Taming the great bear

Russia is using the internet to undermine Western democracies. But Europe has the tools to fight back

The decade after the Cold War was not kind to Russia – a country benighted by Boris Yeltsin's incompetence, vast corruption, economic decline, financial crisis, and the 1999 enlargement of NATO into former Warsaw Pact territory. Beginning in 2000, Vladimir Putin's presidency at first hardly dented this national humiliation. Russia struggled through the civil war in Chechnya; endured a series of national disasters including the Kursk submarine explosion and Beslan massacre; witnessed colour revolutions turn Georgia and Ukraine toward the West; and saw the EU and NATO expand into Russia's spheres of influence in central and eastern Europe. By the mid-2000s Russia was strategically enfeebled.

Putin set out to rehabilitate Russian power, in the first place via growing economic strength undergirded by extractive industries. Along with efforts to bring the media under Moscow's control, Russian hydrocarbon companies, which Yeltsin privatised, were forced back into the Kremlin's hands. With the media supportive of Putin's foreign policy agenda and domestic political power consolidation, and the hydrocarbon industry reviving Russia's economy due to rising commodity prices, Putin began to implement a strategy for regaining lost Russian glory.

Moscow's tainted splendour

Early signs of this were Gazprom cut-offs of natural gas to Ukraine in winter of 2006 and 2009, as well as Russia's annexation of South Ossetia following the 2008 Russo-Georgian war. Putin intensified Russia's revisionism with the 2014 Crimea annexation, followed by occupation of eastern Ukraine and efforts to dismantle Ukraine and regain for Russia strategically important territory lost after the USSR's implosion. Starting in 2015 the Kremlin expanded its geopolitical coercion through support of Bashar al Assad, whose war crimes during the Syrian civil war were overlooked – indeed aided – by Russia, so long as his regime guaranteed Russian access to its Tartus base and port facilities. These kinetic actions have been matched by Moscow's interference in other states' domestic politics. The Kremlin, for instance, supported the rise of extremist parties

in Europe, strengthened the pro-Brexit vote whose aftermath is weakening the EU and the UK, and meddled in European and US elections.

The overall objective of these actions has been to undermine the liberal order—both states and institutions – that has grown to dominate the post-Cold War world. Fittingly for such revisionism, Moscow's playbook harkens back to the USSR: destabilising disinformation campaigns within a hybrid-warfare framework. This is born of necessity, as in the modern, liberal world naked aggression is seen as unacceptable in routine statecraft. The information warfare component of the Kremlin's assault on the liberal order is also opportunistic, exploiting the features of liberal globalisation to undermine it: trans-border flows of information and people, social networks, viral (often tribal) socio-political behaviour, powerful computer algorithms, networked computing and the vulnerability of digital societies to hacking.

The Kremlin deploys cyber-warriors trained to manipulate search results, construct botnet, exploit social media, create fake news, and spy online. Moscow also relies on more conventional outlets to spread its propaganda and disinformation, not least the Russian international news channel RT.

Moscow's $400m annual investment in these capabilities is focused on ensuring their desired message reaches certain target groups. At the same time it rejects the general idea of 'objective' truth and facts in politics: the condition for open, reasoned discussion that is the lifeblood of liberal socio-politics.

Fatal distraction

Four representative acts of disinformation serve to muddy the waters of debate: Dismiss/Deny, Distort, Distract, and Dismay. To wit, Russia denied or dismissed reports that its elite, unmarked soldiers were in eastern Ukraine; distorted the role of non-terrorist Syrian rebels by claiming they are ISIS affiliates; distracted from Donald Trump's unfitness for the US presidency by leaking hacked information about Hillary Clinton; and sowed dismay by evoking escalation should the international community push for reincorporation of South Ossetia into Georgia.

Russian information warfare – especially within a hybrid-warfare context – takes four types of strategic actions. Firstly, Moscow wants to prevent the US and Europe from countering Russian aggression. This entails using the media to create narratives depicting Russia as powerful and

dangerous. Tactically this includes belligerent and misleading statements about Russia's military capabilities, outlandish bellicosity promoting Kremlin leadership as unpredictable – for example threatening the use of tactical nuclear weapons – and spreading misinformation about Russian military movements. Taken together, this sows confusion and confounds the international community.

Secondly, Moscow generalises cynicism about domestic and international politics and discredits the idea of international law and norms. This erodes trust between populations and political leaders, in turn weakening opposition to Russian action. Essential to this is the tactic of disrupting the concept of 'truth' in news media. Russia's most pervasive tool for confusing and exasperating populations of other states is flooding internet news sites with spurious content. This may take the form of 'fake news' that slanders adversaries, conspiracy theories, or the rapid-fire dissemination of falsehoods and half-truths. This gives the impression the internet is unreliable, and therefore consumers should discount internet reporting. Cyber-espionage is another component of this strategy, as it provides material for conspiracy theories and undermines trust in the internet, undercutting its benefits.

Russia's most pervasive tool for confusing and exasperating populations of other states is flooding internet news sites with spurious content

Thirdly, Moscow legitimates illegally created 'facts on the ground' by weaponising otherwise normatively acceptable concepts: popular self-determination, defending sovereign borders, and the inviolability of human rights. For example, Moscow recognises the independence of dubious self-proclaimed republics, such as South Ossetia. Russia has unilaterally created new 'borders' annexing onto South Ossetia territory which according to international standards belongs to Georgia. The Kremlin also has a habit of granting passports – and thus Russian nationality – to ethnic Russians in neighbouring countries. This creates Russian national diasporas and therefore a 'need' for Russia's 'human rights protection' for its citizens abroad against supposed ethnically motivated abuses.

Fourthly, Russia provokes dissension within and among states allied against Russian actions by supporting radical political movements and parties. This both affects particular political outcomes, and, through exacerbating political divisions within target countries, erodes the foundations of democratic politics: election probity, trust between

population and politicians, and the assumption that politicians govern in service of the national interest. This makes affected states less capable of countering Russian action.

The Kremlin also has a habit of granting passports to ethnic Russians in neighbouring countries…thus creating a 'need' for Russia's 'human rights protection' for its citizens abroad

The most (in)famous example was the Kremlin-directed hacking and release of US Democratic Party emails, which damaged Hillary Clinton's presidential candidacy, cast doubt over the legitimacy of US elections, and (under President Trump) has bled into executive branch chaos. Europe's far right, including France's Front National, Hungary's Jobbik, Great Britain's UKIP, and the Austrian FPÖ, has received Russian support extending from positive propaganda to financial backing. Russia is keen to aid these parties' Eurosceptic efforts, including abolishing the Euro and the Schengen area, as well as weakening NATO.

On the offensive

Though the task will never be easy, there are ways to at least partially neutralise Russia's disinformation. The most important is to use strategic communications to generate salient, pro-active narratives describing actions and interests vis-à-vis Russia and third parties. Responding piecemeal to Russian disinformation is a losing strategy. Instead, policymakers in Europe and the US must anticipate and pre-empt Russian information warfare lines-of-attack. This requires agencies to coordinate government and private sector communications. Examples are the EU's Eastern Stratcom Task Force and Centre of Excellence for Countering Hybrid Threads, which must be scaled-up and better resourced.

Targeted polities should also incentivise action from the private sector, notably social media providers used to propagate 'fake news'. A government heavy-hand – censorship for example – would backfire, playing into Moscow's hands. Instead, media regulators should persuade social media providers – Twitter, Google, Facebook and the like – to create better filtering algorithms and the means to identify 'fake news' and possibly remove it.

Cyber-security is also high-priority. Cyber-espionage of political parties potentially reveals proprietary information that Moscow can exploit to undermine and influence elections. This is an immediate concern in Europe, where Italy, Sweden, Austria, Hungary, and the Czech Republic

will hold general elections. Passive cyber-defence is insufficient; solutions must be innovative. One approach is 'cyber-blurring' – creating fake documents and email accounts – to confuse and slow hackers. Emanuel Macron's campaign successfully adopted this approach. A more aggressive approach is 'active cyber-defence'. This goes beyond reactive cyber-security such as anti-malware software, instead privileging defensive intelligence collection and policy measures, including sanctions and trade remedies, for deterring malicious cyber-actors. Considering the political risks and difficulties in attribution, this will require high-level coordination among law enforcement, intelligence, technology and media companies, and political stakeholders.



Mason Richey
Seoul

Mason Richey is associate professor of international politics at Hankuk University of Foreign Studies (Seoul, South Korea), editor-in-chief of the *Journal of East Asian Affairs* and president of the Korea International Studies Association.