first glance looks organic, but in reality is artificially generated. Bots can also aid in the dissemination of malware. The term 'social bot' refers to automated software that acts through a social media account. It is important to note that the credibility of bot behaviour varies greatly, since the efforts put into mimicking human behaviour depend on the goals of the operator managing the bots.⁵⁹ Bodine-Baron et al. differentiate between bots and trolls. Bot accounts automatically post or share information on social media platforms under the direction of humans.⁶⁰ Troll accounts, on the other hand, are operated by humans. It should be underlined that not all trolling activities or bot accounts are connected to influence operations or other organized malign

activities. The original definition of a troll was a person that intentionally engaged in polarizing or annoying messaging online in order to get attention or otherwise cause trouble.⁶¹

In a study of Russian state-sponsored trolls, Zannettou et al. made a number of interesting findings. They used a mathematical method (Hawkes Processes) to model how several communities influenced each other – the Russian troll accounts on Twitter and overall baseline account activity on Twitter as well as social forum platforms Reddit and 4chan. Key observations include that trolls were actively involved in spreading content related to world news and politics, including Russian narratives on topics such as terrorist group IS and Islam. Several troll accounts were also created or repurposed in the weeks leading up to noteworthy world events, including the Republican National Convention or the Charlottesville rally. Accounts in both troll and baseline samples reached a large number of Twitter users with their messages, ranging from 1,000 up to 145,000 followers. This indicates that the amount of followers of the troll accounts is sufficient to share certain narratives with a large number of Twitter users. One behaviour separating the trolls from the baseline was that while random Twitter users mainly tweet from the mobile app, most of the Russian trolls utilized the web client. Zannettou et al. summarize that the influence of the troll accounts studied actually appears quite limited with respect to the baseline platforms: ‘With the exception of news originating from the Russian state-sponsored news outlet RT (formerly Russia Today), the troll accounts were generally less influential than other users on Reddit, Twitter, and 4chan.’ A plausible explanation is that troll accounts are simply not terribly efficient at spreading news – they are more concerned with causing havoc by pushing ideas, engaging other users, or even taking both sides in controversial online discussions.⁶²

Swedish journalists recently examined topics relating to Sweden in a dataset of three million tweets collected by researchers at Clemson University. The data was connected to over 2,800 troll accounts that have been suspended by Twitter. In a comment one of the researchers in the project, professor Darren Linvill, stated that he was surprised by how well organized the troll accounts were. The accounts were of different types and were utilized depending on what happened in the world and what time it was. At 2.00 pm, all the Russian trolls may have been tweeting from left-leaning accounts, then simultaneously switching over to their right-leaning accounts at exactly 3.00 pm. The analysis found 330 English-language accounts that published a total of 1,920 tweets about Sweden. The amount of related messages continuously increased from the time the accounts were activated in 2014 until their peak in 2017. About 1,200 of the tweets were on topics relating to crime, immigration and Muslims. On occasion the accounts took various sides in controversial issues to add fuel to the fire. When President Trump in 2017 exclaimed ‘Look at what happened last night in Sweden’ in a speech to his followers, he was mocked by troll accounts pretending to have a left-leaning stance, while right-leaning troll accounts claimed that he was correct and that Sweden was in a constant state of crisis due to immigration.⁶³

An especially relevant example of research in light of the Covid-19 pandemic and illustrating how a specific subject area can be targeted was presented in a 2018 paper by Broniatowski et al. It is based on Twitter data from 2014 to 2017 which was analysed

to see how bots and trolls participated in the online vaccine debate. The findings of the analysis concerning content and number of posts were that

Russian trolls and sophisticated Twitter bots post content about vaccination at significantly higher rates than does the average user. Content from these sources gives equal attention to pro- and anti-vaccination arguments. This is consistent with a strategy of promoting discord across a range of controversial topics – a known tactic employed by Russian troll accounts.⁶⁴

In a recent paper, Broniatowski et al. presented an example of how a specific subject area can be targeted. Twitter data was collected from 2014 to 2017 to see how bots and trolls participated in the online vaccine debate. Concerning content and number of posts, the analysis found that Russian trolls and sophisticated Twitter bots post content about vaccination at significantly higher rates than does the average user, and that they give equal attention to pro- and anti-vaccination arguments. Actions consistent with a strategy of promoting discord across a range of controversial topics – a known tactic employed by Russian troll accounts.⁶⁵ Lazer et al. recently summarized the challenge concerning amplification by bots on social media platforms: by liking, sharing, and searching for information, social bots (automated accounts impersonating humans) can magnify the spread of fake news by orders of magnitude. By one recent estimate – that classified accounts based on observable features such as sharing behaviour, number of ties, and linguistic features – between 9 and 15 per cent of active Twitter accounts are bots. Facebook estimated that as many as 60 million bots may be infesting its platform. They were responsible for a substantial portion of political content posted during the 2016 US campaign, and some of the same bots were later used to attempt to influence the 2017 French election. Bots are also deployed to manipulate algorithms used to predict potential engagement with content by a wider population.⁶⁶

The development of advanced social bot software is moving along at a rapid pace. Today, automatic accounts can scrape the web for information then used to build a credible profile, independently comment on other users' posts, disseminate collected information at specific times and emulate the production of human organic content at a pace that looks lifelike at a glance. Ferrara et al. underline the importance of improved awareness and knowledge in democracies regarding the utilization of social bots. They conclude that bots can 'hinder the advancement of public policy by creating the impression of a grassroots movement of contrarians, or contribute to the strong polarization of political discussion observed in social media. They can alter the perception of social media influence, artificially enlarging the audience of some people, or they can ruin the reputation of a company, for commercial or political purposes.'⁶⁷

Conclusion

Influence operations employ a wide range of methodologies and tools, but they all benefit from the large amount of readily available data, which makes it possible to learn how a foreign information environment works from a distance. The ability to

evaluate and realign operations has also increased greatly. With the speed, reach and opportunities for anonymity in today's communication channels, it is also easier to engage or disrupt actors in that environment without revealing your identity and true motivations. The debate, and institutional roles, in Western societies often separate cyber- and influence operations. In reality, Russia and other capable offensive actors combine these capabilities when needed. This includes employing social engineering methods to lure users into opening the door to a system so that data can be extracted. It can also involve hacking into and disrupting critical infrastructure systems potentially affecting government credibility or arousing fear among the population in another country. Disseminating messages that fuel polarization and distort the public debate in another country also serves an important purpose. If a country experiences internal strife and politicians or the public struggle to find common ground, they will have less energy and focus to expend on containing and countering the strategies and actions of the offensive actor.

In light of these challenges, how can key actors in a society then limit the effects of malign influence operations? Public awareness is a first line of defence and proactive strategic communication and transparency from the national leadership and other key communicators is therefore vital. This can sustain focus on the issue and minimize the effect of disinformation, while upholding credibility and long-term communication between decision makers and the population. Communication strategies need to be adapted to an information environment where the number of channels to reach the population is considerably more diverse than just a decade ago. This requires a greater knowledge concerning key target audiences; what are their motivations, concerns and experiences, which channels do they use and how should messages be framed to be understandable and effective? Another key aspect is to incorporate relevant skill sets into security- and intelligence agencies, since the ability to maintain situational awareness is a key precondition for several other response and resilience areas. Since influence operations can take aim at many different situations or actors across the public and private sector, it is also important to close potential responsibility or perception gaps that can be exploited by an opponent. One way of reducing these can be to develop an entity that enables information sharing, training and collaboration for key societal actors, as well as maintaining comprehensive tracking of influence-related threats and an early warning mechanism. This can also facilitate long-term relationships with related core capabilities such as law, cyber security and intelligence. Finally, legal frameworks may need to be revised and developed – an undertaking that needs to be adapted to existing legislation and the current information environment, where data flows freely but under the surface has become a very valuable commodity that is traded globally.

Notes

- 1 James Pamment, Howard Nothhaft, Henrik Agardh-Twetman and Alicia Fjällhed, *Countering Information Influence Activities: The State of the Art* (Lund: Lund University, 2018), 8.

- 2 Alicia Wanless and James Pamment, 'How Do You Define a Problem Like Influence?' *Journal of Information Warfare* 18, no. 3 (2019): 1–14.
- 3 Pascal Brangetto and Matthijs Veenendaal, *Influence Cyber Operations: The Use of Cyberattacks in Support of Influence Operations* (NATO CCD COE, 2016).
- 4 Canadian Security Intelligence Service, *China and the Age of Strategic Rivalry: Highlights from an Academic Outreach Workshop* (2018), 75.
- 5 Kanishk Karan, Ayushman Kaul and Ben Nimmo, 'Facebook Removes Iran-based Assets. Again', *Atlantic Council Digital Forensic Research Lab*, 30 May 2019. <https://medium.com/dfrlab/facebook-removes-iran-based-assets-again-fl7358ef21f>.
- 6 Katie Cohen and Lisa Kaati, *Digital Jihad – Propaganda from the Islamic State* (Swedish Defence Research Agency, 2018); Diana Rieger, Lena Frischlich and Gary Bente, *Propaganda 2.0: Psychological Effects of Right-Wing and Islamic Extremist Internet Videos* (Terrorism/Extremism Research Unit of the German Federal Criminal Police Office, 2013); Kate Starbird, *Examining the Alternative Media Ecosystem through the Production of Alternative Narratives of Mass Shooting Events on Twitter* (11th International AAAI Conference on Web and Social Media (ICWSM), 2017).
- 7 Carole Cadwalladr and Emma Graham-Harrison, 'Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach', *The Guardian*, 17 March 2018.
- 8 Donie O'Sullivan, Drew Griffin and Patricia DiCarlo, 'Cambridge Analytica's Facebook Data was Accessed from Russia, MP Says', *CNN*, 17 July 2018.
- 9 Carole Cadwalladr and Emma Graham-Harrison, 'Cambridge Analytica: Links to Moscow Oil Firm and St Petersburg University', *The Guardian*, 17 March 2018.
- 10 Paul Lewis and Julia C. Wong, 'Facebook Employs Psychologist Whose Firm Sold Data to Cambridge Analytica', *The Guardian*, 18 March 2018.
- 11 Paul Grewal, 'Suspending Cambridge Analytica and SCL Group From Facebook', *Facebook Newsroom*, 16 March 2018. <https://about.fb.com/news/2018/03/suspending-cambridge-analytica/>.
- 12 Channel 4 News, 'Exposed: Undercover Secrets of Trump's Data Firm', 20 March 2018. <https://www.channel4.com/news/exposed-undercover-secrets-of-donald-trump-data-firm-cambridge-analytica>.
- 13 Aliya Ram and Hannah Kuchler, 'Cambridge Analytica Shuts Down and Blames "media siege"', *Financial Times*, 2 May 2018. <https://www.ft.com/content/a0345598-4e37-11e8-a7a9-37318e776bab>.
- 14 Michael Riley and Jordan Robertson, 'Russian Cyber Hacks on U.S. Electoral System Far Wider than Previously Known', *Bloomberg*, 13 June 2017.
- 15 US Senate Select Committee on Intelligence, *Hearing on Russian Interference in the 2016 U.S. Elections*, 21 June 2017. <https://www.intelligence.senate.gov/hearings/open-hearing-russian-interference-2016-us-elections#>.
- 16 Gregory F. Treverton, Andrew Thvedt, Alicia R. Chen, Kathy Lee and Madeline McCue, *Addressing Hybrid Threats* (Center for Asymmetric Threat Studies and Hybrid CoE, 2018).
- 17 BBC News, 'How France's TV5 was Almost Destroyed by "Russian hackers"', 10 October 2015.
- 18 Feike Hacquabord, *Two Years of Pawn Storm: Examining an Increasingly Relevant Threat* (Trend Micro, 2017). <https://blog.trendmicro.com/pawn-storm-power-social-engineering/>.
- 19 CrowdStrike, 'Who Is Fancy Bear (APT28)?', 12 February 2019. <https://www.crowdstrike.com/blog/who-is-fancy-bear/>.

- 20 Kim Zetter, 'Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid', *WIRED*, 3 March 2016.
- 21 Marie Baezner and Patrice Robin, *Cyber and Information Warfare in the Ukrainian Conflict* (Eidgenössische Technische Hochschule Zürich, 2018).
- 22 Andy Greenberg, 'Your Guide to Russia's Infrastructure Hacking Teams', *WIRED*, 12 July 2017.
- 23 Mike Isaac and Sheera Frenkel, 'Facebook Security Breach Exposes Accounts of 50 Million Users', *New York Times*, 28 September 2018.
- 24 Jack Nicas, 'Facebook Says Russian Firms "Scraped" Data, Some for Facial Recognition', *New York Times*, 12 October 2018.
- 25 Lorenzo Francheschi-Bicchierai, 'How Hackers Broke Into John Podesta and Colin Powell's Gmail Accounts', *Motherboard-VICE*, 20 October 2016.
- 26 Office of the Director of National Intelligence, *Assessing Russian Activities and Intentions in Recent US Elections*, 6 January 2017. https://www.dni.gov/files/documents/ICA_2017_01.pdf.
- 27 Jim Sciutto, 'How One Typo Helped let Russian Hackers In', *CNN*, 28 June 2017.
- 28 David A. Farenthold, 'Trump Recorded Having Extremely Lewd Conversation about Women in 2005', *Washington Post*, 8 October 2016.
- 29 Treverton et al., *Addressing Hybrid Threats*.
- 30 UK National Cyber Security Center, *Reckless Campaign of Cyber Attacks by Russian Military Intelligence Service Exposed*, 4 October 2018.
- 31 Heather A. Conley and Jean-Baptiste Jeangène Vilmer, *Successfully Countering Russian Electoral Interference* (Center for Strategic & International Studies, 2018).
- 32 France 24, 'French Media Rules Prohibit Election Coverage over Weekend', 7 May 2017.
- 33 Ben Nimmo, Naz Durakgolu, Maks Czuperski and Nicholas Yap, 'Hashtag Campaign: #MacronLeaks: Alt-right Attacks Macron in Last Ditch Effort to Sway French Election', *Atlantic Council DFRLab*, 6 May 2017.
- 34 Christopher Dickey, 'Did Macron Outsmart Campaign Hackers?', *The Daily Beast*, 6 May 2017.
- 35 BBC News, 'French Election: Emmanuel Macron Condemns "massive" Hack Attack', 6 May 2017.
- 36 Conley and Jeangène Vilmer, *Successfully Countering*.
- 37 Baezner and Robin, *Cyber and Information Warfare*.
- 38 Swedish Defence Research Agency, *DDOS-attack visar behovet av att säkra samhällets infrastruktur*, 21 March 2016.
- 39 Kevin Collier and Jason Leopold, 'Russian Hackers Targeted Swedish News Sites In 2016, State Department Cable Says', *BuzzFeed*, 8 October 2018.
- 40 Daniel Cohen and Ofir Bar'el, *The Use of Cyberwarfare in Influence Operations* (Tel Aviv University, Yuval Ne'eman Workshop for Science, Technology and Security, 2017).
- 41 Keir Giles, *The Next Phase of Russian Information Warfare* (NATO StratCom COE, 2016).
- 42 J. Pamment, 'The EU's Role in Fighting Disinformation: Taking Back the Initiative' (Carnegie Endowment for International Peace, 2020).
- 43 AFP, CORRECTIV, Pagella Politica/Facta, Full Fact and Maldita.es (2020) Infodemic Covid-19 in Europe: A Visual Analysis of Disinformation.
- 44 Biros Toucas, 'Exploring the Information-Laundering Ecosystem: The Russian Case', *Center for Strategic and International Studies*, 31 August 2017.

- 45 Swedish Center for Russian Studies, *Russian Influence on the Swedish Election 2018* (2018).
- 46 Per Jodenius, 'Katolska kyrkan vill ringa i klocka', *Smålandsposten*, 11 May 2018. <https://nxt.smp.se/vaxjo/katolska-kyrkan-nekades-klockringning-kunde-stora-villa-omrade/>
- 47 Hugo Ewald and Alexandra Carlsson Tenitskaja, 'Faktiskt helt felaktigt att katolska kyrkan nekades ringa klockor', *Dagens Nyheter*, 21 May 2018. <https://www.dn.se/nyheter/politik/faktiskt-helt-fel-att-katolska-kyrkan-nekades-ringa-klockor/>.
- 48 Sputnik News, 'Swedish City Allows 110 DB Muslim Prayer Calls, Rejects Church Clock Ringing', 14 May 2018. <https://sputniknews.com/europe/201805141064430526-sweden-mosque-loud-prayer-calls/>.
- 49 Swedish Center for Russian Studies, *Russian Narratives on Sweden in 2017* (2018).
- 50 Anton Shekhovtsov, *Russia and the Western Far Right* (New York: Routledge, 2018).
- 51 Juan Pablo Cardenal, Jacek Kucharczyk, Grigorij Mesežnikov and Gabriela Pleschová, *Sharp Power: Rising Authoritarian Influence* (Washington, DC: National Endowment for Democracy, 2017).
- 52 Rosie Gray, 'Russia Today's New Ad Campaign Suggests It Could Have Prevented The Iraq War', *BuzzFeed*, 18 August 2014.
- 53 RT, 'RT. For the Second Opinion', 6 October 2014. <https://www.youtube.com/watch?v=ynBr5AJdZP0>.
- 54 Reporters Without Borders, '2014 World Press Freedom Index'. <https://rsf.org/en/ranking/2014>.
- 55 Facebook (2020) August 2020 Coordinated Inauthentic Behavior Report.
- 56 B. Nimmo, C. Francois, C. Shawn Eib and L. Ronzaud, *IRA Again: Unlucky Thirteen – Facebook Takes Down Small, Recently Created Network Linked to Internet Research Agency* (Graphika, 2020).
- 57 Renee DiResta, Kris Shaffer, Becky Ruppel, David Sullivan, Robert Matney, Ryan Fox, Jonathan Albright and Ben Johnson, *The Tactics & Tropes of the Internet Research Agency* (Austin: New Knowledge, 2018).
- 58 Philip N. Howard, Bharath Ganesh and Dimitra Liotsiou, *The IRA, Social Media and Political Polarization in the United States, 2012-2018* (Oxford: University of Oxford Computational Propaganda Research Project, 2018).
- 59 Norah Abodokhair, Daisy Yoo and David W. McDonald, 'Dissecting a Social Botnet: Growth, Content and Influence in Twitter', in *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing*, Vancouver, 2015, 839–51.
- 60 Elizabeth Bodine-Baron, Todd C. Helmus, Andrew Radin and Elina Treyger, *Countering Russian Social Media Influence* (Santa Monica: RAND Corporation, 2018).
- 61 'Troll', in Cambridge Dictionary. <https://dictionary.cambridge.org/dictionary/english/troll>.
- 62 Savvas Zannettou, Tristan Caulfield, Emiliano De Cristofaroy, Michael Sirivianos, Gianluca Stringhini and Jeremy Blackburn, *Disinformation Warfare: Understanding State-Sponsored Trolls on Twitter and Their Influence on the Web* (Cyprus University of Technology, University College London & University of Alabama at Birmingham, 2018).
- 63 Mikael Delin, '2.000 Tweets från Putins Troll Handlar om Sverige – ett land i förfall', *Dagens Nyheter*, 31 August 2018.

- 64 David A. Broniatowski, Amelia M. Jamison, SiHua Qi, Lulwah AlKulaib, Tao Chen, Adrian Benton, Sandra C. Quinn and Mark Dredze, 'Weaponized Health Communication: Twitter Bots and Russian Trolls Amplify the Vaccine Debate', *American Journal of Public Health* 108, no. 10 (2018): 1378–84.
- 65 Broniatowski et al., 'Weaponized Health Communication', 1378–84.
- 66 David M. J. Lazer, Matthew A. Baum, Yochai Benkler, Adam J. Berinsky, Kelly M. Greenhill, Filippo Menczer, Miriam J. Metzger, Brendan Nyhan, Gordon Pennycook, David Rothschild, Michael Schudson, Steven A. Sloman, Cass R. Sunstein, Emily A. Thorson, Duncan J. Watts and Jonathan L. Zittrain, 'The Science of Fake News', *Science* 359, no. 6380 (9 March 2018): 1094–6.
- 67 Emilio Ferrara, Onur Varol, Clayton Davis, Filippo Menczer and Alessandro Flammini, 'The Rise of Social Bots', *Communications of the ACM* 59, no. 7 (2016): 96–104.