EUROZINE

Hacking, propaganda and electoral manipulation

Moscow’s information war on the West

Markus Wehner
21 July 2017

Europe long overlooked the extent of Russian attempts to influence politics in the West through disinformation and cyber warfare. Now the opposite may be the case. Markus Wehner assesses the risks, and looks at measures being taken by the German government.

It was only the hacking of the German Bundestag, the false rape case of Lisa F. and the hacking affair in the American presidential election that led to a widespread realisation of the massive scale of Moscow’s intervention in the internal politics of Western countries. There is no reason to over-dramatise the situation; but at a time of deep estrangement between Russia and the West following the annexation of Crimea and the war in eastern Ukraine, Russia’s leadership has opted for a policy of confrontation – adopting an approach that is both single-minded and flexible in the aim of dividing the West. So equally, there is no reason to give the all-clear.

Can Russia exert a sustained influence on the public mood, and thus the politics, of other countries through propaganda? Is it capable of manipulating foreign elections with its cyber attacks, and even of influencing their outcome? These questions have been the subject of intense debate in over the last year, particularly following the involvement of hackers, allegedly Russian, in the 2016 American presidential election. This stoked fears in Germany that the Kremlin could also interfere in the parliamentary elections in late September 2017. This might take the form of misinformation – targeted fake news – or cyber attacks, as have already been deployed against the Bundestag, against German MPs and political parties. What is disputed is the scale of the threat. Some people think that western democracies have so far failed to properly recognise Moscow’s influence – covert or not – and are inadequately equipped to fend off the manipulation attempts. Others warn against falling prey to anti-Russian hysteria. They argue that democratic societies are highly resilient and that Russia’s capacity to exert a significant influence over political processes in the West has been exaggerated. What, though, can be said about Russia’s approach so far?

Propaganda starts at home

The economies of the Baltic states are on the verge of collapse. The Finnish government takes away the children of Russian parents if the families show any intention of moving back to Russia. Ukraine has concentration camps for opponents of the regime. The United States is developing chemical weapons in laboratories on the Russian border with a view to invading Russia. Ukraine was represented by a former pornographic actress at the NATO summit. And paedophilia is now allowed in Europe and no longer criminalised.

What do these reports all have in common? They are false – simply made up. They were spread by Russian media. They serve to discredit the West, the United States and the European Union. They are part of the war waged by Russia against the democracies of the West by means of misinformation and propaganda. This war is directed from the Kremlin, by the presidential administration. State media, and some significant non-governmental media outlets, are briefed to this end on a weekly basis. The foreign ministry, intelligence services and the ministry of communications also all play a major role. [1] Russia is spending a lot of money on this war. It operates troll factories, in which employees flood the internet in Europe and the West with targeted propaganda. It maintains the international television station *RT* – formerly *Russia Today* – and the media network *Sputnik*, which operates websites and internet platforms in over thirty languages. They are combined under the umbrella of the media holding company *Rossiya Segodnya*, 'Russia Today'. Its budget for the current year comes to roughly €340 million. That goes a long way.

In the past, dictatorships depended primarily on violence, and only to a lesser degree on propaganda. In modern dictatorships the trend has reversed: they depend to a great extent on propaganda. Vladimir Putin was very quick to understand this. 'The secret of Putinism is propaganda – spin on a highly professional level,' observed the late Russia expert Heinrich Vogel back in 2014. [2] In a state dominated by the secret services, methods of information and misinformation have become part of all areas of state policy. When Putin took office in 2000, the first thing he did was to reign in television – the most important medium in Russia. He wrested power over information away from the oligarchs Boris Berezovsky and Vladimir Gusinsky, who had their own TV channels, and drove the insubordinate tycoons from the country. 'We have to run our own information policy,' Putin said in an internal briefing, after he had been harshly criticised on Berezovsky's and Gusinsky's channels over the case of the submarine *Kursk*, which had sunk with all hands after an on-board explosion. [3]

The propaganda employed by Putin domestically as an instrument of power was then applied to foreign coverage. Particularly in the aftermath of the annexation of Crimea and during Russia's covert war in Ukraine it became clear just how important this propaganda is for Kremlin policy. The Putin regime disguised its aggression by casting events in the Ukraine in the context of the Second World War, which, as the 'Great Patriotic War', plays a special role in the collective memory of Russian society and in the identity of so many Russian citizens. In Moscow's version of events, a fascist putsch had taken place on Kyiv's Maidan Square and a fascist junta had come to power with the support of the US and the EU. While Kiev was accused of committing 'genocide' in the east, Russia itself allegedly did not intervene in the hostilities. This narrative was maintained through a mixture of facts, rumours and lies – including in Russian media

aimed at audiences abroad.

The Kremlin's trolls

Covert agents are also deployed in Russia's information war. It soon became apparent that what journalists working for the dissident newspaper *Novaya Gazeta* had revealed about the internet in their own country also applied to the outside world as well. The Kremlin maintained a large number of so-called 'internet trolls' who worked in secret to influence opinion in line with the views of the Russian leadership. The case of a 'troll factory' became the most famous of all. In an office building in Olgino, a suburb of St Petersburg, there were at least 300 people working for the department of external propaganda online; the enterprise was called 'Internet Research Agency'. From morning till evening employees – mostly students with a good knowledge of foreign languages – would write comments on the forums of western news platforms and online newspapers. They also posted on Facebook, Twitter or other social media and got involved in online chats, all the time appearing to be private users. Their bosses, who included KGB veterans, instructed them as to what they should write to convey the Kremlin's line. Employees were expected to fulfil certain quotas – posting at least 50 comments a day on various internet sites, say, or operating six Facebook accounts. They would regularly report back to their superiors on how many of their tasks they had completed. '305 tweets posted altogether,' one employee wrote in his weekly report to his superior Denis Osadchy on 22 April 2014, according to an e-mail published on a Russian blog. [4]

Staff at the troll factory were paid several hundred euros a month – decent earnings for students in Russia. A young Russian woman, Lyudmila Savchuk, revealed how she was instructed to praise Putin's policies on news portals, chat rooms and blogs, and to 'bash his enemies'. She would write up to 100 comments a day and was paid 640 to 800 euros per month. At the height of the war in Ukraine, websites in the USA and in Europe were flooded with an avalanche of comments, mostly supporting the Kremlin. The webpages of German channels and newspapers, from the German public service broadcaster ARD to the weekly paper *Die Zeit* and the national dailies the *Süddeutsche Zeitung* and the *Frankfurter Allgemeine Zeitung*, were also beset by trolls. The same bogeymen – America, the West and the EU – cropped up again and again in the comments. The impression given by the readers' forums was that proponents of Russian policy represented the majority view in Germany. This contradicted opinion polls suggesting that 70 per cent of Germans had no sympathy with Putin. This led many news sites in Germany to simply switch off their comment functions, not wanting to be made into an instrument of Russia's information war.

It proved possible to identify the contracting authority of the troll factory from internal documents as Yevgeny Prigozhin, a restaurant entrepreneur from St Petersburg. He had met Putin in the 1990s in St Petersburg, when he was running a casino and Putin was responsible for the surveillance of gambling on St Petersburg's city council. Prigozhin is now a restaurant kingpin who puts on the catering at Russian government events, including state receptions, and known as 'Putin's chef'. Prigozhin is understood to have personally invested a major sum in the troll factory, with the lion's share coming from state sources. The troll factory's monthly accounts were sent to Prigozhin's company *Concord*. Yet the most remarkable thing emerging from the revelations about the troll factory was that the reports on the work done at the troll factory in St Petersburg were

sent directly to the then first deputy chief of staff of the presidential administration in the Kremlin, Vyacheslav Volodin. Volodin, currently chairman of the State Duma, was one of Putin's inner circle as a kind of ideologue-in-chief, whose responsibilities in the Kremlin included surveillance of the internet.

The German Chancellor Angela Merkel was on the receiving end of a cruder kind of troll attack in early June 2015, a few days before the start of the G7 summit at Elmau in Bavaria. The target was her new Instagram account. From the outset, people in the government press office responsible for the account were in a state of alarm. Comments could be posted on each individual picture – and there were plenty, almost exclusively in Russian. 'The moment we opened the channel there were several hundred comments in the space of a few hours in Cyrillic script,' a government spokesman said. Only a few employees in Merkel's social media team could speak Russian, so they used an online translation service. Most comments were rants against 'Ukrainian fascists' and personal insults directed at Merkel. The Russian commenters were particularly upset about a picture of Merkel with Ukrainian president Petro Poroshenko. 'A meeting of two friends – an old communist and a new fascist,' commented user 'drdrccp45'. No sooner had it been launched than Merkel's Instagram account had become a platform for Russian propaganda. The government press office eventually prohibited comments in Cyrillic script. 'In the interests of readability' all comments in languages other than German were deleted, 'with the exception of posts in English'. [5]

The troll factories have since become less important and have been replaced by semi- or fully automatically generated comments and messages, posted by bots. They are playing an increasing role in Russia's attempt to exert influence over western countries. [6]

Cyber war in the Bundestag

In mid-May 2015, parliamentarians in the German Bundestag had grounds to feel deeply insecure. Someone had infiltrated the German parliament's internet system: some functions had been crippled and sporadically the network was disappearing altogether. Gradually, news filtered through of what had happened. The main server of the parliamentary network – Parlakom – had been hacked. As a result, the intruders now had access to the Bundestag's data. The German parliament's network was not secured. The Federal Office for Information Security, tasked with protecting the communications of the government and the civil service, investigated the incident with the help of the domestic intelligence agency. It emerged that numerous MPs had received an e-mail from an address ending in the domain name 'un.org'. They assumed that the e-mails were indeed from the United Nations. But anyone who clicked on the mail immediately downloaded spyware that embedded itself deeper and deeper in the Bundestag network.

Once the attack had been discovered, a considerable amount of data had already been leaked. Even subsequently it was impossible to stop the leakage of data straight away, because the intruders had already penetrated so far into the system. What proved disastrous was that the Bundestag network – unlike that of the government – was not protected from attack by the Federal Office for Information Security, by the express wish of the Bundestag, and so was easier to hack. [7] An attack like this made it possible for the intruders to acquire information such as MPs' telephone numbers. They could potentially then be handed over to hostile intelligence services and wiretapped. But even

e-mails or parliamentarians' favourite internet sites could be useful, in order to plant malware or smuggle Trojans into the system. What's more, personal information about members of the Bundestag, for instance about medical conditions, could be used to pressurise politicians. The attack on the German parliament was the most serious case of political cyber espionage in Germany.

After months of investigations the authorities were as sure as they could be that secret services, most probably from Russia, were behind the attack. [8] A group of hackers known as APT28 was responsible. APT, in the language of IT security, stands for 'Advanced Persistent Threat' – sophisticated and planned well in advance. Many Western IT companies also know the group as 'Operation Pawn Storm', 'Sofacy' or 'Fancy Bear'. The group has been active on the internet since at least 2004, operates across several units and always attacks very specific targets: European governments, NATO, and western arms manufacturers, particularly companies in the aerospace industry. The targets affected include not only eastern NATO states but also sites in Great Britain, France, Belgium and Greece, as well as Russian dissidents – as happened in August 2015. The German domestic intelligence service had already identified attacks by this group on the German governmental network between 2009 and 2011. Western intelligence services link APT28 to the Russian military intelligence service GRU. The group was always active during Moscow working hours and the malware used had been developed on a Russian language setting.

Since May 2015 there have been a number of cyber attacks on politicians and political institutions in Germany that have been linked to Russia. For instance, in April 2016 hackers attacked the computer systems at the headquarters of the Christian Democratic Union (CDU; Merkel's party) in Berlin, using fake websites to obtain login details of CDU members. The security company Trend Micro, reporting on the attack, said that the Russian hacking group APT28 was responsible. [9] In September 2016 the Bundestag parliamentary groups involving the Social Democratic Party (SPD) and Die Linke, as well as many individual representatives, were the target of cyber attacks. Computers at the national headquarters of Die Linke and the Junge Union, as well as CDU politicians in the Saarland, were also attacked, with these incidents also attributed to APT28. [10] It was revealed in April 2017 that the group was planning attacks on the servers of the Konrad Adenauer Foundation and the Friedrich Ebert Foundation, using fake websites. The Friedrich Ebert Foundation confirmed an attempted attack, which had, however, been foiled. [11]

Estonia: Russia's first cyber victim

Russian hackers attacking western governmental institutions is nothing new. They usually operate skilfully and professionally. Russia is well ahead of many western countries in mathematical and scientific education, producing many outstanding IT specialists – and indeed many highly skilled hackers. It has been common knowledge for two decades that Russia can hit its foes where it hurts by attacking their computer systems. The first time this became clear was in Estonia. On 27 April 2007 the Baltic state's entire IT infrastructure was brought to a standstill: parliament, government departments, banks and even radio stations and Estonian language newspaper websites.

At the time, part of Estonia's ethnic Russian population was protesting against the

proposed relocation of a Soviet Red Army soldier's memorial from the centre of the Estonian capital Tallinn to a military cemetery. The memorial commemorated the Soviet Union's victory in the Second World War, whereas Estonians tended to associate it with the Soviet occupation of their country. The Russian government had raised objections to the planned relocation. In the night of 27 April 2007 the statue of the soldier was removed from its original site in the centre of Tallinn, leading to unrest in the Estonian capital. [12] Among the protesters were activists of the Kremlin's youth association *Nashi*, who had travelled to Tallinn especially. Russia's state TV channels drew parallels between the scenes in Tallinn and the Second World War, with the Estonians cast as latter-day fascists. The following day, the cyber attacks began. The Estonian government was convinced that they were coordinated from Moscow, but could not prove it. The attack was straightforward enough – the attackers simply unleashed an avalanche of data from tens of thousands of computers, which overloaded the systems they were attacking until they collapsed. In March 2009, Konstantin Goloskokov, a *Nashi* official, revealed himself to be the mastermind behind the attacks. The Russian government, however, continued to deny all responsibility for the attacks. [13]

Russia's second cyber war followed over a year after the attack in Estonia. In July 2008 Georgian websites were infected with viruses, including the sites of the president, the parliament, the foreign office and sites of news agencies and banks. It heralded a war that Russia and Georgia would be fighting a few weeks later in the parallel, 'real' world.

Cyber warfare and organised crime

Russia plays a leading role in the global cyber war. The issue has taken on enormous importance for the military and the intelligence services since 2004. From the start, Russia was anxious to keep pace with the Americans and their intelligence service, the NSA – and also with the Israelis and later the Chinese. The aim of the Russian regime was for the country to have built up a cyber army so powerful that by 2020 it could prove decisive in a military confrontation. Sure enough, Russia has all the prerequisites to be at the forefront of the new warfare. Since Soviet times, its military and intelligence services have always had a particular penchant for everything to do with technology. Under Vladimir Putin, the intelligence services were expanded and generously equipped. The GRU military intelligence service, the FSB federal security service, and the SVR foreign intelligence service now all have the necessary capacities to wage a cyber war. The exact figures are not known. Western intelligence services estimate there are between 4,000 and 10,000 cyber recruits, who are payrolled by the Russian secret services. [14] The core of the Kremlin's team of hackers is said to comprise a few hundred people working for the FSB. At the same time, the Russian secret services have the same problems as their western counterparts. On the free market or on the hacker industry's black market, exceptionally talented IT specialists can earn many times more than the state can pay them. Consequently, many hackers have left Russia to work in Asia, Europe or the United States – thus eluding the clutches of the Russian state and its security apparatus.

The unusual aspect of Russia's cyber army is the close association between the intelligence services and organized crime. It is not unique to Russia that hackers whose skills have come to light in cyber crime are hired by the intelligence services in return for protection or legal immunity – this is also known to happen in the US. But the Russian services, especially the federal secret service, recruit particularly high numbers from

prisons. What's more, they regularly award contracts to organised crime. The hackers' group APT29, also known as 'Cozy Bear', is said to work as a contractor for the FSB. [15] At the same time, the security services have programmes financed by organised crime. This cooperation has advantages for both sides. For example, the Russian services can obtain certain tools through criminal gangs. They can arrange for gateways to foreign IT systems to be spied on by criminals, without having to be directly involved. Organized crime can in turn pursue its own financial interests under the umbrella of the intelligence services. This is possible thanks to the close involvement of politics and organized crime in Russia. To give a recent example: in March 2017 the US Department of Justice charged four men with the theft of 500 million e-mail accounts of the internet provider Yahoo in 2014. Two were FSB agents, the other two were alleged to be Russian and Canadian-Kazakh cyber criminals. [16]

Author: Daniel Oines. Source: Flickr

From espionage to cyber sabotage

Until three years ago, Russian cyber attacks were generally intended for espionage purposes. But since the worsening of Russia's political relations with the West in the course of the annexation of Crimea, Putin has also deployed his cyber army for sabotage. The preferred arena for these activities is Russia's neighbouring states, which belong either to the EU or to NATO, or lean towards the West, in other words the Baltic region and Ukraine in particular. In autumn 2014, Russian saboteurs incapacitated the computers of the Ukrainian electoral commission for some time just before the parliamentary elections. On 23 December 2015, a power plant in Ivano-Frankivs'k in western Ukraine was tampered with, leaving at least 225,000 inhabitants in the region without electricity for several hours. The sabotage was operated by the – presumably Russian – hacker group 'Sandworm', which launched their attack using the malware 'Black Energy'. 'We can gauge the culprits' technical abilities to be considerable,' the Federal Office for Information Security wrote in its report; they had used a range of attack techniques to camouflage their assault and to make it harder to correct any faults. According to the account given by the president of the domestic intelligence services Hans-Georg Maaßen, the campaign 'Sandworm', attributed to Russia, attacked authorities, telecommunications companies, energy providers and research facilities – in other words, sought to tamper with national infrastructure. [17]

Both these operations fit the political message that Moscow intended to send out, both at home and abroad: 'We are strong, NATO and the West cannot protect you, stick with Russia instead' – this was the message to the Ukrainians. 'Russia could stop the "fascists" getting elected in Ukraine and even shut down their power supply' – this was the message to the people at home. The perpetrators of these attacks did not even try to cover their tracks. But Moscow did not limit its acts of sabotage to Ukraine and other neighbouring foreign states. On 8 April 2015, the French channel TV5 Monde was unable to broadcast internationally. That morning, the French foreign minister had appeared in a new series; by the evening the channel had been brought to a standstill by an act of sabotage. The attackers posed as IS sympathizers, but, according to western intelligence, were Russian hackers operating under a 'false flag'. They had penetrated the channel's system some time earlier and had been able to scout it out in detail. This enabled them to

pinpoint the server responsible for preparing the satellite signal and shut it down. The saboteurs even knew that maintenance was not dealt with by the channel itself, and therefore that the channel was guaranteed to be out of commission for several hours. [18]

Yet the attacks on TV5 Monde and on the Ukrainian power plant are child's play in comparison to what Russian cyber forces are capable of today. In both cases the computer systems were not especially difficult to hack. Russia's intelligence services and cyber war activists have been engaged in sabotage for years. Special forces and laboratories work on locating the flaws in the systems of industrial plants and power stations, in traffic control systems and military facilities. Sabotage attacks like the ones carried out by the 'Sandworm' group are no longer restricted to Russia's neighbouring states. Germany has also been affected by similar attacks on numerous occasions. In one case a research facility was warned in time. 'But equally there are cases when we only notice the attacks when it's too late,' the intelligence services reported.

So far these attacks have mainly served to demonstrate what Russia is capable of. There have been no instances to date of large-scale attacks on Germany. It remains unclear whether Russia's current regime would risk changing that approach in future. Over the past three years Moscow has shown how far it is prepared to go in pursuit of its policies.

Hacking elections in the US and Europe

Russian hackers landed what was probably their biggest coup in 2016 during the American election campaign. In the spring of 2016 the APT28 group broke into the servers of the Democratic National Committee (DNC), the headquarters of the Democratic Party in the United States, and obtained thousands of e-mails, of which 19,000 were gradually published online on Wikileaks, the so-called whistleblowing site. This led to uproar in the Democratic Party, and the DNC chair resigned shortly afterwards, as candidate Hillary Clinton had received preferential treatment compared with her party rival Bernie Sanders. The publication of the internal e-mails heightened the feeling of insecurity in a bitterly fought campaign that had already divided the country. The analyses of three independent IT security companies pointed to attacks by the APT28 and APT29 groups. [19] The Kremlin has always denied any involvement – but it must have delighted the Russian regime to be seen as so powerful that it could influence matters anywhere, even in the most powerful country on earth. It seems that Moscow's first concern was to discredit the American political system, and only secondarily to assist the Trump candidacy. The businessman was viewed in the Kremlin as an opportunity to achieve better relations with Washington, whereas Clinton was a no-go for the Russian leadership. It has become clear since Trump's election that any hopes on the Kremlin's part of a rapid improvement in Russia's relationship with the United States have not been fulfilled. The FBI is investigating alleged links with Russian secret agents and diplomats in the election campaign, while committees in the US Congress have been set up to investigate possible links. This in turn restricts Trump's options in his dealings with Russia, whose alleged involvement in the election has proved to be a double-edged sword.

The cyber attacks in the US election campaign gave rise to some alarm in Berlin too. In early 2017 the government expressed its concern that the parliamentary election campaign could be affected by cyber attacks and targeted campaigns of misinformation.

Germany, according to the government, would have to get ready for a ‘new kind of election’, since there was no doubt that Russia would do all it could to influence the campaign. The threat was not merely of political interference; acts of sabotage were also seen as a possible way to indirectly exert influence.

One scenario, involving a combination of three elements, was seen as particularly dangerous. Cyber attacks could be used to sabotage so-called ‘critical infrastructure’ – for instance electricity and water supplies, or the electronic systems of hospitals or of transport providers. At the same time, misinformation could be disseminated on a grand scale. A third element could be the publication of explosive material leaked in the spring of 2015 when the Bundestag network was attacked, aimed at discrediting specific parties or politicians.

The case of ‘Lisa F’ also awakened suspicion in the German government. In early 2016 the false report by a Russian TV channel of the alleged rape of a 13-year-old German girl of Russian extraction by Arab immigrants in Berlin led to demonstrations by thousands of Russian Germans in several German cities. [20] The German government saw these demonstrations as having been ‘orchestrated’ by Moscow. Russian foreign minister Sergey Lavrov’s public accusation that the German authorities had sought to cover up the case strengthened the impression that Moscow was engaged in a deliberate campaign of misinformation. Lavrov spoke out on behalf of ‘our Lisa’ even after the German judicial system had already announced that no rape had taken place. Yet the German intelligence services could find no evidence that the campaign had been planned well in advance. This did not end concerns in Berlin that misinformation could be used as a tactic in future. ‘There are no limits to their imagination in that area,’ was the view of the possibility of similar false reports.

The latest cyber attacks have caused more distant events to be viewed in a new light. One example is the Green MP Marieluise Beck, who was the victim of hackers in 2014. As the Green Party’s spokesman on eastern European affairs, Beck had been a sharp critic of Russia’s conduct in the Ukraine conflict. In 2014 she had not been informed as to the source of the attack on her computer. In autumn 2016 the Federal Office for Information Security revealed, following an enquiry from Beck, that ‘as a result of certain technical features’, the malware program had been attributed to the APT29 group. Most security companies assumed ‘that the perpetrators belonged to the Russian intelligence services or were directed by them’. The president of the domestic intelligence, Hans-Georg Maaßen, wrote in a letter to Beck in November 2016 that ‘Russia [had] to be considered as a potential perpetrator of this campaign’. [21]

Germany prepares for info-war

In early 2017 the German government decided to draw public attention to the danger of Russian interference in the upcoming German election. Angela Merkel repeatedly stressed that Russian involvement was to be expected. According to Thomas de Maizière, the Minister of the Interior, Russia’s cyber attacks had long been part of their campaigns of misinformation. This was the new danger, ‘accompanied by attacks on government, parliament and media companies,’ de Maizière explained in late 2016 when presenting the new cyber security strategy.

The government is also making preparations for an emergency: ‘rapid-response task forces’ are to be set up in order to respond more quickly to online cyber attacks. Additionally, the cyber defence centre, which previously effectively consisted of a dozen staff engaging in daily video conferences, is to be expanded. It remains a matter of debate how Germany should react to possible attacks on critical infrastructure such as power stations and water companies, hospitals or specialized operations. In extreme cases, the view is that the servers used by the aggressors – situated abroad – must be shut down. The Ministry of Defence is currently setting up a cyber unit, but it will be years before it reaches full operational capability. Consequently a small crew of specialists is to be set up in the business unit of the Ministry of the Interior that will be able to pinpoint the servers of hackers abroad and take them down with a counter-strike.

Special precautions will be taken for polling day itself. The federal election commissioner, Dieter Sarreither, expects hackers to attempt to disrupt the parliamentary elections by attacking the administrative network. With this in mind, the infrastructure of the data centre has been trebled in size and computers and sites have been changed. Sarreither has also warned against fake news, advising that it could play a role even on the day of the election itself – for instance reports that particular polling stations are closed. He has promised to react quickly to this kind of fake news on election day – designed to disrupt the electoral process – via his own Twitter channel. [22]

Countering Russian propaganda in Europe?

But how should the West fight back against Russian propaganda and misinformation? The idea of setting up a defence centre to combat misinformation has mostly been viewed with scepticism in the German media. The Federal Press Office has hired a number of staff to observe fake news on the internet – but this is not counted as a defence centre. The objective of rebutting Russian misinformation is pursued by a small group in in the EU’s diplomatic service: the East StratCom Team. A part of their staff, around a dozen in total, gather false reports from Russia. East StratCom releases two newsletters every week regarding fabricated and falsified news reports from Russia and any new campaigns, in English and Russian. Since their work began in late 2015, over 2000 falsified reports have been brought to light. This fact-checking work has only been successful because a network of dozens of people and institutions shares its knowledge about fake news with the group in Brussels. The group was founded on the initiative of Estonia, Latvia, Lithuania, Denmark and the United Kingdom. Other member states initially had considerable reservations about its activities, particularly Italy and France. ‘We shouldn’t make Russia too angry,’ was the attitude. This attitude is arguably the biggest obstacle to a successful response to Russia’s campaigns of misinformation.

Some countries have set up their own centres or sites to counter Russian misinformation. The Czech government has set up a centre within its interior ministry for twenty specialists to analyse the misinformation emanating from Russia, to organize a rapid response and to advise politicians on their approach to the issue. Prague has a particularly clear view of the threat from Moscow. As many as a quarter of Czechs trust ‘alternative’, pro-Russian media more than official ones. [23] In Sweden, which does not belong to NATO, the Civil Contingencies Agency has established a working party of six experts to tackle the threat of Russian misinformation. The Finns have also long seen themselves as targets of Russian propaganda. The government in Helsinki has suggested

setting up a European centre in the Finnish capital to analyse ‘hybrid warfare’ and outline countermeasures. The efforts of the Nordic countries to counter the propaganda have not been unsuccessful: the Russian media network *Sputnik*, which started disseminating its propaganda in Norwegian, Danish, Finnish and Swedish in the spring of 2015, gave up after a year. Evidently there was insufficient interest in Russia’s service.

Underestimated or exaggerated?

For a long time, governments and publics in Germany and other European countries overlooked the influence exerted by Moscow through propaganda and misinformation, and similarly under-appreciated the threat posed by cyber attacks originating in Russia. After underestimating the threat, many have warned against making the opposite mistake and vastly overstating Russia’s influence, demonizing Vladimir Putin in the process. For instance, it was correctly pointed out that *RT* (formerly *Russia Today*) is not a leading cable channel in America and has relatively little influence there. Its large following on YouTube is mainly down to its purchase of sensationalist disaster videos. Equally, *RT*’s influence – exclusively online – is minimal in Germany. [24] A lot of the anti-democratic, anti-liberal propaganda spread on (social) media does not originate from Russian sources, but from other populist sources, often domestic ones, on the far left or the far right. Is the fear of Russian involvement no more than ideological hype? One might counter that information from *RT* or the *Sputnik* network is taken up by many websites – precisely those of a far-right and far-left persuasion – and so by indirect means reaches an audience of millions. This goes for the populist anti-EU ‘Five Star’ movement in Italy. [25] Moreover, despite its economic crisis, Russia continues to spend vast sums on its overseas propaganda, showing that it has no intention of contenting itself with the role of a regional power, to cite Barack Obama’s flippant description. The EU has so far struggled to find an effective way of combating Russia’s foreign propaganda, whether in a conceptual, organizational or financial sense.

It is true that there is no cause for panic about Russian interference. It is also true that the weaknesses of liberal democracies are not of Moscow’s making. The crisis of the EU, Brexit included, the rise of populist anti-European parties on both the left and the right, and the deep political and social divisions in the United States, are not the consequence of Russian politics but of home-grown trends. The estrangement of the elites from the rest of the population, the low rates of social and political participation, and the major problems of illegal immigration are just some of the important factors. Russia itself does not, of course, have an attractive alternative to offer. Instead, it exploits the flaws in the democratic systems and societies of Europe and the United States, in order to present a distorted picture of the weak, corrupt West and to strengthen forces opposed to democracies and organizations such as NATO and the EU. The Russian regime continues to pursue a policy of head-on confrontation with the West. It adopts an approach that is both single-minded and flexible in its aim of dividing its opponents. Whether the Kremlin will go beyond the limits of the campaign it has so far pursued in the field of propaganda and misinformation is unclear – but probable. There is no reason to sound the all-clear.

Footnotes

1. ‘Merkel is the prime target’. Interview with Janis Sarts, director of the Nato Strategic Communication Centre of Excellence in Riga. *Frankfurter Allgemeine Zeitung*, 27 April 2017, www.faz.net/aktuell/politik/russische-propaganda-merkel-ist-das-hauptziel-14989189.html.

2. Heinrich Vogel: ‘Putin, Putinism and Europe’, Berlin, 2015. www.swp-berlin.org/fileadmin/contents/products/sonstiges/Putinismus_Vogel_SV_2015_01.pdf. For more detail on the issue of Russian propaganda under Putin, see Markus Wehner, *Putins Kalter Krieg. Wie Moskau den Westen vor sich hertreibt* (‘Putin’s Cold War: How Moscow is pushing the West around’), Munich, 2016, pp. 80–95.

3. Mikhail Zygar: *Endspiel. Die Metamorphosen des Wladimir Putin* (‘Endgame: The Metamorphoses of Vladimir Putin’), Cologne, 2015, pp. 42–43.

4. Quoted by Julian Staib: ‘Putin sends a whole battalion of paid agents into the internet’, *Frankfurter Allgemeine Zeitung*, 20 June 2014.

5. Markus Wehner: ‘Russian trolls versus Angela Merkel’, *Frankfurter Allgemeine Sonntagszeitung*, 7 June 2015, www.faz.net/aktuell/politik/g-7-gipfel/angela-merkels-instagram-account-ist-ziel-von-troll-attacken-13633102.html.

6. Sarts, ‘Merkel is the prime target’ (see note 1). More generally: Simon Hegelich, *Social Bots. Invasion der Meinungsroboter* (‘Social Bots: The invasion of the opinionated robots’), Sankt Augustin, 27 September 2016, www.kas.de/wf/de/33.46486.

7. ‘Burglars’ greeting from Moscow’, in *Der Spiegel*, 50/2015, p.33.

8. See also the report by the IT security researcher Claudio Guarnieri, commissioned by the left-wing parliamentary group in the Bundestag. It was published on netzpolitik.org: https://netzpolitik.org/2015/digitaler-angriff-auf-den-bundestag-investigativer-bericht-zum-hack-der-it-infrastruktur-der-linksfraktion/.

9. ‘Security company reports phishing attack on CDU HQ’, *Spiegel Online*, 12 May 2016.

10. ‘German parties hacked’, *Süddeutsche Zeitung*, 20 September 2016.

11. Justus Bender & Eckart Lohse, ‘How a nerd tracked the hackers down’, *Frankfurter Allgemeine Zeitung*, 27 April 2017.

12. On the conflict, Karsten Brüggemann, *Denkmäler des Grolls. Estland und die Kriege des 20. Jahrhunderts* (‘Monuments of resentment: Estonia and the wars of the 20th century’), in *Osteuropa*, 6/2008, pp. 129–146.

13. ‘Kremlin youth group admits role in attack’, *Die Welt*, 11 March 2009, www.welt.de/wirtschaft/webwelt/article3355416/Kreml-Jugend-bekennt-sich-zu-Attacke-auf-Estland.html.

14. According to Western security services’ estimates. The figure of 4,000 refers to cyber soldiers of the FSB, GRU and SVR. ‘Russia said to be behind IS cyber attacks’, *Spiegel*

Online, 18 June 2016, www.spiegel.de/netzwelt/netzpolitik/islamischer-staat-cyberattacken-als-werk-russischer-hacker-enttarnt-a-1098249.html#ref=recom-plista. A similar number of hackers is reported to work for the NSA.

15. Marie Katharina Wagner: 'The Kremlin's hackers', *Frankfurter Allgemeine Sonntagszeitung*, 5 March 2017, www.faz.net/aktuell/politik/ausland/russland-rekrutiert-seine-hacker-im-gefaengnis-14909771.html.

16. Peter Winkler, 'US charge Russian agents with hacking', *Neue Zürcher Zeitung*, 15 March 2017, www.nzz.ch/international/amerika/fuers-vaterland-und-fuers-eigene-portemonnaie-usa-klagen-russische-agenten-fuer-hacking-an-ld.151553.

17. *Bundesamt für Sicherheit in der Informationstechnik: Die Lage der IT-Sicherheit in Deutschland 2016* ('Federal Office for Security in Information Technology: the state of IT security in Germany'), www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht 2016.pdf?_blob=publicationFile&v=5, p.40. – Jörg Diehl: 'Constitutional protection office warns against attacks from Russia'. *Spiegel Online*, 13 May 2016, www.spiegel.de/netzwelt/netzpolitik/hans-georg-maassen-warnt-vor-cyber-angriffen-in-russland-a-1092238.html.

18. How France's TV5 was almost destroyed by 'Russian hackers', BBC News, 10 October 2016, www.bbc.com/news/technology-37590375.

19. The German government's response to a brief parliamentary enquiry by the left-wing group in the Bundestag on 22 December 2016: 'Cyber attacks allegedly planned by the Russian government against the German parliamentary elections', http://dip21.bundestag.de/dip21/btd/18/107/1810759.pdf.

20. See: Nikolay Mitrokhin, 'The "Russian World" in Germany', in Eurozine, http://www.eurozine.com/the-russian-world-in-germany/

21. Markus Wehner: 'Beck hacked', *Frankfurter Allgemeine Sonntagszeitung*, 25 December 2016, www.faz.net/aktuell/politik/inland/gruenen-politikerin-marieluise-beck-ist-opfer-eines-hackerangriffs-14590122.html.

22. 'Federal election commissioner: We're preparing ourselves for cyber attacks', *Frankfurter Allgemeine Zeitung*, 14 January 2017, www.faz.net/aktuell/politik/bundeswahlleiter-will-bundestagswahl-vor-hackerangriffen-schuetzen-14651555.html.

23. Jakub Janda, Ondřej Kundra: 'Mechanisms of Influence of the Russian Federation into Internal Affairs of the Czech Republic', www.europeanvalues.net/wp-content/uploads/2016/09/Mechanisms-Of-Influence-Of-The-Russian-Federation-Into-Internal-Affairs-Of-The-Czech-Republic.pdf.

24. Stefan Meister: 'A dangerous paper tiger', in *Internationale Politik*, 3/2017, pp. 8–13. – Siege: 'RT's propaganda is far less influential than Westerners fear', in *The Economist*, 21 January 2017. – 'Much ado about nothing?' Gemma Pörzgen, Moritz Gathmann, Vytautas Bruveris and Alexei Kovalyov. Ostpol, 20 January 2017,

www.ostpol.de/beitrag/4797-viel-larm-um-nichts. – Gemma Pörzgen: ‘“Soft power” and Moscow’s burnishing of its own image: easy prey for a PR offensive during the media crisis’ in *Osteuropa*, 1/2014, pp. 63–88.

25. Alberto Nardelli, Craig Silvermann: ‘Italy’s Most Popular Political Party Is Leading Europe In Fake News And Kremlin Propaganda’, Buzzfeed, 29 November 2016, www.buzzfeed.com/alberto nardelli/iralys-most-popular-political-party-is-leading-europe-in-fak?utm_term=.dnQozK0yeB#.qneZ7Bqo2N.

Published 21 July 2017

Original in **German**
Translation by **Saul Lipetz**
First published in **Osteuropa 5/2017 (German version); Eurozine (English version)**
Downloaded from eurozine.com (https://www.eurozine.com/hacking-propaganda-and-electoral-manipulation-2/)