Second-Strike Communications

Elisabeth Braw

To counter disinformation campaigns, liberal democracies should focus on second-strike capabilities.

Just over one year ago, a Russian former double-agent and his daughter were found unconscious on a park bench in the English cathedral town of Salisbury. But the attempted poisoning of Sergei and Yulia Skripal was almost a sideshow to the Russian disinformation attack on the UK that followed, which sought to obfuscate the attack’s nature and the identity of its perpetrators. Today, disinformation attacks can cause chaos in the targeted country, as the public struggles to understand what, exactly, is transpiring. As with nuclear weapons, Western countries need a second-strike capability.

Several European countries already engage in effective defence against Russian disinformation operations

The second-strike capability is a central tenet of nuclear policy, which asserts that a country attacked by nuclear weapons must be able to launch a counter-attack that inflicts similar damage on the enemy. Put another way, as defined by Austin Long and Brendan Rittenhouse Green, a nuclear-weapons state must have ‘the ability of a nuclear force to absorb a preemptive attack and nonetheless retaliate with enough weapons to cause unacceptable damage’. The calculation is that the second-strike capability will deter two nuclear states from launching nuclear attacks against each other.

Almost immediately after the attempted murder of the Skripals, the British government concluded that it had been carried out by Russian agents. There are ‘only two plausible explanations for what happened in Salisbury on the 4th of March. Either this was a direct act by the Russian State against our country. Or the Russian government lost control of this potentially catastrophically damaging nerve agent and allowed it to get into the hands of others’, Prime Minister Theresa May told Parliament eight days after the attack.

Her assignation of blame unleashed a massive Russian information offensive, which involved government spokesmen, political leaders, news outlets, and social media trolls. Russian Foreign Minister Sergei Lavrov suggested that the UK’s own secret services had carried out the attack. The Russian embassy in London tirelessly used Twitter to discredit British institutions such as the police, suggesting that Agatha Christie’s fictional detective Hercule Poirot would have done a better job of identifying the perpetrator. Russian government-linked media, meanwhile, delivered a string of other explanations; a January 2019 report by the Centre for the Study of Media, Communication & Power at King’s College London puts the number of alternative explanations presented by RT and Sputnik alone at 138. The report’s authors, Gordon Ramsay and Sam Robertshaw, note:

Narratives often appeared following public interventions by Western governments. Following Theresa May’s speech to the UK Parliament on 12th March in which Russia was accused and the nerve agent ‘Novichok’ identified, a flurry of narratives contesting the origins and existence of Novichok appeared on RT and Sputnik, and narratives framing the incident as defined by geopolitics and Western domestic political problems began to emerge.

As the UK discovered following the poisoning of the Skripals, disinformation can be efficiently combined with a physical attack. Indeed, the physical attack may take on secondary importance once the disinformation campaign is launched. The Russian government had tested the strategy before. In 2014, for example, the Kremlin orchestrated a disinformation campaign against Sweden, after a suspected Russian submarine was spotted off the coast of Stockholm. As the Swedish Navy chased the sub, Russian government spokesmen and media outlets energetically offered alternative scenarios: the intruder was, they suggested, a Dutch submarine. Russian media also suggested that the intruder was, in fact, a sea animal, while Russia’s embassy in Stockholm took to Facebook to criticise Sweden’s alleged...
obsession with ‘phantom submarines’ and hostility towards ‘Russia’s peaceful intentions’. The Russian tactic is to put on a blank face and sow uncertainty among everyone who doesn’t have 100-percent-certain evidence’, General Sverker Göranson, Sweden’s Chief of Defence at the time, later explained. ‘And the Russians always try to make the other side look like idiots. As soon as the suggestion appeared that the detected sound might come from an animal, the Russians picked it up in order to ridicule us’. The campaign appeared designed to make Swedes lose faith in their armed forces.

The Swedish government managed to assemble a united front against the information offensive, with the prime minister, the defence minister and General Göranson coordinating their statements about the nature of the intrusion and the armed forces’ progress in identifying the perpetrator. On several occasions the three leaders jointly delivered the information, reinforcing the message of unity. The front was, however, purely defensive. Crucially, it failed to deter the Russians, as evidenced by the continuing disinformation directed at Sweden. ‘Increasingly since 2014, Sweden has been the target of a wide array of active measures: disinformation, forged telegrams and fake news items have surfaced in the information landscape’, reported Swedish Russia scholars Martin Kragh and Sebastian Åsberg in a 2017 article on Russian disinformation for the Journal of Strategic Studies.

After Salisbury, the Kremlin encountered something very different: a second strike. As soon as Russia launched its disinformation campaign after the Skripal attack, the UK government struck back. A recently installed central communications team coordinated government messaging. Indeed, perhaps somewhat surprisingly the government – otherwise bitterly divided and distracted by Brexit – managed to focus on the unfolding Russian disinformation campaign. It did so quickly. And unlike the Swedes, the Britons did not just defend themselves against rapidly spreading narratives: they went on the offensive. The government unceremoniously took Russia to task at the UN, expelled Russian diplomats, rallied support among EU and NATO partners, who did the same, and released details about the two men linked to the attack. Non-government groups such as the investigative network Bellingcat used the details to identify the perpetrators: Russian military intelligence officers Anatoliy Chepiga and Alexander Mishkin. With their covers so dramatically blown, the agents will never work abroad again, and the Kremlin will think twice before unleashing another disinformation campaign against the UK.

Sweden’s repeated experiences as the target of disinformation campaigns – another wave took place during the 2015–2016 refugee crisis, with a steady stream of news stories with headlines such as ‘Sweden to Refugees: Find a Bed or Go Back to Germany’ – has encouraged it to...
Second Strike

Adopt a more muscular tone as well. ‘When the threat of disinformation surfaced during the election campaign last year, Prime Minister Stefan Löfven announced that we’d accept no interference, and that we’d name and shame the perpetrators’, Fredrik Konnander, head of counter-influence at Sweden’s Civil Contingencies Agency, told the author. His position was created in 2015.

Disinformation campaigns, to be sure, belong to a different category of aggression than nuclear weapons use. A communications assault can, however, inflict devastating damage on the target country by causing the population to lose faith in their democratic institutions. It can also multiply the effect of another attack. In a report on power grid security for the Johns Hopkins Applied Physics Laboratory, Paul N Stockton points out that in case of a successful attack on the US grid ‘the public declaration of a grid security emergency will be almost certain to spark a media frenzy and a flood of ill-informed speculation. Against a backdrop of fear and uncertainty, adversaries may use social media and other means to spread further disinformation and incite public panic as part of their attacks’. In March 2019, General Valery Gerasimov, Russia’s Chief of the General Staff of the Armed Forces, who has spearheaded his country’s successful use of blended aggression (often referred to as hybrid warfare), highlighted information as a tool of war.

Russia is, of course, neither the first nor the only country to use information as a tool of war. Traditional territorial wars are usually accompanied by information campaigns aimed at convincing the adversary’s civilian population that resistance is futile. During the Cold War, the Warsaw Pact and NATO countries maintained elaborate news organisations whose sole purpose was to win the other side’s civilian population over. The US-funded radio (and now digital) channel Radio Free Europe/Radio Liberty (RFE/RL) reports that ‘RFE and RL’, originally separate organizations, were conceived by George F. Kennan (United States Department of State) and Frank G. Wisner (Office of Policy Coordination, later the United States Central Intelligence Agency) to utilize the talents of post-World War II Soviet and Eastern European émigrés in support of American foreign policy’, adding that they were initially principally funded by the CIA. Today the Kremlin similarly considers itself the subject of hostile Western information operations.

A communications assault can, however, inflict devastating damage on the target country by causing the population to lose faith in their democratic institutions

In disinformation/information, the second strike must not be identical to the first strike. Because surprise is an advantage, the second strike’s content should be a surprise until the moment it is launched. Indeed, the targeted country can – and should – refrain from indicating whether it will strike back. The second strike’s key advantage is the country’s ability to carry it out, which deters the adversary from carrying out the first strike.

That does not mean that there is a moral equivalence between Russian and Western information operations. The question is the balance of power. As with nuclear weapons, the balance must be neutral. If it is not, the side with the power advantage will continue its hostile activities. Western countries, then, need to develop second-strike communications capabilities.

Several European countries already engage in effective defence against Russian disinformation operations. The Lithuanian government has a team that debunks disinformation. Lithuanian techies, in turn, have founded the debunking platform demaskuok.lt. Using a charming fantasy analogy, Lithuanian volunteer ‘elves’ identify Russian internet trolls in their spare time. The elves’ approach is that by unmasking the trolls, they will be able to silence them or at least limit their effectiveness. The EU has its own debunking team. These are laudable efforts. The response to a disinformation assault, however, must be so intolerable that the would-be attacker refrains from launching one.

The UK’s response to the Skripal incident was not perfect. In an interview, Gary Aitkenhead – chief executive of the Defence Science and Technology Laboratory, which operates the Porton Down lab where the poison was analysed – said that ‘we were able to identify it as novichok, to identify it was a military-grade nerve agent. We have not verified the precise source, but we have provided the scientific information to the government, who have then used a number of other sources to piece together the conclusions that they have come to’. The Russian government immediately used his comments to argue that the UK government had not established the toxin’s source. The Britons did, however, demonstrate second-strike intent and capability. So did Mr. Löfven: the 2018 Swedish parliamentary election had surprisingly little interference.

If launching a disinformation assault poses no risk, the adversary will keep attacking. The target country needs to not just defend itself, but show offensive capabilities as well. Those capabilities include speed. As Göranson points out, Western countries are wary of responding with less than complete certainty regarding an attack’s provenance. A delayed response does, however, blunt its force. Western countries need to develop second-strike communications capabilities, not just against Russia but against any adversary. And they need to display them. Otherwise disinformation campaigns will keep being launched, by Russia and by countries studying its methods.

Elisabeth Braw
Elisabeth is an associate fellow at RUSI and directs its Modern Deterrence project.

The views expressed in this article are the author’s, and do not represent those of RUSI or any other institution.