Combating Information Operations

Developing an Operating Concept

Simon Jones
Master in Public Administration Candidate, Harvard Kennedy School
Combating Information Operations

Developing an Operating Concept

Simon Jones
Master in Public Administration Candidate, Harvard Kennedy School
About the Author

Simon Jones is a British Civil Servant, working for the last seven years for the British Ministry of Defence on issues including Euro-Atlantic security policy, national preparedness, and domestic counter terrorism. Having graduated with a Mid-Career Master’s Degree in Public Administration from the Harvard Kennedy School, Simon is a Research Associate with the Belfer Center, supporting its Defending Digital Democracy Project.
Table of Contents

Introduction ................................................................................................................. 1

The Ends ....................................................................................................................... 3

The Ways ...................................................................................................................... 9
  Information Sharing and Analysis Organizations ...................................................... 12
  Local Resilience Forums ............................................................................................ 12
  Joint Terrorism Task Forces ....................................................................................... 13

The Means ................................................................................................................... 15
  International Organizations ....................................................................................... 15
  NATO and the EU ....................................................................................................... 15
  The Organization for Security and Co-operation in Europe ..................................... 16
  Interpol and Europol .................................................................................................. 18
  International Norms and Treaties ............................................................................ 19
  The US Federal Government .................................................................................... 22
  The Not-for-Profit and Private Sectors .................................................................... 27
  Targeted and Impacted Organisations ..................................................................... 29

Conclusion .................................................................................................................. 34
Introduction

Recent Russian Information Operations (IO) and election interference should have come as no surprise to Western Governments, given that it reflects the trend of an increasingly belligerent and provocative Russia, willing to use the full range of levers available to advance its foreign policy objectives. It is more striking that following the conclusion of the US intelligence community that Russia interfered in the 2016 US Presidential Election¹, there has been lack of concrete policy proposals implemented in the US or other Western democracies to address Russian behavior and ensure that future elections do not fall victim to Russian interference.

Much has been written on encouraging social media companies to help stem the flow of disinformation, either by incentivizing voluntary efforts or through government regulation, including the Shorenstein Center’s authoritative work on the subject². In recent weeks, a number of welcome initiatives have emerged, including the EU’s proposed voluntary code for social media companies³ and Facebook’s announcement that it will filter political adverts during elections.⁴ While this is an important part of countering disinformation, it is questionable whether social media platforms themselves have the necessary capacity and capability to counter state-sponsored disinformation. For example, despite its best efforts, Google has struggled to prevent search engine manipulation, a tactic that has already been used


to achieve financial, political, and disinformation objectives. Russia has repeatedly proven that it is adept at adapting its tactics, using illegal methods, and exploiting legal loopholes to exploit social media platforms and channels. This means that technology—and technology companies—alone cannot solve the issue and a more comprehensive approach is needed.

This paper instead focuses on developing an operating concept—composed of ends, ways, and means—for those who are tasked to respond and those affected by foreign interference and IO. Based on the principle of information superiority and drawing on best practice from efforts to counter cyberattacks, terrorism, and civil emergencies, the paper seeks to develop a more holistic and collaborative approach for planning for and responding to disinformation, identify additional sources of support and expertise, and outline new norms and standards of behavior to assist an effective response.

While this paper predominantly draws on Russian IO conducted for the US 2016 Presidential Election and elections across Europe and aims to prevent Russia from conducting similar activity again, a number of nations and groups have proven willing to utilize similar tactics, techniques, and procedures. Therefore, the approach outlined is applicable to any concerted disinformation campaign or IO that has national security implications.

---

The Ends

Based on a common understanding of threats, Western nations must strive to develop a coherent and whole-of-society approach, increased resilience, and new norms of behavior to plan for and respond to IO. This will help to deter state-sponsored activity and reinforce the commitment of Western nations to democratic principles. Taking each of the elements in turn:

i. Common understanding—nations need to understand who Russia is targeting and why, how it is nuancing its messages, and the legal gaps and grey areas that Russia is exploiting.

ii. Coherence—responders and affected parties need to understand their roles and obligations, the legal basis for how they can refute disinformation, and how they should collaborate with counterparts.

iii. Whole of society response—Russian activity has targeted moderate political parties and candidates across the political spectrum, as well as civil liberties groups and private firms. Nations need to protect all parts of society and maintain internal cohesion in the face of attempts to inflame social tensions. Countering IO that is targeted at elections should remain a key national and international area of focus. To do this effectively, it is important that a bi-partisan approach is built outside the election and campaign cycle.

iv. Increased resilience and deterrence—Increased preparedness will foster greater resilience by building redundancy and additional capacity into the ways that IO is detected and refuted. Noting that Russia typically undertakes careful and thorough battlefield analysis and preparation before it enters conflicts, this may deter foreign interference by making it more difficult and costly for it to conduct IO.

v. Behaviors and norms—accompanying improved response mechanisms, nations must also increase their population’s understanding of the threat that IO poses and change behaviors accordingly.

---

vi. Democratic principles—as with counter terrorism and cybersecurity efforts, nations need to consider the balance that they strike between measures to prevent disinformation and the protection of civil liberties and free speech. Ensuring that efforts to counter IO are underpinned by a genuine commitment to democratic principles will help to avoid efforts to crackdown on disinformation disenfranchising parts of Civil Society, which can be further exploited by IO.

To understand the utility of these elements it is important to consider why Russia conducts IO and election interference and the tactics that make it so effective. IO is part of Russia’s doctrine of ‘information confrontation or information warfare’ and it supports Russia’s domestic and foreign policies in a number of ways:

i. **To project Putin’s vision of a powerful Russia with a global reach.** Russia no longer has the conventional military or economic influence of the Soviet Union and must be more strategic in picking the areas in which it is prepared to compete with the West. Russia has realized that if it cannot compete then it must strive to dominate the narrative around world events. Russia is also prepared to undertake audacious actions to achieve foreign policy objectives that it can reasonably assume will be attributed to Russia because it perceives that attribution feeds the narrative of a powerful Russia.

ii. **Opportunism.** Russian foreign policy behavior is opportunistic, with the use of political, diplomatic, economic, and military levers to achieve its objectives. IO tactics are a low, or even no, cost way to achieve its goals on the basis that it is unlikely that nations could or would unilaterally sanction Russia for meddling. Russia has also repeatedly pressed its narrative that the ‘color revolutions’ were the product of Western interference, emphasizing that its attempts to interfere in elections are comparable.

---


iii. **The failure of Western nations to develop modern deterrence postures.** In February 2013, Russia’s Chief of the General Staff Army-General Valeriy Gerasimov concluded that Russia cannot “catch up” with the West but should instead expose and target its vulnerabilities. Western models of deterrence have not been modernized to reflect this changing form of Russian competition, with Western nations focused on achieving conventional and nuclear deterrence. The inability of the West to devise modern deterrence postures that can deter Russia from activity that stops short of conventional military force has effectively signaled that the West is only prepared to confront Russia for its most egregious behaviors. This has emboldened its activities and it is likely that it will continue to use unconventional tactics to confront and challenge the West.

iv. **To tarnish Western liberal democratic principles.** The Putin Regime has witnessed nations on Russia’s periphery become liberal democracies and members of NATO and the EU. It fears that this could trigger Russians to demand the same rights and freedoms within Russia, overthrowing the Regime in the process. Disrupting Western elections, especially through leaks and accusations of corruption and voter fraud, shows the Russian public that Western politics and politicians are no better than their Russian counterparts, demonstrating that the Western democratic elections are not free and fair. As well as conducting IO, Russia has undermined the EU and NATO by financially supporting opposition groups in the West, fomenting populism and the rise of undemocratic parties.

v. **The insecurity of the Putin Regime.** The 2018 Russian Presidential Elections has highlighted the inability of the Putin Regime to influence younger generations of voters and has seen the emergence of a genuine opposition that has rallied around Alexei Navalny. Although Putin won the Election, unverified independent estimates indicate that this could have been with up to 10.3 million falsified

---

votes. Attempts by the Regime to drum up popular support demonstrate the lengths it will go to demonstrate the strong grasp that Putin has on Russia and a popular mandate.

Building on RAND’s findings, there are six key elements that explain why Russian IO has been so effective in the West:

i. **Volume and diversity of channels and contents.** Russia has shown great aptitude in subverting and modifying social media marketing and amplification tools to achieve its information operations goals, using fraudulent accounts, political rallies, online advertisements to reach 126 million Americans through Facebook alone. Some of these approaches are relatively quick and easy to establish, while others took careful planning to create more believable sources. This helps to repeat key messages and means that this messaging continues even if one channel or avenue is closed down or discredited.

ii. **Rapid propagation of narratives and repetition across channels.** Russian operators understand the importance of quickly espousing a narrative on an incident and repeating this narrative. For example, in the immediate aftermath of the Westminster Bridge terrorist attack in London, the Russia 24 news agency incorrectly identified the attacker, stating that his attire indicated that he had links to

---


Afghanistan or Pakistan. This photograph was quickly picked up and disseminated by other Russian news agencies, with similar commentary applied about his origins.  

iii. **Continuous activity.** In-line with Gerasimov’s assertion that “Wars are not declared but have already begun,” Russia practices the art of information confrontation continuously, refining its approach over time, and tailoring activities to specific audiences. This means that West cannot afford to simply react to Russian activity and must be anticipatory and proactive.

iv. **Inconsistency and adaptation.** Narratives can quickly be discarded if they fail to achieve a notable effect, and it will often propagate several narratives at the same time. These narratives may be inconsistent, unrelated or even contradictory to each other. This reflects the fact that Russian IO is conducted by a wealth of actors and entities with only tangential links between them, including its intelligence agencies, troll farms, and proxies. For example, in the aftermath of the London Bridge attack Russian trolls also spread an image that purported to show a Muslim woman in a hijab ignoring injured victims. Similarly, during the 2016 US Presidential Election and Primaries, Russian activities supported both the Trump and Sanders campaigns to target the Clinton campaign.

v. **Plausible presentation.** An important characteristic of Russian propaganda is the look and feel of channels such as RT and Sputnik. Visually, they look similar to mainstream Western news channels,

---


they have built a roster of presenters and anchors familiar to viewers from other channels, such as Larry King from CNN and Ed Schultz from MSNBC\textsuperscript{19} like news programs, and hosted politicians and political commentators such as Lt Gen Michael T Flynn, and the UK Labour Party Leader, Jeremy Corbyn.\textsuperscript{20} Considerable effort was taken to ingratiate Russian trolls into social movements before and during the Presidential Elections, with Russian operatives seizing on themes and issues of importance to Black Lives Matter Campaigners and the Alt-Right\textsuperscript{21}.

vi. National borders. Russian IO does not stop at national borders and it will deliberately stoke tensions between nations to divide and conquer. For example, it has directed disinformation at Canadian troops in Latvia and German troops in Lithuania.\textsuperscript{22} This makes it more difficult for nations to tackle disinformation on their own.

Therefore, Russia is not peddling a consistent narrative that can in itself be refuted or challenged. Instead, it is seeding distrust both within and between Western nations to weaken resolve, complicate decision-making, and draw attention away from Russia's actions. This brings both opportunities and risks. This opportunistic, adaptable approach can seize on prevailing issues within nations, as shown by the attempts to capitalize on the protests following the Parkland School shooting in Florida\textsuperscript{23}, costing


the West considerable time and effort, with no one part of the Government or Civil Society seeing the full picture of its activities.

However, this also means that Western nations are not facing the kind of Cold War-era IO that was underpinned by competition between ideologies and coherent narratives. Individual groups and sections of Western societies may agree with the Putin Regime on single issues, such as attitudes toward Islam, but Russia has finessed its disruptive and spoiling IO approach because it cannot comprehensively compete.

The Ways

The development of enhanced information sharing processes and comprehensive crisis management arrangements can help Western nations to plan for and respond to IO and disinformation. Nations should think in terms of competing with Russia for information superiority. As defined by UK Joint Doctrine, information superiority is: “The competitive advantage gained through the continuous, directed and adaptive employment of relevant information principles, capabilities and behaviors.” Therefore, information superiority is the means of fostering formal and informal links to draw together the wealth of information and resources needed to enable decision-makers to make effective and collective decisions on IO.

In the US, the successful delivery of each of these elements is reliant upon collaboration and co-operation between the wealth of stakeholders and affected entities, including:

a. International institutions and Allies;

b. The US Federal Government, including intelligence agencies and law enforcement bodies, and Congressional oversight committees;

c. Other tiers of government, including States and Counties;

---

d. The private sector, including cyber security companies, social media and marketing optimization firms, social media platforms themselves, and targeted companies; and,

e. Not-for-profit entities, including political campaigns and election monitoring groups.

To achieve information superiority, there are four key elements that must be delivered: collection across all activities; analysis of the aggregated data; dissemination of information; and leveraging and exploitation of the information.  

**Collection and alternative sources.** The multitude of channels that can be exploited and creative approaches conducted by Russia means that prioritization and the identification of appropriate sources of information is essential. For political campaigns and private firms, the process to prioritize and identify sources may bear resemblance to the identification of key voter demographics or social influencers and building an understanding of the campaigning activities and methods of opposing political campaigns.

**Analysis.** The nature of IO deliberately makes it difficult for one entity or group to possess the technical expertise and subject matter knowledge to attribute and refute attacks and decide what constitutes an information operation and what does not. For example, the difficulties are highlighted by the fact that Facebook's initial efforts to moderate contents has seen the removal of legitimate contents. This may become even more difficult as political campaigns adopt social media optimization techniques and tactics that bear a resemblance to information operations: for example, the British Conservative Party hiring social media influencers to ‘professionalize’ its online campaign activities. This means that the analysis to piece together


IO puzzles will rely on collaboration and co-operation across sectors and party political lines.

**Dissemination.** Research suggests that the sharing of fact-checking content typically lags that of misinformation by 10-20 hours and closing this time lag is an essential component of an effective response.\(^\text{28}\) This is often compounded by avoidable delays: for example, the time it took for the Obama Administration to make public statements on Russian hacking of the DNC\(^\text{29}\) allowed Russia to dictate the narrative on the incident, focusing public attention on the contents of information leaked from the hacks rather than the hack itself. Timely dissemination of analysis and intelligence on information operations is essential to enabling an effective response and allowing other stakeholders to protect themselves.

**Leveraging information.** As with cyber-attacks, it is insufficient to accurately detect and attribute incidents. Although the hacking of the DNC by Russian intelligence-affiliated adversaries was detected and publicly attributed by cyber security firms\(^\text{30}\), Russia was able to dictate the narrative by drip-feeding leaked information. Stakeholders need a way of delivering consistent and clear messages on IO if they are to seize the initiative and counter Russian narratives.

---


Information Sharing and Analysis Organizations

The Federal Government should leverage existing information sharing arrangements and models, particularly those that share information between public and private organizations in response to cyberattacks, terrorism, and civil emergencies, to help foster the characteristics of information superiority. The Information Sharing and Analysis Organization (ISAO) model is the most obvious one to draw on to help counter IO. ISAOs help facilitate the sharing of information on cybersecurity risks and incidents between and among their memberships. ISAOs can be region or industry specific and they help members to enhance situational awareness; develop a common picture of the threat faced by a specific sector or region; implement common responses to incidents; and share best practice. DHS could encourage sectors most likely to be impacted by IO to form ISAOs, or the model of founding a ISAO Standards Organization and then developing best practice for ISAOs could be adapted to deliver IO-specific ISAOs.

Local Resilience Forums

Building on the information sharing arrangements of ISAOs, the Federal Government could deliver something more in keeping with the UK’s Local Resilience Forums (LRFs). Set up on a geographical basis to ensure the effective delivery of crisis management arrangements in the event of civil resilience and terrorist incidents, membership of LRFs include emergency responders; military liaison officers; utility providers and representatives from critical national infrastructure owners; NGOs; and sizeable private firms. LRFs are mandated to deliver a range of outputs, including an agreed risk profile for its area and a co-ordinated approach to the most significant challenges, specifically considering: risk management; business continuity; and arrangements to warn and inform the public. LRFs help to facilitate

the development of multi-agency plans and co-ordinate multiagency exercises.\textsuperscript{32}

LRFs most notably go beyond the ISAO role in the event of a crisis, when it transitions to become a Strategic Co-ordination Group (SCG). An SCG should: agree priorities in responding to the incident; arrange and allocate adequate resources and financial controls; interface with other areas and national government departments; develop and maintain Shared Situational Awareness across all partner agencies; co-ordinate communications both internally and externally and facilitate media liaison.\textsuperscript{33} An organization coordinating and conducting of these tasks and functions in the event of a crisis would be useful, but there is a trade-off in terms of developing the degree of institutional and sectoral interoperability needed to do this effectively. The LRF/SCG model is effective in the UK due to the fact that it is grounded in legislation that mandates the involvement of emergency responders and critical national infrastructure providers. It is unlikely that the Federal Government would enact similar legislation in the US for an IO-focused entity and therefore all information sharing and involvement in these structures would probably be on a voluntary basis.

**Joint Terrorism Task Forces**

Joint Terrorism Task Forces (JTTF) in the US are composed of personnel from across US law enforcement and intelligence agencies, including the FBI, police forces, and Immigration and Customs Enforcement. Their role is to conduct counter-terrorism investigations and provide assessments and intelligence products on regional and local threats in over 104 US cities.\textsuperscript{34} While JTTFs do not include private and non-governmental stakeholders, the principle of drawing together government stakeholders at the local


level to better understand and address specific issues would help the fight against IO. In particularly contentious elections, for example, the Federal Government could stand up Task Forces of those with law enforcement or regulatory responsibilities to ensure that their efforts and insight are aligned.

Information sharing and crisis management forums focused on IO would help to deliver more effective and consistent efforts across all four elements needed to achieve information superiority. The ISAO, LRF, JTTF models offer ways to engage and involve the breadth of stakeholders involved in countering IO and further thought is need on how they would be adapted for IO. These forums could also help to shape the consensus on how to deal with IO and develop new norms of behavior in response to IO, across partisan and social boundaries.
The Means

Western nations need to think more comprehensively about the means available to them to counter IO. Across all aspects of information superiority, there is more that stakeholders at the international, national, and local levels can do.

International Organizations

While the tactics and scale of IO mean that responding to IO is more likely to be led by individual nations, there is a wealth of existing international co-operation that could be better leveraged. A systemic, joined-up approach by international institutions, underpinned by treaties and bilateral agreements, could help to tackle disinformation and give greater transparency on election interference. Broadening and deepening the range of international organizations that is involved would open new information sharing channels and could lead to solutions based on best practice from other cross-cutting international issues. International institutions with a role to play in planning for and responding to IO include:

NATO and the EU

NATO and the EU are actively involved in countering Russian IO. Both contribute to the European Hybrid Warfare Centre of Excellence, which is built on contributions from Estonia, Finland, France, Germany, Latvia, Lithuania, Netherlands, Norway, Poland, Spain, Sweden, the UK and the USA. The institutions also have specific assets and capabilities available to counter and refute disinformation, including the EU’s East StratCom Task Force35 and NATO’s Strategic Communications and Cyber Centres of Excellence. Although NATO and EU collaboration is taking place, it has

---

been hampered by institutional competition and an inability to define and de-mark the responsibilities of the respective institutions.

NATO and the EU could help to develop international information sharing arrangements and best practice for responding to IO. This could involve the development of situational analysis platforms for sharing information between the EU and NATO’s hybrid threats branches, national government agencies, and other stakeholders\(^{36}\) and greater collaboration between NATO and EU centres of excellence to devise technical and operational responses to IO.

There is also more that the institutions could do individually. For example, the EU could use its linguistic and technical capacity to develop an open source monitoring analysis, along the lines of BBC Monitoring or the Foreign Broadcast Information Service, and building on its EU vs Disinfo campaign\(^{37}\). NATO could help the dissemination of classified information across the Alliance and with partners through its security accredited IT infrastructure and information handling policies and processes.

### The Organization for Security and Co-operation in Europe

The Organization for Security and Co-operation in Europe’s (OSCE) Office for Democratic Institutions and Human Rights (ODIHR) carries out election observation in OSCE participating States\(^{38}\). Although Observers do not carry out systematic or comprehensive observation of voting, they do look at the effectiveness electoral systems, including elements such as campaign finance rules, the administration of elections, and the conduct the campaigns. The ODIHR’s credibility and experience in this field, which


also supports the activities of citizen observer groups, means that it could independently verify external interference and IO that takes place during elections. This would help to convince more skeptical parts of society and other nations of disinformation campaigns. An ODIHR team was deployed during the Italian Parliamentary Elections in March 2018\(^\text{39}\) at the invitation of the Italian Government and this could have also reported on Russian interference.

The OSCE also has a key role to play in reducing the dangers of armed conflict that result from a misunderstanding or miscalculation on military activities. The implementation of new cyber and ICT confidence building measures by the OSCE sets a precedent for how IO could be approached. Along the lines of the measures implemented in 2016 to prevent tensions resulting from cyber activities, including the establishment of official contact points and communication lines\(^\text{40}\), measures could be implemented to allow increased transparency and debate about the IO capabilities that nations possess\(^\text{41}\). While Russia is unlikely to detail the full extent of its disinformation and IO capabilities, Western nations can use the OSCE to brief their own use of influence operations and strategic communications activities and to refute Russian narratives. Similarly, official contact points could be used to message to Russia on future incidents of IO, raising awareness of its activities in an international forum.


\(^{40}\) “OSCE participating States, in landmark decision, agree to expand list of measures to reduce risk of tensions arising from cyber activities”. OSCE. Accessed March 6, 2018. [https://www.osce.org/cio/226656](https://www.osce.org/cio/226656)

Interpol and Europol

Interpol has a role to play in complex investigations and prosecutions of criminal activities across national borders. Interpol’s growing expertise in cybercrime, which draws heavily on partnerships with private sector cybersecurity and forensics firms, and the relationships it has with national law enforcement agencies, would allow it to develop best practice and share expertise on how to enable the effective prosecution of the criminal aspects of IO across borders, denying operators a safe haven. In addition, it could also use its command and control centers to facilitate investigations for cross border incidents. Beyond this, Interpol could also help to independently verify incidents of disinformation and IO by facilitating peer reviews of national investigations.

Europol is the EU’s law enforcement agency. With 220 Liaison Officers and 100 crime analysts, it has already helped to co-ordinate the efforts of EU members and non-members, including the US, to disrupt Daesh’s propaganda and web presence. It also has expertise in a number of fields related to IO, including Organized Crime, and publishes annually its 'Internet Organized Crime Threat Assessment'. Europol could play a similar role for IO and disinformation, helping nations to co-ordinate efforts to take down hosting websites; supporting international efforts to prosecute those conducting IO; and providing Threat Assessments that identify tactics, trends, and developments.


International Norms and Treaties

Russian IO and election interference has been so successful because it has capitalized on the increasing interconnectedness that social media and the internet has brought. Russia has also exploited the fact that most national governments have been slow to understand and shape the impact of these technologies and citizens have not acknowledged and adapted to the commodification of their private data. Beyond national debates and discussions on legislating social media platforms, more thought is needed on the international legal implications of IO in the 21st Century.

Global institutions and think tanks, such as the World Economic Forum, have a role to play in ensuring effective public-private engagement to realize the benefits and minimize the risks from disruptive technologies, including social media and AI. The global footprint of social media companies, the reliance of many businesses and firms on their products, and the willingness of nations to target private firms as part of IO means that the private sector should have a voice at the national and international levels to shape policies and processes around social media, IO, and disinformation.45

Increased efforts by international institutions should be accompanied by the development of international norms of behavior and international treaties on IO and election interference. While it is debatable whether Russian IO has broken international law, its activities have broken the spirit of the principle of non-intervention, particularly with regards to the International Court of Justice's 1986 judgement that the principle forbids interventions in "matters in which each State is permitted, by the principle of State sovereignty to decide freely … [including] the choice of political, economic, social, and cultural system, and the formulation of foreign policy."46 Similarly, the UN Special Rapporteur on Freedom of Opinion and Expression


noted the ‘positive obligations’ of nations to promote free and fair media⁴⁷, which still applies even as more and more people obtain their news from social media.

More thought is needed on how these principles should be interpreted in relation to cyberspace. Norms and treaties would need to be carefully calibrated to ensure that nations can raise legitimate concerns at the standards of democracy or adherence to democratic standards in other nations, without raising criticism of services aimed at providing objective and accurate news in regions that are otherwise only served by propaganda, such as the Voice of America and BBC World Service.

There are a number of significant examples of Western and US interference in democratic elections from the Cold War that Russia could legitimately point to in the event of international dialogue on IO.⁴⁸ However, it is not accurate to compare Cold War era IO and disinformation with Russian activities in the 21st Century, given the way that Russia has sought to influence and distort the voting preferences of Western citizens and undermine democracy itself by tainting all elections with allegations of vote rigging and corruption. The West would need to clearly outline that its continued support to democratic parties in Eastern Europe and Central Asia is not about coercion but about a wholehearted belief in liberal democratic values. Furthermore, if Russia is genuinely worried about the interference of the West in its domestic elections and believes that the ‘color revolutions’ were not legitimate national expressions of democratic fervor, but fomented by the West through IO, then it is in its interests to engage in this debate.

Developing this theme, it could be possible to devise an International Agreement on IO and election interference. Building on the thinking


behind a Cyber ‘Geneva Convention’\(^49\), which proponents argue is the best way to enforce the principle that international law applies to cyberspace and that destructive state-sponsored attacks are already taking place against civilians,\(^50\) an IO International Agreement could focus on rejecting the ‘weaponization’ of social media platforms and mass data collection. The first step for this would be agreeing with like-minded Allies and Partners the ‘rules of the road’ on the use of influence operations, strategic communications activities, propaganda, and deception. NATO could act as the vehicle, drawing up statements that note the commitment of all 29 Allies to democratic principles and rejecting activity that undermines the democratic principles and institutions of other nations.

On a bilateral basis, the US and Russia could sign an agreement along the lines of the 2015 US-China Cybersecurity Agreement that focuses on IO and election interference. As with the Cybersecurity Agreement, this could pledge to end state-sponsored IO and election interference and could be accompanied by practical measures to build confidence and defuse and de-escalate incidents, including emergency hotlines and regular meetings of to discuss IO.\(^51\) While this would have practical benefits, it is likely that Russia would message that this treaty is tacit recognition by the US that it has also interfered in such a direct manner in Russian elections.


The US Federal Government

Russian IO tactics pose significant challenges for the national governments. For election interference in particular, national administrations often lack the ability and/or will to determine whether stories and incidents have arisen because of genuine political discourse or disinformation and a desire to be avoid being seen to politicize national security incidents. A good example of this was the hesitancy of the Obama administration to publicly acknowledge Russian interference in the Presidential Election.

IO will often bring into play different actors and agencies within the Federal Government that are unused to collaborating. This has challenges for information sharing and crisis management arrangements: for example, for incidents during Presidential Elections, the Federal Communications Commission and the Federal Election Commission would have a role to play alongside law enforcement agencies and the intelligence community. Similarly, detecting Russian involvement in environmental protests around the Dakota Access Pipeline, and investigations into suspected wider Russian efforts to influence US energy policy, drew on resources from the Department of the Treasury and the Department of Energy. In many examples, IO is enabled by criminal activities, including identify and financial fraud. Therefore, detecting and disrupting this activity is important and should be factored into an effective response.

It is also possible to imagine IO tactics, techniques, and procedures targeted at a range of sectors and industries. Disinformation targeted at the financial sector that tries to disrupt share prices, conducted by either state actors or criminals, could have a significant economic impact, and operations targeting hospitals and emergency responders during natural disasters or civil emergencies could result in significant losses of life.

---


There are several specific steps the Federal Government needs to undertake to enhance its ability to combat IO:

i. **Clarify, map, and test within the Federal Government who is involved and owns counter-IO efforts.** The Federal Government will need to be capable of reacting rapidly to incidents and conducting planning ahead of major events, such as elections, and this depends on each part understanding its role and how it interacts with other agencies and departments. The National Security Council will have an important role to play in co-ordinating this activity, as will the Senate Select Committee on Intelligence in providing oversight and scrutiny. As with other threats to national security, this increased co-operation will need to be exercised and tested routinely.

ii. **Develop the role of the State Department’s Global Engagement Center.** The GEC’s mandate has been expanded since the Presidential Elections, with the purpose of the GEC to ‘lead, synchronize, and coordinate efforts of the Federal Government to recognize, understand, expose, and counter foreign state and non-state propaganda and disinformation efforts aimed at undermining United States national security interests’\(^ {54}\). The GEC has a specific mandate to work with international institutions, allies, thinktanks, academic, and Civil Society to analyze the threat to the US, identify capability gaps, and develop and disseminate counter-narratives.\(^ {55}\)

The GEC, and its UK equivalent, the National Security Communications Unit, can take on additional tasks such as working with social media platforms and traditional media providers on processes to request the removal of disinformation; ensuring that the threat that disinformation and IO poses to democratic values is understood and factored into national risk assessments and security strategies; and working with at-risk groups, including

---


political campaigns and multi-national corporations to ensure they understand the potential impact of IO and how they can help to mitigate it.

iii. **Enhanced open source intelligence collection capabilities.** The US intelligence community should explore ways to leverage its capability and capacity in other forms of intelligence to enhance its open source intelligence collection abilities. This could include making use of AI and pattern analysis, and fusing this with traditional intelligence sources. Effort is needed to rebuilding relationships between the Federal Government and social media platforms to collaboratively counter IO, with careful consideration paid to the Constitutional and privacy concerns that this may raise. Finally, the intelligence community also needs to consider its relationship with private firms, including cyber security and commercial threat intelligence firms, noting that there is a reasonable expectation that private firms will detect and publicly attribute IO first.

iv. **Provision of open source threat assessments and alerts.** In-line with the UK’s National Cyber Security Centre56, and State Department travel advice, the Federal Government could offer more open source assessments and alerts on IO-related threats and incidents. This could include cyber-attacks, attempts by trolls to fuel violent protests, and use of botnets to amplify disinformation. This would allow the private sector and Civil Society to better understand threats and prepare themselves accordingly.

v. **Devise options to respond to Russian IO and sub-Article 5 activity.** The success of Russian meddling means that Russia will almost certainly continue to conduct IO against the US, with the mid-term elections later this year an obvious target. This could also embolden other foreign nations to conduct similar activity. The US needs to consider how it raises the cost to Russia of conducting IO or how it would punish Russia for the range of activity it has conducted against Western nations that stop short of conventional

---

warfare. This does not have to be a response in-kind—it could be financial sanctions against seniors in the Putin Regime or geopolitical moves, such as increasing military assistance to Ukraine—but the US should have a clear strategy and set of options on how it will message its discontent to Russia and cause Russia additional cost.

vi. **Educate citizens and the provision of factual information.** The Federal Government could do more to help inform and educate citizens and targeted groups of the threat that IO poses and how to refute it. Part of this involves the provision of threat assessments and information on incidents, but this could also include campaigns to make citizens more discerning in the news and media they choose to consume and more information on how and why foreign actors may target the West. While fact checking and refuting disinformation can help to partially mitigate the impact of the disinformation, national governments need to think more comprehensively about transparency and how they can enable and encourage civil discourse through the release of factually accurate and verifiable data. Making Census data and other government-owned datasets more accessible and searchable would help to make citizens more informed on social issues.

vii. **Enabling and incentivizing a whole of society response.** Beyond building information sharing arrangements, the Federal Government can enable and incentivize private sector and not-for-profit organizations to respond. This could be in a number of ways, including offering bounties for the identification of substantial troll farms and botnets; recognition for white hat hackers and groups that expose IO vulnerabilities; and offering software developers tax breaks for social media analysis tools that detect and attribute disinformation.

There are useful lessons from the Cold War on how the US responded to Soviet disinformation, with many of the tactics employed similar to what is seen today. The most effective measure adopted was the Active Measures

---

Working Group (AMWG), an interagency committee that monitored Soviet disinformation, engaged with Western media, and refuted disinformation. The AMWG had a few notable successes, including its first report, ‘State Department Special Report 88’, a four-page factual summary of Soviet tactics, of which 14,000 copied were distributed in October 1981 to news organizations, federal agencies and allies. In 1987, Mikhail Gorbachev personally complained about the document to Secretary of State George Shultz. 58

Whilst the AMWG highlights the potential benefits of the GEC helping to align the Federal Government’s efforts to refute and challenge disinformation, it is important to note the different political and social context of the Cold War, with significant divisions within Western societies on how seriously to take the threat that Russia poses. Similarly, the politically contentious and divisive nature of the outputs of IO means that the Federal Government cannot alone undertake the detection, analysis, and attribution of disinformation, and the track records of Western Governments in response to Russian IO highlight these limitations. The State Department has been criticized for the lack of progress to-date to expand the GEC’s mandate59.

The GEC’s Czech equivalent, the Centre Against Terrorism and Hybrid Threats, has not fared much better. Announced in 2016 with a mission to monitor disinformation and undertake a range of tasks, including training representatives from political parties to resist hacking60, it has been repeatedly criticized by senior Czechs, including President Milos Zeman, who has accused it of threatening the free speech of its citizens.61 Given


President Trump’s willingness to label mainstream media reporting as ‘fake news’, it would be interesting to see how he would react to the GEC refuting media reporting if its outputs implied criticism of the Trump Administration.

The Not-for-Profit and Private Sectors

The not-for-profit and private sectors can help to fill the technical skills gap to detect and attribute IO. The sectors possess the political insight to determine what is genuine political discourse and what is disinformation. Non-government actors can also help to bridge party political and partisan divides. An effective response relies on an understanding that IO campaigns do not stop at political party lines. Russian activity during the US presidential elections and primaries denigrating candidates from both sides of the aisle, such as Hillary Clinton, Ted Cruz, and Marco Rubio, and acted in the interests of both Bernie Sanders and Donald Trump.62

Building on the efforts of NGOs and cybersecurity groups during the French and Italian Elections, there are a number of ways that non-government actors and entities can support efforts to counter IO:

1. **The creation of counter-IO networks.** The creation of counter-IO networks. These could help to share expertise and insight, and develop common techniques, tactics, and procedures. This could build on the creation of IO-focused ISAOs or be formed as stand-alone entities. Stand-alone networks could focus more broadly on disinformation and misinformation, considering issues such as the psychology of how disinformation impacts society. The announcement by 31 technology companies, including Microsoft and Facebook, to sign a Cybersecurity Tech Accord, that commits to improve the security, stability and resilience of cyberspace is a good starting point that has direct benefits for efforts to counter IO.63

---


ii. **Crisis management and incident response.** Networks could also be utilized proactively or reactively to provide a common operating picture of IO incidents and to independently verify foreign interference. For example, during elections joint reports from left and right leaning thinktanks, or even political parties that conclude that IO is taking place would be compelling. The same would be true for reporting on interference on the Dakota Access Pipeline protests with input from trade bodies, private firms, and environmental campaigners.

iii. **Foster links across borders.** An important benefit of NGOs is their ability to work with campaigners and civil liberties groups in other countries to understand the development of IO tactics, techniques, and procedures. This could include groups in Russia who have exposed troll factories, and groups in countries such as the Czech Republic and Hungary, that have been the subject of persistent IO campaigns.

iv. **Amplification and alignment of messaging.** Non-government actors can also help to shift the narrative around IO. Rather than refuting messages, non-government actors can help by raising awareness of incidents and amplify key messages. Research suggests that the sharing of disinformation is dominated by very active users, while fact checking has tended to be a grass-roots activity.\(^{64}\) The Alt-Right has been particularly effective at its use of social media super users and private rooms on Twitter to amplify and co-ordinate its messaging,\(^{65}\) playing into the fact that people are more likely to believe stories from sources that they are believe are known to them.\(^{66}\) Networks of civil liberties and pro-democracy groups from across the political spectrum could work together to message about foreign interference and disinformation for the sake of supporting democratic principles.

---


Targeted and Impacted Organisations

More consideration is needed on the private sector impact of IO and disinformation. Notable cases where the private sector has been subjected to disinformation or misinformation impacted include:

i. Reports that Hurricane Sandy had flooded the New York Stock Exchange;\(^\text{67}\)

ii. Attempts to use Nintendo’s *Pokémon Go* Game to inflame racial tensions;\(^\text{68}\)

iii. Russian-linked Twitter accounts stoking controversy around NFL players kneeling during the US National Anthem;\(^\text{69}\)

iv. The impact on Montenegro’s tourism industry of statements by the Russian Government on the safety and security of its citizens in the country;\(^\text{70}\)

v. Cyber-attacks and disinformation campaigns against voting software suppliers.\(^\text{71}\)

It is difficult to quantify the cost or impact of these incidents, but they demonstrate that IO is not only targeted directly at national governments and will often be targeted at the full spectrum of Civil Society and the


private sector to attack Western interests and stoke social tensions. Targeted groups, including political campaigns, NGOs, and private firms, can do more to counter IO and disinformation themselves. Using tactics, techniques, and procedures already available to them, they can better understand the threat environment and work to mitigate risks, including:

i. **Social media optimization and monitoring.** Most private companies and political campaigns have public communications expertise and social media strategies. These rely on organizations understanding and influencing key demographics and consumers. To do this, many use social listening and influencer identification tools to monitor digital media channels, learn about their customers and competition, and identify key influencers. These same techniques and platforms can help to identify IO and disinformation. By understanding the information environment in which they are operating and identifying key influencers, organizations may be able to anticipate and detect incidents.

Hamilton 68’s Russian IO tracking dashboard is an example of this approach. By identifying and monitoring 600 twitter accounts suspected of pushing Russian IO, the dashboard helps to identify narratives that Russia is pushing and debates that it is seeking to influence. Non-government actors could adopt a similar approach, possibly related to their industry or geographical area.

ii. **Visualization and presenting the threat.** In-line with leveraging information, organizations can use marketing and campaigning tools to show IO and disinformation and its impact on their operations. Disinformation specialists have used visualization tools effectively to demonstrate links and contacts between bots and social influencers and to show the spread of disinformation. Rather than focusing on refuting and proving stories are fake, organizations can use creative and impactful ways to shift the narrative for consumers and voters to highlight the malign influence of foreign interference.

---

iii. **Understanding threats and changing mindsets.** Despite the fact that 64% of Americans have personally experienced a major data breach, with 49% of Americans feeling that their personal information is less secure than it was five years ago, only 13% feel the US Government is ‘very prepared’ to prevent cyberattacks on public infrastructure and 9% feel that US businesses are ‘very prepared’ for a cyber-attack.\(^{73}\) Research does not exist on how IO is perceived, but the time it has taken for organizations to adapt to the modern cyber threat environment highlights the change in mindset that non-government actors need to instill in their people to adapt to IO.

Enhanced cybersecurity is a key component of efforts by public, not-for-profit, and private organizations to become more resilient against IO. However, it is important to recognize that the objectives and motives of those conducting IO are different from other types of cyberattacks—cutting across the confidentiality, integrity, availability information security triad—and this might lead to different security measures and approaches. For example, Qatar claims that the recent spat with UAE and Saudi Arabia was caused by hackers compromising the networks of the state-run Qatar News Agency and planting disinformation on its website.\(^{74}\) The ultimate cause of this incident was inadequate cybersecurity, but an understanding of IO threats could have allowed the Qatar News Agency to configure its security posture more effectively.

As with other threats and hazards, IO needs to be built into organizational business continuity and crisis management plans. IO threats can also result from the behavior, conduct, and actions of employees and personnel in their private lives too: for example, false reports of a serious sexual assault by German troops in Lithuania meant that German and Lithuanian authorities had to

---


conduct an extensive investigation. Organizations should develop education initiatives for employees; reporting processes for those targeted; and crisis management plans to ascertain facts quickly, inform the public, and collaborate with other affected parties and law enforcement agencies.

Some of these tactics, techniques, procedures have already been utilized to help identify and mitigate the impact of IO and disinformation with some success, such as the analysis offered by the EU Disinfo Lab during the French Presidential Elections in 2017, which helped to demonstrate that Russian-backed trolls had sought to spread documents obtained by hacks from the Macron Campaign. However, there is no easy solution or one-size-fits-all approach; organizations will need to carefully investigate incidents seriously, even if they suspect that they are based on disinformation. Organizations need themselves to consider how they can organically draw on expertise and insight to understand and address the threats they face, allowing them to react as quickly as possible to dictate the narrative around incidents and allegations.

Targeted and impacted organizations could also focus on establishing new norms and rules to help decrease the impact of IO. These norms and approaches reflect the simple premise that organizations and parties across the political spectrum should be able to put aside political partisanship in the face of foreign interference. These norms could include:

On the basis that IO has and will continue to impact parties across the political spectrum, campaigns could agree before Elections to not exploit information obtained through leaks and would collaborate to correct disinformation if it was verified as false by a third party, such as law enforcement agencies or specialist NGOs. This approach is bears


resemblance to attempts to limit the use of negative campaigning and attack adverts\textsuperscript{77}

Private companies could withdraw advertising and marketing campaigns from social media platforms that do not tackle disinformation, on the basis that bots and fake accounts artificially inflate the anticipated reach of marketing campaigns by overstating the numbers of unique users.

Whilst maintaining the freedom of the press and freedom of expression, media platforms could devise voluntary codes of conduct for dealing with disinformation and information made public as a result of hacking and IO. This may not go as far as withholding the information, but could include best practice on how to report the information in a manner that reflects its source.

Conclusion

Social Media has changed the way many facets of Western life are conducted, from political campaigning to making and sustaining friendships. Western governments are still coming to terms with the substantial privacy and legal issues that social media generates and still do not have an understanding how the digital landscape can be manipulated to erode and undermine the democratic fabric of our societies. Russia has adapted, exploited, and weaponized our digital way of life. Now it has been proven that its tactics work, Russia—and other foreign states in competition with the West—will continue to attempt to distract and disorientate Western Governments and sow disagreement and disunity within and between Allies and Partners. This could be through election interference, inflaming social tensions around environmental or civil liberties issues, or disrupting financial markets. Carefully targeted disinformation or tightly co-ordinated IO that carefully treads the line between legal and illegal activity could cause significant harm, and the impact and opportunities will only increase as more and more of our interactions, civic engagement, and services move online.

There are no easy ways to plan for and respond to IO, disinformation, and election interference, but a change in approach, mindset, and mentality can offer significant improvements. For national governments and international organizations, this means creating new structures, partnerships, and information sharing relationships. It means drawing on the insight and expertise that Civil Society has to offer and helping targeted groups to better protect themselves. Doing so through coherent, whole of society, collection, analysis, dissemination, and leveraging will help to deliver information superiority. Competing for information superiority with Russia will allow liberal democracies to anticipate, mitigate, and respond to IO by creating resilient societies that understand the threat they face based on analysis, intelligence, and insight.

To achieve this, citizens and governments must be prepared to understand and adapt to the willingness of state actors and terrorists to interfere in their daily lives. As societies tolerated increased physical security in the wake of 9/11 and Daesh-inspired terrorist attacks, in cyberspace we must
learn to adopt new behaviors, accepting that protecting ourselves online goes further than secure passwords and antiviruses. It means citizens becoming more discerning about the source and authenticity of their news; journalists understanding that publishing leaked information without context or caveats may only tell part of the story if the information has resulted from state-sponsor hacks; and private firms better understanding the information and social media environment in which they operate.

IO and subversion of social media and cyberspace by hostile states should generate an international debate on norms and standards. Russia has breached the spirit of the principle of non-intervention and the obligation to promote an independent and diverse media, but there has been little focus on this issue. This highlights that international law and norms of behavior do not reflect the ways in which nations co-operate and compete in the 21st Century. While it is right that international arms control treaties and regimes have been pursued most vigorously for the most destructive and deadly weapons, it is important to note that IO is a direct challenge to liberal democratic principles and could seriously disrupt the current international order.